Première partie

Techniques mathématiques, à travers l'histoire

Chapitre 1

Calculs polynomiaux

Résumé -

Nous commençons l'année en revisitant l'histoire de la résolution des équations polynomiales. On donne/rapelle ainsi quelques bases essentielles pour la suite : existe-t-il un moyen pour résoudre toute équation polynomiale, on verra que l'important est de pouvoir factoriser ; que nous dit la géométrie des équations polynomiales ; que nous dit l'analyse pour une résolution (approchée) d'une équation polynomiale.
Ce sera l'occasion de mettre en place quelques définitions et de nombreux savoir-faire. Comme chaque chapitre, celui-ci commence par des problèmes ouverts.

Enfin, voici une liste de petites vidéo ou conférence visionnable sur internet et en lien avec le sujet. A visionner à loisir :
- *Mathieu Bautista - L'histoire du x. https ://www.youtube.com/watch ?v=AW7uNg9RLCs*
- *MicMath - Conique à la plage. https ://www.youtube.com/watch ?v=eFPhYYKCyFc*
- *El Jj - Différence équations et fonctions. https ://www.youtube.com/watch ?v=sJKjFgtIBKY*

Sommaire

1. Quelques problèmes 6
1.1. Problèmes 6
1.2. Vocabulaires et contextes 7
2. Equation polynomiale. Algèbre et géométrie 7
2.1. Révolution 1 : Viète 7
2.2. Révolution 2 : Descartes 9
3. Opérer (=calculer) avec des polynômes 12
3.1. Développer 12
3.2. Factoriser 14
3.3. Expliciter formellement les racines 17
4. Equation polynomiale et analyse 18
4.1. La meilleure méthode : l'essai/erreur 18
4.2. Retro-contrôle 19
4.3. Méthode de la sécantes 19
4.4. Vers la dérivation. Méthode de la tangente 20
5. Bilan 21

1. Quelques problèmes

1.1. Problèmes

? Problème 1 - Kwarizmi

Résoudre, comme El Kwarizmi, l'équation $x^2 + 10x = 39$ en n'exploitant que des méthodes géométriques (calcul d'aire, nombres positifs…).
On commence par considérer un carré de côté x et deux rectangles de côtés x et 5. On complète…
Adapter la méthode pour résoudre $x^2 + 21 = 10x$.
Que pensez-vous de la nature des nombres a, b ou c si l'on souhaite générer la méthode pour résoudre l'équation associée au trinôme du second degré : $ax^2 + bx + c = 0$

? Problème 2 - Mauvais vers italiens

« Tartalea exposa sa solution en mauvais vers italiens » (Lagrange, Oeuvres, 1795).
Il existe une méthode (Tartglia-Cardan) pour résoudre les équations de degré 3 (voir cours). Comment pouvait-on l'écrire alors qu'il n'existait ni le symbole =, ni les notations x^2…?

? Problème 3 - Tartaglia et Cardan

Trouver toutes les solutions de l'équation $x^3 + 6x = 20$, avec la méthode de Tartaglia et Cardan, en posant $x = u - v$ et en exploitant les symétries du problème (on peut résoudre : $u^3 - v^3 = \ldots$ et $u^3 v^3 = \ldots$).
Et pour une équation de type $ax^3 + px + q = 0$?
De même donner les solutions de l'équations $x^4 + px^2 + 1 = 0$.

? Problème 4 - Polynôme de degré 2 et représentation graphique

Représenter la courbe d'équation $y = ax^2 + bx + c$.
On fera la différence entre $a > 0$ et $a < 0$. On notera en particulier les coordonnées du sommet

? Problème 5 - Chercher à côté…

Si on sait que $f(x_0) = 0,001$, quelle stratégie mettre en place pour trouver une racine de f? On peut chercher du côté de x_0, pas très loin…

? Problème 6 - Formule de Taylor et développement limité

Soit $f : x \mapsto a_0 + a_1 x + \cdots + a_n x^n$, une fonction polynomiale de degré n.
Pour tout $k \in \mathbb{N}$, exprimer $f^{(k)}(0)$ en fonction des nombres (a_i) qui définissent la fonction polynomiale.
$f^{(k)}(0)$ est la valeur en 0 de la k^e dérivée de la fonction f.

1.2. Vocabulaires et contextes

Principe : On appelle équation, une relation calculatoire avec des objets inconnues i.e. à expliciter, définies à partir de cette (ces) relation(s) calculatoire(s).

Définition - Résoudre une équation
Soit E un ensemble (souvent $E=\mathbb{R}$ ou $\mathbb{C}$ ou $\mathbb{R}^p\ldots$, mais pas uniquement).
Soit une application $f:E\to F$ et $b\in F$(= $\mathbb{R}$ ou $\mathbb{C}$ ou autre).
On dit qu'on résout l'équation $f(x)=b$, d'inconnue $x\in E$, lorsqu'on trouve tous les « nombres » $x\in E$ tel que $f(x)=b$.

On parle d'antécédent de b par f

Remarque - Il n'existe qu'une méthode infaillible pour résoudre une équation : Faire l'essai.
Soit $x_0\in E$. Alors (calcul) : $f(x_0)=\ldots$.
Si la réponse est b, on a trouvé une solution. Sinon, on essaye à nouveau.
Mais cela est souvent long, surtout si l'ensemble E est infini…
Autre question : pourquoi se concentrer (uniquement?) sur des équations polynomiales?

Pour aller plus loin - Des tortues à l'infini
Les mots application (ou fonction), $\mathbb{R}$, $\mathbb{C}$… seront définis (légalisés) plus tard dans l'année ou plus loin dans le polycopié.

2. Equation polynomiale. Algèbre et géométrie

La motivation historiquement première est la motivation ludique. La plupart des résultats ici a été obtenu dans le cadre de joutes mathématiques, de défis si l'on préfère.
Les révolutions successives qui marquent la mathématiques européennes consistent souvent en l'installation de nouvelles notations. Cela crée des ponts!

2.1. Révolution 1 : Viète

Algebra Nova

Heuristique - Généraliser avec des lettres
François Viète a l'idée fondamentale d'écrire des lettres $A,B,C,\ldots X$ pour les inconnues et les données d'un problème (ie. les connus!) et de faire les calculs algébriques. Dès lors, aucun problème des anciens Grecs ne semble résister au schéma :

Problème géométrique $\xrightarrow{\text{mêmes lettres}}$ Problème algébrique $\xrightarrow{\text{calculs}}$ Solution

et Viète écrit en majuscules : *« NVLLVM NON PROBLEMA SOLVERE »*.

Histoire - Algèbre spécieuse
Montucla dans Histoire des mathématiques : *« Il est peu de mathématiciens à qui l'algèbre doive plus qu'à cet homme célèbre… On doit d'abord à M. Viète d'avoir établi l'usage des lettres pour désigner, non seulement les quantités inconnues, mais même celles qui sont connues, ce qui fit donne à son algèbre le nom de spécieuse, nom qu'elle a gardé longtemps, à cause que tout y est représenté par des symboles…*
C'est nous osons le dire à ce changement que l'algèbre est redevable d'une grande partie de ces progrès. »
Comment énoncer aisément la règle du discriminant sans les lettres a, b et c?

Saut historique et définition

Définition - Fonction polynomiale (d'une variable)
On dit que $f:\mathbb{R}\to\mathbb{R}$ est une application polynomiale s'il existe $n\in\mathbb{N}$ et $a_0,a_1,\ldots a_n\in\mathbb{R}$ (voire $\mathbb{C}$) tels que :

pour tout réel x, $f(x)$ est obtenu par le calcul $\sum_{k=0}^{n} a_k x^k$.

On note $f:x\mapsto\sum_{k=0}^{n} a_k x^k$.

Remarque - Un unique type de calcul, pour tout x
C'est toujours le même calcul : une combinaison linéaire des puissances de x qui donne le valeur de $f(x)$.
Cette définition au cas de plusieurs variables (à avoir en tête en particulier pour les manipulations)

Définition - Polynôme de plusieurs variables
On appelle fonction polynomiale de p variables (abrégé ici en « polynôme de p variables ») une fonction de la forme :

$$f_p:(x_1,x_2,\ldots x_p)\mapsto\sum_{(k_1,\ldots k_p)\in\mathbb{N}^p} a_{k_1,k_2,\ldots k_p}\prod_{i=1}^{p}x_i^{k_i}$$

la somme étant finie (nombre de termes est fini) où $\forall\,(k_1,\ldots k_p)\in\mathbb{N}^p$, $a_{k_1,k_2,\ldots k_p}\in\mathbb{R}$ (ou $\mathbb{C}$) ;
Il s'agit d'une combinaison linéaire finie de puissances entières des inconnues réelles (ou complexes) $x_1,\ldots x_p$.
La somme et le produit de deux fonctions polynomiale est une fonction polynomiale.
On appelle degré de f_p, le nombre $\max\{k_1+k_2+\cdots+k_p \mid a_{k_1,k_2,\ldots k_p}\neq 0\}$. Si f n'a qu'une variable, $\deg(f)=\max\{n\in\mathbb{N},$ tel que $a_n\neq 0\}$.

Exemple - $f:(x,y,z)\mapsto 3x^2y-2xyz-xz^2$
Il s'agit d'une fonction polynomiale de trois variables, de degré 3.

Histoire - François Viète



François Viète (1540-1603), n'est pas un mathématicien professionnel, mais un avocat. Néanmoins, il sera le représentant français des joutes mathématiques (cryptanalyse) avec les italiens ou les anglais. Il est célèbre pour son algèbre nouvelle où il est le premier à exploiter les lettres pour décrire les nombres dans des équations. Ce point de vue est révolutionnaire!

Vocabulaire

On donne un peu de vocabulaire et une notation bien pratique, même si historiquement cela s'est fait beaucoup plus tardivement…
Analyse - Unicité d'écriture
Considérons deux fonctions polynomiales $f:x\mapsto\sum_{k=0}^{n}a_kx^k$ et $g:x\mapsto\sum_{k=0}^{m}b_kx^k$.
Supposons qu'il s'agisse bien de deux écritures différentes, donc $\{h\in[\![0,\max(n,m)]\!]\mid a_h\neq b_h\}$ est non vide.
Comme tout ensemble inclus dans $\mathbb{N}$, fini (ou majoré) et non vide, il admet un plus grand élément, notons le h.
On a donc pour tout $x\in\mathbb{R}$:

$$f(x)-g(x)=(a_h-b_h)x^h+\sum_{k=0}^{h-1}(a_k-b_k)x^k$$

On veut montrer que $f\neq g$, ie : $\exists\,x_0\in\mathbb{R}$ tel que $f(x_0)\neq g(x_0)$.
— Méthode 1 (réflexes de terminale) :
$\lim_{x\to+\infty} f(x)-g(x)=\text{signe}(a_h-b_h)\infty$ et $f-g$ est continue, donc nécessairement ie : $\exists\,x_0\in\mathbb{R}$ tel que $f(x_0)-g(x_0)\neq 0$.
— Méthode 2 (même chose mais redémontré). On note $c_k=a_k-b_k$.

$$\frac{f(x)-g(x)}{x^h}=a_h-b_h+\sum_{k=0}^{h-1}\frac{c_k}{x^{h-k}}$$

Pour tout $k\in[\![0,h-1]\!]$, $\frac{c_k}{x^{h-k}}\xrightarrow[x\to+\infty]{}0$.
Il existe donc $X_k\in\mathbb{R}_+^*$ tel que $\forall\,x\geqslant X_k$, $\left|\frac{c_k}{x^{h-k}}\right|\leqslant\frac{|a_h-b_h|}{2h}$.
Il suffit de prendre $X_k=\sqrt[h-k]{2h\frac{|c_k|}{|a_h-b_h|}}$ Et donc pour $x\geqslant X:=\max(X_0,X_1,\cdots X_{h-1})$ (inégalité triangulaire) :

$$\left|\frac{f(x)-g(x)}{x^h}-(a_h-b_h)\right|=\left|\sum_{k=0}^{h-1}\frac{c_k}{x^{h-k}}\right|\leqslant\sum_{k=0}^{h-1}\frac{|a_h-b_h|}{2h}=\frac{|a_h-b_h|}{2}$$

Ainsi, comme $|\alpha| \leqslant \beta \iff -\beta \leqslant \alpha \leqslant \beta$, on a donc pour $x \geqslant X$:

$$-\frac{|a_h - b_h|}{2} \leqslant \frac{f(x) - g(x)}{x^h} - (a_h - b_h) \leqslant \frac{|a_h - b_h|}{2}$$

Et donc si $a_h - b_h > 0$: $\dfrac{f(x) - g(x)}{x^h} \geqslant -\dfrac{a_h - b_h}{2} + (a_h - b_h) = +\dfrac{a_h - b_h}{2} > 0$

Et si $a_h - b_h < 0$: $\dfrac{f(x) - g(x)}{x^h} \leqslant \dfrac{b_h - a_h}{2} + (a_h - b_h) = -\dfrac{b_h - a_h}{2} < 0$

Ainsi, par contraposée : si deux écritures polynomiales donne une même fonction, c'est nécessairement la même écriture!

Définition - Degré et $[f]_k$
Soit f une application polynomiale. Alors son écriture est unique.
Ainsi, il existe un unique $n \in \mathbb{N}$ et un unique $(n+1)$-uplet de réels $(a_0, a_1, \dots, a_n)$ tels que $f : x \mapsto \sum_{k=0}^{n} a_k x^k$.
Le nombre entier n s'appelle le degré de la fonction polynomiale f.
$a_n x^n$ s'appelle le terme dominant de la fonction polynomiale f.
Et on aura pour habitude de noter $[f]_k$, le k coefficient a_k (devant x^k) dans l'écriture de f.

2.2. Révolution 2 : Descartes

Heuristique - Algèbre et géométrie
La motivation est ici GEOMETRIQUE. Une nouvelle façon de concevoir le problème est de maintenant lui donné un sens géométrique et en particulier de donner à $\mathbb{R}$ le sens du continu (comme une droite) et à $f(\mathbb{R})$ une déformation continue de $\mathbb{R}$.

Pour aller plus loin - Notations
Les notations x^5... a été popularisé par Descartes (avant on écrivait simplement xxxxx).
Le symbole = a été popularisé par Leibniz (avant on écrit adeq).

Représentation graphique

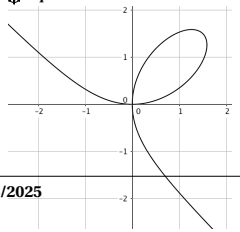
En mathématique, l'apport principal de Descartes a consisté à donner une vision géométrique à l'algèbre et une approche calculatoire à la géométrie (de l'ordre de la précision du langage). C'est une véritable révolution.
Ce qui suit reste vrai même si H n'est pas poiynomiale.

Définition - Graphe dans $\mathbb{R}^2$
Soit $H : \mathbb{R}^2 \to \mathbb{R}$.
On note $\Gamma_H = \{(x, y) \in \mathbb{R}^2 \mid H(x, y) = 0\}$, une sous-partie de $\mathbb{R}^2$.
On dit que $H(x, y) = 0$ est une équation du graphe Γ.

Sans condition supplémentaire sur H, Γ peut être très variés.

Exemple - Folium de Descartes
DESCARTES et ROBERTVAL ont étudié dans leur correspondance la courbe $\mathscr{F}$ d'équation $x^3 + y^3 - 3xy = 0$ (cubique).
Sa représentation graphique est dans la marge.

Représentation - Folium



$\mathscr{F}$ *d'équation* $x^3 + y^3 - 3xy = 0$

Définition - Exemple. Graphe d'une fonction
Si $f : \mathbb{R} \to \mathbb{R}$, on appelle representation graphique de f (ou graphe de f), la courbe $\mathscr{C}$ d'équation $y = f(x)$

Dans ce cas $H : (x, y) \mapsto y - f(x)$. Une telle courbe ne peut « revenir en arrière ». En effet, cela signifierait qu'un nombre x_0 aurait deux images.

Représentation des fonctions polynomiales...

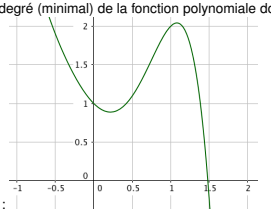
Heuristique - Réprésentation
La représentation d'une fonction polynomiale $x \mapsto \sum_{k=0}^{n} a_k x^k$ est continue.
Cette fonction polynomiale est de degré n, donc admet au plus n racines (de l'équation polynomiale).
Par dérivation (que l'on expliquera plus loin), il y a également au plus n sens de variation différents...

Pour aller plu
Nous reverrons
nuité.
Vous pouvez déj
nition formalisé

Exercice
Donner l'exemple d'une fonction polynomiale de degré 4 n'ayant que deux sens de variations différentes

Correction
$x \mapsto x^4$, tout simplement

Exercice
Quel est le degré (minimal) de la fonction polynomiale dont la représentation graphique est



donnée par :

Correction
C'est un polynôme de degré impair.
Le terme dominant est nécessairement négatif (dominant en $\pm\infty$).
Il y a 3 variations, donc le degré est au moins 3.
(Ici, il s'agit de $x \mapsto x^5 + x^3 + 2x^2 - x + 1$.)

Calculs algébriques et symétries géométriques

Proposition - Translation
La courbe Γ présente une invariance par translation de vecteur $\vec{u} = T\vec{i}$, si et seulement si, on a l'équivalence : $H(x, y) = 0 \iff H(x + T, y) = 0$

Remarque - Qui sont x et y?
Est-ce pour tout x, y ou avec l'existence d'un x et d'un y?
Cela doit être vrai pour x et y dans l'ensemble de définition, puis $x + T$ doit y appartenir également...

Exemple - Graphe d'une fonction
Dans le cas particulier d'une fonction, $\mathscr{C}_f$ présente d'une invariance par translation de vecteur $\vec{u} = T\vec{i}$ si et seulement si $\forall\, x \in \mathscr{D}_f$, $f(x + T) = f(x)$. On dit que f est T-périodique.
En particulier cos ou sin sont 2π-périodique.

Analyse - Symétrie axiale, centrale
Si la courbe présente une symétrie axiale autour de l'axe $x = x_0$.
Alors on a $H(x_0 + x, y) = 0 \iff H(x_0 - x, y) = 0$.
En posant $x' = x_0 + x$, on trouve $x_0 - x = x_0 - (x' - x_0) = 2x_0 - x'$.
Ce qui donne l'équivalence suivante : $H(x, y) = 0 \iff H(2x_0 - x, y) = 0$.
La réciproque est vérifiée.

Proposition - Symétrie axiale
La courbe Γ présente une symétrie axiale d'axe $x = x_0$,
si et seulement si, on a l'équivalence : $H(x,y) = 0 \iff H(2x_0 - x, y) = 0$

Exemple - Graphe d'une fonction
Dans le cas particulier d'une fonction, $\mathscr{C}_f$ présente d'un symétrie axiale d'axe $x = x_0$ si et seulement si $\forall\ x \in \mathscr{D}_f$, $f(2x_0 - x) = f(x)$.
En particulier pour $x_0 = 0$. On dit alors que f est paire (comme $x \mapsto x^2$). Une symétrie centrale de centre $M_0(x_0, y_0)$ est la composition d'une symétrie d'axe $x = x_0$ et d'axe $y = y_0$.

Proposition - Symétrie centrale
La courbe Γ présente une symétrie centrale de centre $M(x_0, y_0)$,
si et seulement si, on a l'équivalence : $H(x,y) = 0 \iff H(2x_0 - x, 2y_0 - y) = 0$

Exemple - Graphe d'une fonction
Dans le cas particulier d'une fonction, $\mathscr{C}_f$ présente d'un symétrie centrale centrée en $M_0(x_0, y_0)$ si et seulement si $\forall\ x \in \mathscr{D}_f$, $f(2x_0 - x) = 2y_0 - f(x)$.
En particulier pour $x_0 = y_0 = 0$. On dit alors que f est impaire (comme $x \mapsto x^3$).

Une astuce pour le calcul

De manière générale, on ne démontre pas un résultat de calcul par une exploitation graphique, mais cela permet largement de vérifier une série de calculs.

Truc & Astuce pour le calcul - Transformer le résultat d'un calcul en une représentation visuelle
Depuis Descartes, l'algèbre et la géométrie sont totalement liés et il est possible de passer « du diable de l'algèbre à l'ange de la géométrie » (Hermann Weyl).
Il est donc important de savoir faire cette transformation : donner du sens géométrique à un calcul algébrique. On peut ainsi anticiper ou vérifier un résultat.

Exercice
Montrer que le système $\begin{cases} x^2+y^2+2x-2y &= 0 \\ x^2+y^2-4y+3 &= 0 \end{cases}$ admet exactement deux solutions.

Correction
Ces équation s'écrivent : $(x+1)^2+(y-1)^2 = 2$ et $x^2+(y-2)^2 = 1$ Il s'agit de l'intersection du cercle de centre $(-1,1)$ de rayon $\sqrt{2}$ (qui passe par O) et du cercle de centre $(0,2)$ et de rayon 1.
Le changement de registre ici est une force si on sait bien l'employer, mais aussi un gros problème pour les élèves bloqués dans leur registre.

Truc & Astuce pour le calcul - Avec des fonctions
Le calcul sur les fonctions est à l'intersection du calcul algébrique, du calcul graphique, du calcul différentiel et intégrale, du calcul de limites…
Les problèmes où interviennent ces fonctions sont aussi très variés, et il n'est pas rare de voir des changements de registre, d'un domaine à l'autre dans une même problème ! Il faut avoir un esprit bien souple…
C'est tout particulièrement le cas de l'étude des polynômes (où l'on bascule facilement d'un domaine à l'autre).

Exercice
Démontrer que le polynôme x^3+3x-1 admet une unique racine sur $\mathbb{R}$

Correction
Il ne faut surtout pas factoriser, mais faire l'étude de la fonction $f : x \mapsto x^3+3x-1$, dérivable et finalement strictement croissante. Elle admet une unique racine sur $\mathbb{R}$ (théorème de la bijection).

3. Opérer (=calculer) avec des polynômes

3.1. Développer

Stabilité

On commence par le développement, c'est a priori plus simple car c'est une opération *mécanique*.
A ce stade, c'est surtout la pratique qui justifie le théorème suivant :

Théorème - Stabilité
L'addition, la soustraction et la multiplication de deux (ou plus) fonctions polynomiales donne une nouvelle fonction polynomiale.

Exercice
Soient $f : x \mapsto 2+x-x^2+3x^3$ et $g : x \mapsto 1+x-x^2+x^4$ définies sur $\mathbb{R}$.
Evaluer, pour tout $x \in \mathbb{R}$, $(f+g)(x)$ et $(f \times g)(x)$

Correction
$f+g : x \mapsto 3+2x-2x^2+3x^3+x^4$.
$f \times g : x \mapsto 2+3x-2x^2+x^3+6x^4$.
Un peu plus théorique :
Exercice
Soient $f : x \mapsto a_0+a_1x+\cdots a_nx^n$ et $g : x \mapsto b_0+b_1x+\ldots b_mx^m$ définies sur $\mathbb{R}$.

1. Evaluer, pour tout $x \in \mathbb{R}$, $(f+g)(x)$ et $(f \times g)(x)$.
2. Exprimer alors, pour tout $k \in \mathbb{N}$, $[f+g]_k$ en fonction des $[f]_i$ et $[g]_j$.
3. Exprimer alors, pour tout $k \in \mathbb{N}$, $[f \times g]_k$ en fonction des $[f]_i$ et $[g]_j$.

Correction

1.
2. On trouve $[f+g]_k = [f]_k + [g]_k$, et de manière générale, cette opération est linéaire.
3. On a le produit de Cauchy : $[f \times g]_k = \sum_{i=0}^{k} [f]_i [g]_{k-i} = \sum_{i+j=k} [f]_i [g]_j$, valable même si les coefficients sont nuls.

Développer malin

Mais il existe plusieurs façons de développer un produit polynomial. Certaines sont plus intelligentes que d'autres…
Exercice
Développer $(a+b+c)^3$

Correction
La solution sera de la forme $\sum A_{i,j,k} a^i b^j c^k$ avec $i+j+k = 3$. Reste à trouver la valeur de $A_{i,j,k}$.
Pour obtenir, par exemple, le nombre $A_{1,1,1}$, il faut prendre un a, un b et un c, il y a $3 \times 2 \times 1 = 3! = 6$ possibilités.
Pour obtenir, par exemple, le nombre $A_{1,2,0}$, il faut prendre un a, deux b et 0 c, il y a $3 \times 1 \times 1 = 3 = 3$ possibilités.
Ensuite il y a une symétrie entre a, b et c qui commutent : $A_{1,2,0} = A_{0,2,1} = \cdots = A_{0,1,2}$.
Finalement : $(a+b+c)^3 = 6abc + 3(a^2b+a^2c+b^2c+b^2a+c^2a+c^2b)$
Exercice
On admet que $(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$.
En organisant convenablement votre calcul $(a+b)^5$, trouver comment passer des coefficients (1,4,6,4,1) de $(a+b)^4$ à ceux de $(a+b)^5$.
Cela vous rappelle-t-il quelque chose ? En déduire la formule générale qui donne une expression de $(a+b)^n$.

Correction
$(a+b)^5 = (a+b)^4(a+b) = a(a+b)^4 + b(a+b)^4$

$$\begin{array}{rccccccc} = & a^5 & +4a^4b & +6a^3b^2 & +4a^2b^3 & +ab^4 & & \\ & & +a^4b & +4a^3b^2 & +6a^2b^3 & +4ab^4 & +b^5 & \\ = & (1+0)a^5 & +(4+1)a^4b & +(6+4)a^3b^2 & +(4+6)a^2b^3 & +(1+4)ab^4 & +(0+1)b^5 & \\ = & a^5 & +5a^4b & +10a^3b^2 & +10a^2b^3 & +5ab^4 & +b^5 & \end{array}$$

On retrouve le triangle de Pascal : de $(1,4,6,4,1)$ à $(1,5,10,10,5,1)$… Cela ne fait pas une démonstration mais permet d'anticiper, comprendre, retenir la formule du binôme de Newton :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Truc & Astuce pour le calcul - Anticipation

Il s'agit de ne plus être à chaque instant derrière son calcul, mais bien en avant!. Il s'agit bien là aussi de voir quelque chose… Lorsque le calcul demandé est ouvert (on ne donne pas une forme fermée : montrer que $A = B$), il faut savoir vers où l'on va.
Par exemple, lorsqu'on dérive une fonction, ce qui nous intéresse souvent c'est de connaître son signe. Il faut donc donner une forme factorisée…

Exercice
On peut exprimer de 3 façons différentes $A = f(x) = (3x^2+8x-1)-(x^2+3x-4)$. Associer chacune de ces expressions à l'exploitation qu'on peut en faire.

$A = 2x^2+5x-3$	étude du minimum de f
$A = -6+3(x+1)+2(x+1)^2$	développement limité de f en -1
$A = 2\left(x+\frac{5}{4}\right)^2 - \frac{49}{8}$	étude du signe de f
$A = (x+3)(2x-1)$	étude du polynôme f

Correction

$A = 2x^2+5x-3$	$\longrightarrow$	étude du polynôme f
$A = -6+3(x+1)+2(x+1)^2$	$\longrightarrow$	développement limité de f en -1
$A = 2\left(x+\frac{5}{4}\right)^2 - \frac{49}{8}$	$\longrightarrow$	étude du minimum de f
$A = (x+3)(2x-1)$	$\longrightarrow$	étude du signe de f

Truc & Astuce pour le calcul - Reconnaissance de formes

En visualisant les formes dans les formules, il est plus aisé de garder en mémoire le calcul effectué (pour le retro-contrôle) et surtout, il est plus aisé de savoir dans quel ordre faire le calcul de manière à être efficace : ne pas se tromper et agir rapidement.

Exercice
Démontrer :
$4[(a^2-b^2)cd+(c^2-d^2)ab]^2 + [(a^2-b^2)(c^2-d^2)-4abcd]^2 = (a^2+b^2)^2(c^2+d^2)^2$
On pourra y voir la forme $A = B^2 - C^2$…

Correction
Notons $B = (a^2+b^2)(c^2+d^2)$ et $C = (a^2-b^2)(c^2-d^2)-4abcd$. Alors
$B^2 - C^2 = (B-C)(B+C)$
$= [(a^2+b^2)(c^2+d^2)-(a^2-b^2)(c^2-d^2)+4abcd]\,[(a^2+b^2)(c^2+d^2)+(a^2-b^2)(c^2-d^2)-4abcd]$
$= [2a^2d^2+2b^2c^2+4abcd]\,[2a^2c^2+2b^2d^2+4abcd] = 4\left[(ad+bc)^2\right]\left[(ac-bd)^2\right]$
On reconnait une fois E^2+F^2+2EF et une fois F^2+G^2-2FG. Donc
$B^2-C^2 = 4\big((ad+bc)(ac-bd)\big)^2 = 4(a^2dc+c^2ab-b^2cd-d^2ab)^2 = 4[(a^2-b^2)cd+(c^2-d^2)ab]^2$

Attention - Ne pas trop écrire

Pour apprendre à se projeter vers l'avant, il faut ne pas écrire trop de calculs intermédiaires. De nombreuses petites réécritures doivent être simplement pensées, sans être écrites.
Le prix à payer : une insécurité forte pour l'élève.
Le prix à gagner : une plus grande concentration et une meilleure vitesse d'exécution!

, Deux ans avant les concours, il faut investir dans cette stratégie.

Truc & Astuce pour le calcul - Garder en mémoire « vive » le calcul

Si on garde en mémoire immédiate le calcul, il est possible de déceler les erreurs plusieurs lignes de calcul plus loin. On évite des erreurs bêtes, comme des signes + et − qui se mélangent, une page qui se tourne et qui conduit à des nombres qu'on oublie…
Pour apprendre à exploiter une mémoire globalisante du calcul, on peut essayer après chaque calcul à réécrire le résultat obtenu sur une page blanche. Evidemment, un tel résultat doit rester en mémoire immédiate, il n'est pas nécessaire de le placer en mémoire de travail plus profonde.

Exercice
Quel est le résultat obtenu lors du dernier calcul que vous avez effectué ?

Correction

3.2. Factoriser

Avec les petits Bernoullis

Analyse - $x^k - a^k$

Considérons une inconnue réelle x et une connue a.
$(x-a)(x^4+x^3a+x^2a^2+xa^3+a^4) = x^5+x^4a+x^3a^2+x^2a^3+xa^4-x^4a-x^3a^2-x^2a^3-xa^4-a^5 = x^5-a^5$.
Soit $k \in \mathbb{N}^*$.
Calculons

$$\begin{aligned}(x-a)\sum_{i=0}^{k-1} x^i a^{k-1-i} &= (x-a)\times\left(x^{k-1}+x^{k-2}a+x^{k-3}a^2+\dots xa^{k-2}+a^{k-1}\right)\\ &= x^k - x^{k-1}a + x^{k-1}a - x^{k-2}a^2 + \dots + x^2a^{k-2} - xa^{k-1} + xa^{k-1} - a^k = x^k - a^k\end{aligned}$$

Exercice
Comment rendre ce calcul rigoureux ?

Correction
Avec des suites géométriques, ou par récurrence (voir plus bas) ou par télescopage (cf chapitre sur les sommes)

Pour aller plus loin - Polynômes de Bernoulli

On appelle (ici en MPSI3) cette famille de polynômes, les « petits Bernoullis », pour ne pas les confondre.

Définition - Les petits Bernoullis

Pour tout $n \in \mathbb{N}$ et $a \in \mathbb{K}$, on note $b_a^n : x \mapsto x^n + ax^{n-1} + \dots a^{n-1}x + a^n = \sum_{i=0}^{n} x^i a^{n-i}$.
On appelle cette famille de fonctions polynomiales $(b_a^n)_{n\in\mathbb{N}}$, les petits Bernoullis.
On a alors :

$$\forall\, x \in \mathbb{K}, \qquad (x-a)\times b_a^n(x) = x^{n+1} - a^{n+1}$$

Il faut faire une démonstration. On exploite le résultat sur les sommes des termes consécutifs d'une suite géométrique, vu en terminale.

Démonstration
Notons que pour $x \neq a$:

$$b_a^n(x) = \sum_{i=0}^{n} x^i a^{n-i} = a^n \sum_{i=0}^{n} \left(\frac{x}{a}\right)^i = a^n \frac{1-\left(\frac{x}{a}\right)^{n+1}}{1-\frac{x}{a}} = a\frac{a^n - \frac{x^{n+1}}{a}}{a-x} = \frac{x^{n+1}-a^{n+1}}{x-a}$$

Donc pour $x \neq a$: $(x-a)b_a^n(x) = x^{n+1} - a^{n+1}$.
Et si $x = a$: on a aussi $(x-a)b_a^n(x) = 0 = x^{n+1} - a^{n+1}$. □

Exercice

En notant que $b_a^{n+1} = ab_a^n + x^{n+1}$ (à démontrer), montrer par récurrence la factorisation de Bernoulli

Correction

Notons, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$: « $\forall\, x \in \mathbb{K},\ (x-a)b_a^n(x) = x^{n+1} - a^{n+1}$. »

— $(x-a)b_a^0(x) = (x-a)1 = x-a$. Donc $\mathscr{P}_0$ est vraie.

— Soit $n \in \mathbb{N}$. On suppose $\mathscr{P}_n$ vraie : $\forall\, x \in \mathbb{K},\ (x-a)b_a^n(x) = x^{n+1} - a^{n+1}$.
Pour tout $x \in \mathbb{K}$, $(x-a)b_a^{n+1}(x) = (x-a)(x^{n+1} + ab_a^n) = x^{n+2} - ax^{n+1} + a(x^{n+1} - a^{n+1}) = x^{n+2} - a^{n+2}$.
Donc $\mathscr{P}_{n+1}$ est vraie.

Grâce à une racine

On a les corollaires important suivant :

Proposition - Factorisation (1)
Soit f une fonction polynomiale de degré n.
Pour tout $a \in \mathbb{K}$, il existe g_a, fonction polynomiale de degré $n-1$ tel que

$$\forall\, x \in \mathbb{K}, \qquad f(x) - f(a) = (x-a)g_a(x)$$

Démonstration

Supposons que $f(x) = \sum_{k=0}^{n} c_k x^k$ avec $c_n \neq 0$.

Alors

$$\begin{aligned} f(x) - f(a) &= \sum_{k=0}^{n} c_k x^k - \sum_{k=0}^{n} c_k a^k = \sum_{k=1}^{n} c_k (x^k - a^k) + c_0 - c_0 \\ &= \sum_{k=1}^{n} c_k (x-a) b_a^{k-1}(x) = (x-a) \times \underbrace{\sum_{k=1}^{n} c_k b_a^{k-1}(x)}_{=g_a(x)} \end{aligned}$$

On note bien que g_a est une fonction polynomiale. Le terme x^{n-1}, apparait avec le coefficient $c_n \neq 0$ dans b_a^{n-1} uniquement. Aucun monôme de degré plus élevé n'apparait dans la combinaison linéaire. □

Corollaire - Factorisation (2)
Soit f une application polynomiale sur $\mathbb{K}$(=$\mathbb{R}$ ou $\mathbb{C}$) de degré n.
Soit $x_0 \in \mathbb{K}$ tel que $f(x_0) = 0$.
Alors il existe g, application polynomiale de degré $n-1$ telle que

$$\underbrace{\text{pour tout } x \in \mathbb{K},}_{\forall\, x \in \mathbb{K}} \qquad f(x) = (x - x_0) \times g(x)$$

Savoir que g existe est une excellente chose.
Mais savoir comment obtenir g connaissant x_0 et f est encore mieux (sans développer tous les petits Bernoullis) !
On peut donc décrire un algorithme pour obtenir g :

Savoir faire - Factoriser

Notons $f : x \mapsto x^3 + 2x^2 - x - 2$.
Alors $f(1) = 1 + 2 - 1 - 2 = 0$. Donc $f(x) = (x-1) \times g(x)$.
Pour appliquer l'algorithme, on prend l'habitude d'écrire le plus à gauche le terme sur lequel on agit en premier (comme pour une division euclidienne entière), on écrit donc les polynômes dans le sens des puissances décroissantes :

x^3	$+2x^2$	$-x$	-2	$x-1$
	$(2+1)x^2$			$1x^2+3x+2$
		$(-1+3)x$		
			$-2+2$	

Donc $x^3 + 2x^2 - x - 2 = (x-1)(x^2+3x+2)$.
On oublie jamais de **vérifier le calcul réciproque** s'il est beaucoup plus simple !

Pour aller plus loin - Division euclidienne
En fait on obtient ici un algorithme de division euclidienne. Mais uniquement par un polynôme de degré 1.
On reprendra cela plus tard.

Trouver toutes les racines

La factorisation permet de décomposer un problème en plusieurs sous-problèmes.

Proposition - Factorisation
Soient f et g deux fonctions polynomiales à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $x \in \mathbb{K}$.
$f(x) \times g(x) = 0$ si et seulement si $f(x) = 0$ ou $g(x) = 0$

Pour ce genre de proposition, on fait un raisonnement en deux temps (double implication) :

Pour aller plus loin - Anneaux intègres
Un ensemble d'élément neutre 0 *pour une première loi* + *et vérifiant :*

$$a \times b = 0 \Longrightarrow a = 0 \text{ ou } b = 0$$

est appelé ensemble intègre.
$\mathbb{R}$ *ou* $\mathbb{C}$ *sont intègres. Ce n'est pas le cas de* $\mathscr{M}_n(\mathbb{R})$.

Démonstration

Si $f(x) = 0$ ou $g(x) = 0$, alors $f(x) \times g(x) = 0$, car l'un des deux termes est nuls.
Réciproquement. Si $f(x) \times g(x) = 0$, alors car $\mathbb{K}$ est intègre : $f(x) = 0$ ou $g(x) = 0$ □

Exercice

Trouver toutes les racines réelles de l'équation $x^4 - 5x^2 + 4 = 0$

Correction

On note $f(x) = x^4 - 5x^2 + 4$.
On a $f(1) = 1 - 5 + 4 = 0$, et comme f est paire (bi-carrée), $f(-1) = 0$.
$f(x) = (x-1)(x^3 + x^2 - 4x - 4) = (x-1)(x+1)(x^2-4) = (x-1)(x+1)(x-2)(x+2)$.
Un produit de nombres réels est nul si et seulement si l'un des facteurs est nul ($\mathbb{R}$ intègre).

$$f(x) = 0 \Longleftrightarrow x = 1 \text{ ou } x = -1 \text{ ou } x = 2 \text{ ou } x = -2$$

Théorème - Factorisation multiple
Soit f une fonction polynomiale de degré n. Soit $p \leqslant n$
Si $x_1, x_2, \ldots x_p$, p solutions différentes de l'équation $f(x) = 0$ (racines de f).
Alors il existe g_p, fonction polynomiale de degré $n-p$ tel que

$$\forall\, x \in \mathbb{K}, \qquad f(x) = (x - x_1)(x - x_2)\ldots(x - x_p) \times g_p(x)$$

Démonstration

On fait une récurrence finie sur $p \leqslant n$.

— $\mathscr{P}_0$ (et $\mathscr{P}_1$) est vraie.

— Soit $p < n$. Supposons que $\mathscr{P}_p$ est vraie.
Soient $x_1, x_2, \ldots x_p, x_{p+1}$ $p+1$ solutions de $f(x) = 0$.
Alors d'après $\mathscr{P}_p$. Il existe g_p de degré $n-p$ tel que

$$\forall\, x \in \mathbb{K}, \qquad f(x) = (x - x_1)(x - x_2)\ldots(x - x_p) \times g_p(x)$$

Puis $f(x_{p+1}) = 0 = (x_{p+1} - x_1)(x_{p+1} - x_2)\ldots(x_{p+1} - x_p) \times g_p(x_{p+1})$.
Comme $x_{p+1} \neq x_i$, alors $x_{p+1} - x_i \neq 0$ et nécessairement $g_p(x_{p+1}) = 0$.
Et donc il existe g_{p+1} de degré $n-p-1$ tel que

$$\forall\, x \in \mathbb{K}, \qquad g_p(x) = (x - x_{p+1}) \times g_{p+1}(x) \Rightarrow \forall\, x \in \mathbb{K}, \qquad f(x) = (x - x_1)\ldots(x - x_{p+1}) \times g_{p+1}(x)$$

Et donc $\mathscr{P}_{p+1}$ est vraie.

La récurrence est démontrée □

On arrive à un résultat énoncé par Descartes, mais pas vraiment démontré…

Corollaire - Nombre maximal de solution
Une équation polynomiale de degré n admet au plus n solutions différentes

Démonstration
Il suffit de raisonner par l'absurde □

Identification

Il n'existe qu'une seule fonction polynomiale nulle :

Proposition - Une seule fonction polynomiale nulle
Si $f : x \mapsto \sum_{i=0}^{n} a_i x^i$ est une fonction polynomiale nulle alors pour tout $i \in \mathbb{N}$, $a_i = 0$.

Démonstration
On fait un raisonnement par contraposée.
Si f n'est pas le polynôme nulle, elle est de degré n avec $n \geqslant 0$ (rappelons que le polynôme nul est de degré $-\infty$).
Donc f admet au plus n racines. Donc f n'est pas identiquement nul.
Bilan : $\exists\, i \in \mathbb{N}$ tel que $a_i \neq 0 \Longrightarrow f \neq 0$. □

Avec la même démonstration améliorée et adaptée à $f-g$, on trouve :

Proposition - Identification des coefficients
Soient f et g deux fonctions polynomiales et $E \subset \mathbb{C}$ tel que $\forall\, x \in E$, $f(x) = g(x)$.
Si $\text{card}(E) > \deg(f-g)$, alors $f = g$.
Plus précisément : pour tout $k \in \mathbb{N}$, $[f-g]_k = 0$ donc $[f]_k = [g]_k$

Remarque - Essentiel
On aura noté que :
- $[p]_k$ est le coefficient du polynôme p devant le monôme x^k. C'est une application linéaire.
- L'addition, la multiplication et la composition de deux polynômes donnent toujours un polynôme.

3.3. Expliciter formellement les racines

Avec les notations de Viète, il est facile de donner toutes les racines (complexes) d'un polynôme de degré 2 à coefficients dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, à condition de savoir calculer la racine carrée d'un nombre complexe (cas où $\Delta \in \mathbb{C} \setminus \mathbb{R}$).

Proposition - Discriminant
On considère l'équation $ax^2 + bx + c = 0$, où $a, b, c \in \mathbb{R}$ ou $\mathbb{C}$.
On note $\Delta = b^2 - 4ac$.
Si δ vérifie $\delta^2 = \Delta$, alors les racines de cette équation sont $\dfrac{-b+\delta}{2a}$ et $\dfrac{-b-\delta}{2a}$

On commence par une petite remarque :

Remarque - Théorème de Viète
Soient $(S, P) \in \mathbb{C}^2$. Les solutions du système

$$\begin{cases} z_1 + z_2 = S \\ z_1 \times z_2 = P \end{cases}$$

sont exactement (à permutation près) les solutions de $x^2 - Sx + P = 0$.
En effet :

$$(x-z_1)(x-z_2) = x^2 - (z_1+z_2)x + z_1 z_2 = x^2 - Sx + P$$

Démonstration
Il suffit de calculer

$$(x-\frac{-b+\delta}{2a})(x-\frac{-b-\delta}{2a} = x^2 - \left(\frac{-b+\delta}{2a} + \frac{-b-\delta}{2a}\right)x + \frac{-b+\delta}{2a} \times \frac{-b-\delta}{2a} = x^2 + \frac{b}{a}x + \frac{b^2-\delta^2}{4a^2} = \frac{1}{a}(ax^2+bx+c) = 0$$

□

Remarque - Autres idées de démonstration ?
Avec la forme canonique.
En réfléchissant sur la symétrie et la moyenne des racines... On ne démontre pas ces résultats qui datent du XVI siècle :

Proposition - Formule de Tartaglia-Cardan (1545)
Les solutions complexes z_k ($k \in \{0,1,2\}$) de l'équation du troisième degré $x^3 + px + q = 0$ où p et $q \in \mathbb{R}$ sont donnés par

$$z_k = u_k + v_k$$

avec $u_k = j^k \sqrt[3]{\frac{1}{2}(-q + \sqrt{\frac{-\Delta}{27}})}$, $v_k = j^{-k} \sqrt[3]{\frac{1}{2}(-q - \sqrt{\frac{-\Delta}{27}})}$
et où $j = e^{\frac{2i\pi}{3}}$ et $\Delta = -(4p^3 + 27q^2)$ est le discriminant de l'équation.
On peut vérifier que $\Delta = (z_0-z_1)^2(z_1-z_2)^2(z_2-z_0)^2$ et $3u_k v_k = -p$

Exercice
Faire la démonstration

Correction
On calcule. Intelligemment...

Exemple - Racines de l'équation $x^3 - 2x = 4$
Ici $p = -2$ et $q = -4$. Donc $\Delta = -(4 \times (-8) + 27 \times 16) = -25 \times 16$.
Ainsi $u_k = j^k \sqrt[3]{\frac{1}{2}(4 + \frac{20}{\sqrt{27}}} = \frac{1}{\sqrt{3}} j^k \sqrt[3]{(6\sqrt{3}+10}$ et de même $v_k = \frac{1}{\sqrt{3}} j^k \sqrt[3]{(6\sqrt{3}-10}$
Ainsi $z_0 = \frac{1}{\sqrt{3}}\left(\sqrt[3]{(6\sqrt{3}+10} + \sqrt[3]{(6\sqrt{3}-10}\right) = \cdots = 2$.
On peut par exemple chercher des nombres entiers a, b tels que $(a\sqrt{3}+b)^3 = 6\sqrt{3}+10$... par développement, divisibilité, essai/erreur, on trouve : $(\sqrt{3}+1)^3 = 6\sqrt{3}+10$ et $(\sqrt{3}-1)^3 = 6\sqrt{3}-10$...
On peut vérifier qu'il est plus simple ici de voir que 2 est racine évidente, factoriser par $(x-2)$, puis trouver les deux autres racines conjuguées...

Remarque - Degré 4
Il existe également une formule pour l'équation de degré 4. Vous la trouverez sans problème sur internet.
Vous y trouverez également l'histoire de la découverte des ces formules. C'est assez intéressant Nous ne démontrons pas :

Histoire - Niels Henrik Abel



Niels Henrik Abel *(1802-1829) est un mathématicien norvégien génial, mort très jeune. Une météorite dans le ciel septentrional.*

Théorème - Ruffini-Abel (1824)
Pour tout entier $n \geqslant 5$, il n'existe pas de formule générale exprimant « par radicaux » les racines d'un polynôme quelconque de degré n.
C'est-à-dire de formule n'utilisant que les coefficients, la valeur 1, les quatre opérations et l'extraction des racines n-ièmes

4. Equation polynomiale et analyse

4.1. La meilleure méthode : l'essai/erreur

Heuristique - La meilleure solution

Si l'on veut résoudre un problème, dont on ne sait rien excepté ses réalisations pour certains réalisations des variables. Alors la solution naturelle consiste à faire des essais/erreurs.
Concrètement, pour résoudre $f = 0$, on prend une première valeur pour x. On essaye $f(x_1)$.
Est-il égal à 0?
Si non, on essaye une autre valeur…

Est-il possible d'apprendre de nos essais/erreurs?

4.2. Retro-contrôle

Une méthode classique en ingénierie (mais aussi en biologie) est d'exploiter le retro-contrôle ou une retro-action positive.

Truc & Astuce pour le calcul - Exploiter le retro-contrôle

Pour du calcul raisonné, il s'agit d'abord de réinjecter les résultats obtenus dans la formule initiale pour voir si le résultat est juste.
Mais si le résultat n'est pas juste, alors tout n'est pas perdu : il ne faut pas repartir de 0. Avec le calcul de vérification, il est parfois possible de voir où est l'erreur (erreur de signe, oublie d'un puissance…).
Et le second résultat ne doit pas être trop éloigné du premier résultat (plus grand si la fonction est croissante…).
Principe : on crée une suite (x_n) qui converge vers x, la vraie valeur que l'on cherche.
A chaque étape, on prend $x_{n+1} = x_n + y_n$, meilleure approximation de x que x_n,
et donc y_n est une suite telle que :
— y_n est beaucoup plus petit que x_n, donc négligeable face à x_n
— $(y_n) \to 0$
— pour $k \in N$, $k \geqslant 2$, y_n^k est toujours beaucoup plus petit que y_n, donc négligeable face à y_n^k.

Nous allons expliquer la méthode à partir d'un exercice. Exercice

On cherche à donner une valeur approchée de $\sqrt{8}$. Donner une valeur approchée (à deux chiffres), par rétro-contrôle

Correction

$\sqrt{8} \approx \sqrt{9} = 3$. On a donc $\sqrt{8} = 2,\ldots$. On pose donc $x_1 = 3$. On considère $x_2 = x_1 + y_1 = 3 + y_1$. On a alors $x_2^2 = x_1^2 + 2x_1y_1 + y_1^2 = 9 + 6y_1 + y_1^2$.

On aimerait être proche de 8 pour x_2^2, et donc si y_1^2 est négligeable par rapport à y_1, on a $6y_1 = -1$, donc $y_1 = -\frac{1}{6}$.

On considère donc $x_2 = 3 - \frac{1}{6} = \frac{17}{6}$.

On considère ensuite $x_3 = x_2 + y_2$, donc $x_3^2 = x_2^2 + 2x_2y_2 + y_2^2 = \frac{289}{36} + \frac{17}{3}y_2 + y_2^2$.

On aimerait être proche de 8 pour x_3^2, et donc si y_2^2 est négligeable par rapport à y_2, on a $\frac{17}{3}y_2 = -\frac{288-289}{36} = \frac{-1}{36}$, donc $y_2 = -\frac{-1}{204}$.

On considère donc $x_3 = \frac{17}{6} - \frac{1}{204} = \frac{17^2 \times 2 - 1}{204} = \frac{577}{204}$.

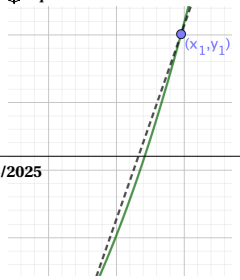
On a (calculatrice) : $\sqrt{8} = 2,8284\ldots$

4.3. Méthode de la sécantes

Analyse - Principe

On cherche à résoudre une équation polynomiale $f(x) = 0$.
On essaye : $f(x_1) = y_1 \neq 0$ et $f(x_2) = y_2 \neq 0$.
Que valeur x_3 choisir pour obtenir une bonne approximation de la solution à $f(x) = 0$.
On peut faire une représentation graphique.
— Si $y_1 = -y_2$, on a envie d'essayer $x_3 = \frac{1}{2}(x_1 + x_2)$.
— si y_1 est proche de 0 et y_2 est loin. On va prendre x_3 proche de x_1.
Plus grand, plus petit? Selon les signes de y_1 et y_2, on peut imaginer que x_3 est entre x_1 et x_2, ou non.

Représentation - Méthode de la sécante



— …

Est-il possible de réponde quantitativement à cette question?
On connait deux points de la courbe $y = f(x)$, on peut imaginer que la droite qui passe par ces deux points est la meilleure approximation de la fonction polynomiale.
On cherche alors la racine du polynôme, de degré 1, qui passe par ces deux points.
C'est la fonction polynomiale $d(x) = \frac{y_2-y_1}{x_2-x_1}(x - x_1) + y_1$.
En effet, par construction : $f(x_1) = y_1$ et $f(x_2) = y_2$.
On prend alors x_3, tel que $d(x_3) = 0$, i.e. : $x_3 = x_1 - \frac{x_2 - x_1}{y_2 - y_1}y_1$

Définition - Algorithme de la sécante

Considérons la fonction polynomiale $f(x) = \sum_{k=0}^{n} a_k x^k$.
On considère deux nombres $a, b \in \mathbb{R}$, puis la suite (u_n) définie par :

$$u_0 = a,\ u_1 = b \forall\ n \in \mathbb{N},\ u_{n+2} = u_{n+1} - \frac{u_{n+1} - u_n}{f(u_{n+1}) - f(u_n)} f(u_{n+1})$$

La suite ainsi définie suit l'algorithme de la sécante

Pour aller plus loin - Convergence

Nous verrons plus loin ce que signifie la convergence pour une suite.
Vous pouvez déjà chercher à donner une définition formalisée…

Sous certaines conditions, relativement robuste, la suite (u_n) converge vers une racine de f

4.4. Vers la dérivation. Méthode de la tangente

Analyse - Quand 0 s'invite

Au moment de la convergence vers une limite notée x, on trouve que u_n comme u_{n+1} est proche de x. Et donc $u_{n+1} - u_n$ est proche de 0.
Mais c'est aussi le cas de $f(u_n) \approx f(x) \approx f(u_{n+1})$.
On se trouve donc naturellement en présence d'une forme indéterminée $\frac{0}{0}$.
Comment gérer cette forme?

Heuristique - Toute forme indéterminée $\frac{0}{0}$…

| … peut se voir comme un calcul de dérivée, avec la formule de L'HOSPITAL.

Rappelons ce qu'est un nombre dérivée :

Définition - Nombre dérivée

Soit f une fonction (polynomiale), on appelle dérivée de f en x_0, le nombre :

$$\lim_{h\to 0} \frac{f(x_0 + h) - f(x_0)}{h} = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

On note ce nombre $f'(x_0)$, selon la notation de Lagrange (1797).

Exemple - Monôme et polynôme. Dérivation

Considérons h petit (en valeur absolue), que pensez de $(x + h)^n$?
C'est un polynôme en x de degré n. Il vaut presque x^n (surtout si h petit). On peut appliquer les petits Bernoullis :

$$k > 0, \qquad (x+h)^k - x^k = -(x^k - (x+h)^k) = -(x - (x+h)) \times b_{x+h}^k = h \times \sum_{i=0}^{k-1} (x+h)^{k-1-i} x^i$$

Notons que pour $k = 0$, $(x + h)^k - x^k = 1 - 1 = 0$. Donc si $f(x) = \sum_{k=0}^{n} a_k x^k$, par linéarité :

$$f(x + h) - f(x) = h \times \sum_{k=1}^{n} a_k \sum_{i=0}^{k-1} (x + h)^{k-1-i} x^i$$

Par conséquent (par continuité polynomiale)

$$\frac{f(x+h) - f(x)}{h} = \sum_{k=1}^{n} \sum_{i=0}^{k-1} (x + h)^{k-1-i} x^i \underset{h\to 0}{\Longrightarrow} \sum_{k=1}^{n} a_k \sum_{i=0}^{k-1} x^k = \sum_{k=1}^{n} k a_k x^{k-1}$$

Finalement : la dérivée de $x \mapsto b_0 + b_1 x + \dots b_n x^n$ est $x \mapsto b_1 + 2b_2 x + \dots n b_n x^{n-1}$.

Analyse - Méthode de la tangente

On a donc pour $u_n = x + h_n$, avec h_n proche de 0, $f(u_n) = f(x+h_n) = f(x) + h_n f'(x)$:

$$\frac{u_{n+1} - u_n}{f(u_{n+1}) - f(u_n)} = \frac{(x+h_{n+1}) - (x+h_n)}{[f(x) + h_{n+1}f'(x)] - [f(x) + h_n f'(x)]} = \frac{1}{f'(x)}$$

On a l'aglorithme suivant qu'on associe à NEWTON, pour son utilisation en toute généralité :

Définition - Algorithme de la tangente

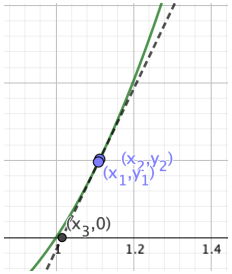
Considérons la fonction polynomiale $f(x) = \sum_{k=0}^{n} a_k x^k$.
On considère deux nombres $a \in \mathbb{R}$, puis la suite (u_n) définie par :

$$v_0 = a, : \forall\ n \in \mathbb{N}, v_{n+1} = v_n - \frac{1}{f'(v_n)} f(v_n)$$

La suite ainsi définie suit l'algorithme de la tangente

Sous certaines conditions, relativement robuste, la suite (v_n) converge vers une racine de f

Représentation - Méthode de la tangente (Newton)



Pour aller plus loin - Méthode de la Newton

En informatique, au second semestre, nous justifierons plus précisément l'algorithme de Newton. Nous donnerons des conditions de convergence.

5. Bilan

Synthèse

- ⇝ En science, les problèmes se traduisent sous forme d'équations, souvent polynomiales. Ces fonctions polynomiales sont très présentes car elles sont stables par addition, multiplication et composition. La multiplication s'appelle développement. On développe avec intelligence !
- ⇝ Le plus important pour résoudre une équation est de savoir factoriser. Le théorème de factorisation est très important : il permet de séparer les problèmes de résolution.
  Dans quelques rares cas (degré faible), il existe des formules explicites qui donnent les expressions des racines d'une fonction polynomiale.
- ⇝ On peut aussi regarder les fonctions polynômiales comme des transformations géométriques de la droite réelle. Faire le lien : fonction polynomiale/représentation géométrique permet d'enrichir chacun des deux points de vue. On peut penser à l'exemple des coniques.
- ⇝ Une autre idée est d'exploiter ce lien pour chercher les racines : localement une branche de courbe polynomiale ressemble à un segment de droite. Les algorithmes de la sécante ou de la tangente exploitent cette idée pour trouver une valeur approchée d'une racine d'une fonction polynomiale.

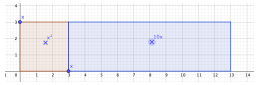
Savoir-faire et Truc & Astuce du chapitre

- — Truc & Astuce pour le calcul - Anticipation
- — Truc & Astuce pour le calcul - Reconnaissance de formes
- — Truc & Astuce pour le calcul - Garder en mémoire « vive » le calcul
- — Savoir-faire - Factoriser
- — Truc & Astuce pour le calcul - Exploiter le retro-contrôle

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$[f]_k$	coefficient de la fonction polynomiale f devant le monôme x^k	Linéarité : $[\lambda f + \mu g]_k = \lambda [f]_k + \mu [g]_k$	$\deg f = n \iff \forall\ k > n, [f]_k = 0$
		Convolution : $[f \times g]_k = \sum_{i=0}^{k} [f]_i [g]_{k-i}$	
$b_a^n(x)$	Petit Bernoulli en a d'indice n	$\forall\ x \in \mathbb{K}\ b_a^n(x) = \sum_{i=0}^{n} x^i a^{n-i}$ (fonction polynomiale)	$x^{n+1} - a^{n+1} = (x-a) \times b_a^n(x)$

Retour sur les problèmes

1. 
2. Il faut transformer en phrase les opérations $\times, \sqrt{\cdot}\dots$
3. $x = u - v$, $x^3 = (u-v)^3 = u^3 - 3u^2 v + 3uv^2 - v^3$.
   On a donc : $x^3 + 6x - 20 = u^3 - v^3 - 3uv(u-v) + 6x - 20 = u^3 - v^3 + 3x(2 - uv) - 20$.
   Ajoutons la condition $uv = 2$, on a donc $u^3 - v^3 = 20$ et $u^3 v^3 = 8$.
   Ainsi, u^3 et $-v^3$ sont racines de $x^2 - Sx + P = x^2 - 20x - 8 = 0$.
   $\delta = 432$, puis $u^3 = 10 + \sqrt{108}$ et $v^3 = 10 - \sqrt{108}$.
   Et enfin, $x = \sqrt[3]{10 + \sqrt{108}} - \sqrt[3]{10 - \sqrt{108}}$.
   Autre méthode : $x^3 + 6x = 20$? Par essai : $x = 2$ fonctionne.

   $$x^3 + 6x - 20 = (x-2)(x^2 + 2x + 10) = (x-2)(x+1-3i)(x+1+3i)$$

   Puis, on exploite la formule de Cardan et enfin on reconnait une bicarré :

   $$x^4 + px^2 + 1 = (x^2 - \frac{-p+\sqrt{p^2-4}}{2})(x^2 - \frac{-p-\sqrt{p^2-4}}{2})$$
   $$= (x - \sqrt{\frac{-p+\sqrt{p^2-4}}{2}})(x + \sqrt{\frac{-p+\sqrt{p^2-4}}{2}})(x - \sqrt{\frac{-p-\sqrt{p^2-4}}{2}})(x + \sqrt{\frac{-p-\sqrt{p^2-4}}{2}})$$

4. Voir cours de terminale (ou de première)
5. C'est la méthode de la retro-action.
6. Par récurrence : $f^{(k)}(x) = \sum_{i=k}^{n} i(i-1)\dots(i-k) a_i x^{i-k} = k! a_k + \frac{(k+1)!}{1!} a_{k+1} x + \dots + \frac{n!}{(n-k)!} a_n x^{n-k}$.
   Et donc $f^{(k)}(0) = k! a_k$. Ainsi, $a_k = \frac{f^{(k)}(0)}{k!}$.

Chapitre 2

Calculs trigonométriques

Résumé -

Il s'agit, pour commencer, de revoir les propriétés des fonctions trigonométriques. Nous choisissons une présentation constructive, selon le sens de l'histoire et de la formation du lycéen. Nous nous appuyons sur les formules de base : $\cos(a+b) = \cos a\cos b - \sin a\sin b$ *et* $\sin(a+b) = \sin a\cos b + \cos a\sin b$ *pour développer toute la trigonométrie.*
Avec l'exponentielle complexe (chapitre 7), les formules seront revues plus efficacement.
Pour résoudre $f(x) = y$*, il faut pouvoir écrire* $x = f^{-1}(y)$*, i.e. trouver la fonction* f^{-1} *réciproque de* f*. On s'intéresse donc à la trigonométrie réciproque (*arcsin, arccos *et* arctan*)*
Vidéos :
- *Kitoumath. Les mathématiques fantastiques - Les formules de trigo à apprendre sans peine. https ://www.youtube.com/watch ?v=lKj1zQpToxA*
- *Micmath - La conjugaison complexe est un automorphisme de corps. https ://www.youtube.com/watch ?v=AVDMpnwsztg*
- *Les maths en finesse - Racines nieme de l'unité. https ://www.youtube.com/watch ?v=aZLGdnktO8k*

Sommaire

1. Problèmes 24
2. Fonctions trigonométriques 24
2.1. Construction historique 24
2.2. Fonctions sinus et cosinus 25
2.3. Fonction tangente 26
3. Formules trigonométriques 27
3.1. Formules de Regiomontanus 27
3.2. Produit en somme et réciproquement 29
3.3. Angle moitié 30
4. Trigonométrie réciproque 31
4.1. Arcsinus 31
4.2. Arccosinus 32
4.3. Arctangente 33
5. Bilan 34

1. Problèmes

Pour aller plus loin - Triangles semblables
On dit que deux triangles sont semblables si deux (et donc trois) angles sont de mêmes mesures

Problème 7 - Fonctions définies sur des angles nulles et droits. Et plus loin ?
Pour tout angle θ, les triangles rectangles dont l'un des angles vaut θ sont tous semblables.
Il y a donc un coefficient de proportionnel entre les mesures des côtés de ces triangles, qui dépend uniquement de θ. Prenons un triangle rectangle de référence d'hypothènuse égale à 1.
On note $\cos\theta$ la mesure du côté adjacent et $\sin\theta$ le côté opposé.
Que se passe-t-il si l'angle dépasse 90° ?

Problème 8 - Unité de mesure d'angles
Au début du lycée, on vous a fait changer l'unité de mesure des angles : des degrés à des radians ?
Pourquoi ? Qu'est-ce qu'on y gagne, pour chaque unité ?

Problème 9 - Relation entre les formules de trigonométrie
Quelles relations entre $\cos(a+b)$ et $\cos a$, $\cos b$. Et d'autres ?
De même peut-on linéariser $\cos(a)\sin(b)$ (c'est-à-dire, l'écrire sous forme d'une somme !).
Beaucoup de formules !
Une autre question, non négligeable : comment apprendre toutes ces formules ?

Histoire - Claude Ptolémé
Ptolémée (Ptolémaïs de Thébaïde (Haute-Égypte) vers 90 - Canope vers 168) est un astronome et astrologue grec qui vécut à Alexandrie (Égypte).



Il est connu pour ses apports en géographie et en mathématique (géométrie et trigonométrie).
Même s'il n'exploitait pas les fonctions cos *et* sin *mais plutôt la fonction corde (cord), il donna le premier élan (après Hipparque ?) à la trigonométrique que nous connaissons. Ces travaux ont été repris par les mathématiques indiennes (III à VI siècle) puis les mathématiques arabes (VIII à XIII siècle)*

Problème 10 - Equation polynomiale et trigonométrie
Montrer que pour tout entier n, et pour tout $\theta \in \mathbb{R}$,
$\cos(n\theta)$ s'exprimer comme une fonction polynomiale en $\cos\theta$.
Ce polynôme s'appelle le polynôme de Tchebychev d'ordre n.

Problème 11 - Fonction réciproque
Si souvent, nous aurons besoin d'inverser les relations $\sin\theta = x$ en $\theta = \sin^{-1}(x)$.
Mais, sin ou cos ne sont pas des fonctions bijectives. Comment faire ?

2. Fonctions trigonométriques

2.1. Construction historique

Analyse - Triangles rectangles semblables
D'après le théorème de Thalès, le rapport des longueurs de deux côtés similaires de deux triangles semblables est constant.
Dans l'ensemble des triangles rectangles, deux triangles sont semblables dès qu'ils ont chacun un angle de même mesure.
Ainsi les rapports de deux côtés consécutifs dans un triangle rectangle ne dépendent que de la mesure d'un angle (non droit).

Ce qui donne une première définition, *non encore totalement satisfaisante* :
Soit θ un angle compris entre 0 et 90 degrés.

Soit ABC un triangle rectangle en A et tel que $\widehat{ABC} = \theta$.

Alors le rapport $\frac{AB}{BC}$ est indépendant du triangle considéré, noté $\cos^\circ \theta$.

De même $\frac{AC}{BC}$ est indépendant du triangle considéré, noté $\sin^\circ \theta$.

Et $\frac{AC}{AB}$ est indépendant du triangle considéré, noté $\tan^\circ \theta$.

La notation choisie ici n'est pas standardisée, et est sûrement contradictoire avec celle vue en fin de collège. Elle permet de différencier de la vraie fonction cosinus (définie avec des angles en radians).

Analyse - Simplification : hypoténuse égale à 1

Pour éviter tout problème de division, on peut se concentrer sur les triangles rectangles dont l'hypothènuse a une longueur unité ($BC = 1$).
Ainsi, pour chaque angle θ compris entre 0 et 90 degrés, il existe un « unique » triangle rectangle en A, tel que $\widehat{BAC} = \theta$ et $BC = 1$. Dans ce cas $\cos^\circ \theta = AB$ et $\sin^\circ \theta = AC$.

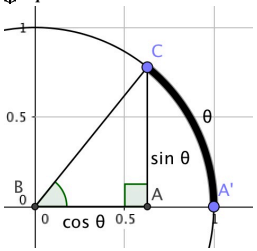
Analyse - Mesure naturelle d'angle

Les cultures (babyloniennes…) choisirent des mesures d'angles différentes. Toutes étaient proportionnelles les unes aux autres, une est-elle plus naturelle que les autres? Oui!
Après l'étape précédente, nous considérons des triangles rectangles d'hypothènuse de longueur 1. D'une certaine façon, tous ces triangles se trouvent dans le cercle de rayon 1 et centrée en B. L'angle en B est proportionnel à la longueur de la corde CA' (voir dessin).
Ainsi l'angle habituellement (jusqu'en seconde) noté 90ř a une longueur : quart de périmetre de cercle de rayon 1 i.e. $\frac{1}{4}(2\pi \times 1) = \frac{\pi}{2}$. On a la correspondance :

$$\theta^\circ = \frac{180}{\pi}\theta^r \iff \theta^r = \frac{\pi}{180}\theta^\circ$$

Le calcul devient simple : il suffit de mesurer une longueur (avec une corde qu'on superpose, puis qu'on détend).

Représentation - Radian



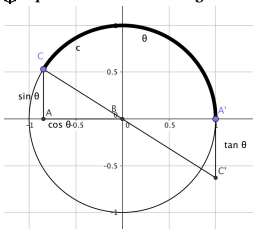
2.2. Fonctions sinus et cosinus

Représentation

D'après ce que l'on a vu, par construction, on retrouve $\cos\theta$ et $\sin\theta$ sur la figure comme indiqué en marge.
Par définition : $\tan\theta = \frac{\sin\theta}{\cos\theta} = \frac{\tan\theta}{1}$.
Donc, par théorème de Thalès, en plaçant la parallèle au sinus dans le triangle prolongé tel que $BA' = 1$, on retrouve le sinus en $A'C'$.

Reste une dernière étape : franchir les angles frontières de 0 et $\frac{\pi}{2}$ radians (ou 0° et 90°). Avec la dernière représentation, ce n'est pas compliqué : on continue la projection sur l'axe BA' et sur l'axe orthogonal.

Représentation - Cercle trigonométrique



Périodicité et symétrie

On a alors les résultats suivants, qu'il faut surtout savoir retrouver :
Exercice
Compléter les résultats suivants :

$\sin(-\theta) =$ $\cos(-\theta) =$ $\sin(\theta+\pi) =$ $\cos(\theta+\pi) =$

$\sin(\pi-\theta) =$ $\cos(\pi-\theta) =$ $\sin(\frac{\pi}{2}-\theta) =$ $\cos(\frac{\pi}{2}-\theta) =$

Correction

$\sin(-\theta) = -\sin(\theta)$ $\cos(-\theta) = \cos(\theta)$ $\sin(\theta+\pi) = -\sin(\theta)$ $\cos(\theta+\pi) = -\cos\theta$
$\sin(\pi-\theta) = \sin\theta$ $\cos(\pi-\theta) = -\cos\theta$ $\sin(\frac{\pi}{2}-\theta) = \cos\theta$ $\cos(\frac{\pi}{2}-\theta) = \sin\theta$

Avec la définition suivante :

Définition - Congruence modulo α
Soient θ, θ' et α trois réels.
On dit que θ est congru à θ' modulo α
s'il existe $k \in \mathbb{Z}$ tel que $\theta = \theta' + k\alpha$:

$$\theta \equiv \theta'[\alpha] \iff \exists k \in \mathbb{Z} | \theta = \theta' + k\alpha$$

on a la proposition :

Proposition - Propriétés des congruences
Soit $\alpha \in \mathbb{R}$. On a pour tout $(\theta, \theta', \theta'') \in \mathbb{R}^3$:
- $\theta \equiv \theta[\alpha]$ (reflexivité)
- $\theta \equiv \theta'[\alpha] \Rightarrow \theta' \equiv \theta[\alpha]$ (symétrie)
- $(\theta \equiv \theta'[\alpha]$ et $\theta' \equiv \theta''[\alpha]) \Rightarrow \theta \equiv \theta''[\alpha]$ (transitivité)

On dit que la relation de congruence modulo α est une relation d'équivalence.

Démonstration
Reflexivité : $\theta \equiv \theta[\alpha]$, il suffit de prendre $k = 0$.
Symétrie : Si $\theta \equiv \theta'[\alpha]$, alors il existe k tel que $\theta = \theta' + k\alpha$, donc $\theta' = \theta + (-k)\alpha$ et donc $\theta' \equiv \theta[\alpha]$.
Transitivité : Si $(\theta \equiv \theta'[\alpha]$ et $\theta' \equiv \theta''[\alpha]$
alors il existe k et k' tel que $\theta = \theta' + k\alpha$, $\theta' = \theta'' + k'\alpha$.
donc $\theta = \theta'' + k'\alpha + k\alpha = \theta'' + (k+k')\alpha$, donc $\theta \equiv \theta''[\alpha]$ □

A savoir parfaitement retrouver :

Savoir faire - Cas d'égalité de sinus ou de cosinus
Pour tout $(\theta, \theta') \in \mathbb{R}^2$ on a :

$$\sin\theta = \sin\theta' \iff$$

$$\cos\theta = \cos\theta' \iff$$

Démonstration
En exploitant les représentations graphiques, on se place par 2π-périodicité sur un intervalle simple.
Puis, on trouve : $\sin\theta = \sin\theta' \iff \begin{cases} \theta \equiv \theta' & [2\pi] \\ \theta \equiv \pi - \theta' & [2\pi] \end{cases}$
De même : $\cos\theta = \cos\theta' \iff \begin{cases} \theta \equiv \theta' & [2\pi] \\ \theta \equiv -\theta' & [2\pi] \end{cases}$ □

2.3. Fonction tangente

Définition - Tangente d'un angle
Soit $\theta \in \mathbb{R}$, $\theta \not\equiv \frac{\pi}{2}[\pi]$. On appelle *tangente* de θ le réel, noté $\tan\theta$, défini par :

$$\tan\theta = \frac{\sin\theta}{\cos\theta}$$

Remarque - fonction cotangente
On définit de même la fonction cotangente sur $\mathbb{R} \setminus \pi\mathbb{Z}$ par $\text{cotan}\theta = \frac{\cos\theta}{\sin\theta}$.
Sur le cercle trigonométrique, on la trouve sur la tangente au cercle au point $(0,1)$.
Si $\theta \not\equiv 0\left[\frac{\pi}{2}\right]$ on a $\text{cotan}\theta = \frac{1}{\tan\theta}$.

Proposition - (Im)parité et périodicité
Soit $\theta \in \mathbb{R}, \theta \neq \frac{\pi}{2}[\pi]$. On a

$$\tan(-\theta) = -\tan\theta \qquad \tan(\pi+\theta) = \tan\theta \qquad \tan(\pi-\theta) = -\tan\theta$$

Démonstration
On applique, directement la définition, par exemple : $\tan(\theta+\pi) = \frac{\sin(\theta+\pi)}{\cos(\theta+\pi)} = \frac{-\sin\theta}{-\cos\theta} = \tan\theta$ □

Exercice
Etudier et représenter la fonction tan

Correction
La fonction tan est définie sur $\mathscr{D} = \{x \in \mathbb{R} \mid \cos\theta \neq 0\} = \mathbb{R} \setminus \{\frac{\pi}{2} + k\pi; k \in \mathbb{Z}\}$.
La fonction tan est π-périodique d'après la formule trouvée plus haut.
On peut l'étudier sur $]-\frac{\pi}{2}, \frac{\pi}{2}[$, puis exploiter des translations de vecteurs $\pi\vec{i}$.
Par division de deux fonctions dérivables, tan est dérivable sur son ensemble de définition.

$$\forall\, x \in \mathscr{D}, \qquad \tan'(x) = \frac{\cos^2(x)+\sin^2(x)}{\cos^2(x)} = 1+\tan^2(x) = \frac{1}{\cos^2(x)}$$

La fonction tan est donc strictement croissante sur les intervalles de la forme $]\frac{-\pi}{2}, \frac{-\pi}{2}[$ et à valeurs dans $]-\infty, \infty[$.
$\tan(0) = 0$ et la pente de la tangente au point 0a pour pente : $\tan'(k\pi) = \frac{1}{\cos^(k\pi)} = 1$.
Enfin, comme $\frac{1}{\cos^2}$ est croissante sur $[0, \frac{\pi}{2}[$, tan est convexe sur $[0, \frac{\pi}{2}[$ et $\frac{1}{\cos^2}$ est décroissante sur $]-\frac{\pi}{2}, 0]$, tan est concave sur $]-\frac{\pi}{2}, 0]$.
On obtient la représentation graphique suivante :

Proposition - Cas d'égalité de tangentes
Pour tout $(\theta, \theta') \in \mathbb{R}^2$ on a :

$$\tan\theta = \tan\theta' \Leftrightarrow \theta \equiv \theta'[\pi]$$

3. Formules trigonométriques

Nous démontrons la plupart des relations avec des angles inférieurs à $\frac{\pi}{2}$, puis nous étendons les résultats par périodicité/symétrie.

3.1. Formules de Regiomontanus

Très important! A connaître par coeur, absolument! Il peut être bon d'avoir un moyen mnémotechnique auprès de soi…

Histoire - Trigonométrie : une vieille discipline
Ces formules apparaissent pour la première fois chez Ptolémée, 150 après J-C. On les retrouve chez Regiomontanus en 1464

Proposition - Formules fondamentales

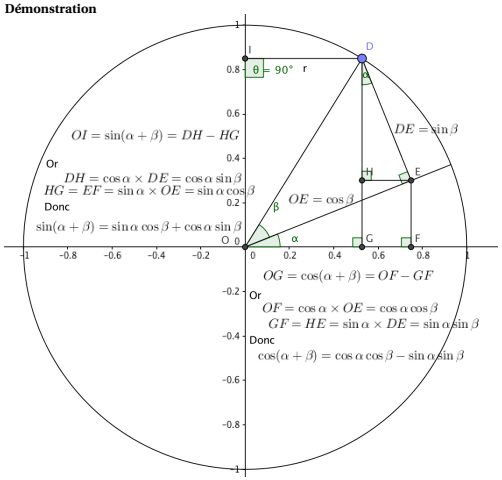
$$\cos^2\theta + \sin^2\theta = 1 \qquad 1+\tan^2\theta = \frac{1}{\cos^2\theta} \text{ où } \cos^2\theta = (\cos\theta)^2$$

$$\cos(a+b) = \cos a\cos b - \sin a\sin b \qquad \cos(a-b) = \cos a\cos b + \sin a\sin b$$
$$\sin(a+b) = \sin a\cos b + \sin b\cos a \qquad \sin(a-b) = \sin a\cos b - \sin b\cos a$$

Truc & Astuce pour le calcul - Exploiter les symétries du calcul
Une piste pour retrouver la formule $\cos(a+b)$.
Nous savons qu'il existe une relation, mais laquelle. Notons $\varphi(a,b) = \cos(a+b)$.
La relation doit vérifier :
— $\varphi(b,a) = \varphi(a,b)$, cela ne peut donc pas être $\varphi(a,b) = \sin a\cos b - \sin b\cos a$.

— $\varphi(-a,-b) = \varphi(a,b)$, cela ne peut donc pas être $\varphi(a,b) = \sin a\cos b + \sin b\cos a$.
— $\varphi(a,-a) = \cos(0) = 1$, cela ne peut donc pas être $\varphi(a,b) = \cos a\cos b + \sin a\sin b$, dans ce cas $\varphi(a,-a) = \cos^2 a - \sin^2 a \neq 1$ (pour la plupart des a)

Démonstration



La première formule dérive directement de la relation de Pythagore.
Avec $A(\cos\theta, \sin\theta)$, $M\cos\theta, 0)$ et $O(0,0)$, on a OMA est rectangle.
D'après le théorème de Pythagore : $OA^2 = OM^2 + MA^2$ ie $1 = \cos^2\theta + \sin^2\theta$.
Concernant les formules $\cos(a+b)\ldots$, on pourra trouver une démonstration plus efficace avec les notations exponentielle…
Pour obtenir $\cos(a-b)$, on remplace β par $-b$ et donc $\cos\beta = \cos b$ alors que $\sin\beta = -\sin b\ldots$ □

Exercice
On peut aussi exploiter les équations différentielles.
On note $f : x \mapsto \cos(a+x)$. Montrer que f est solution du problème de Cauchy :

$$\begin{cases} y''+y &= 0 \\ y(0) &= \cos a \\ y'(0) &= -\sin(a) \end{cases}.$$

En déduire une expression de f.

Correction
Il suffit de faire le calcul. La solution du problème de Cauchy est unique, c'est une combinaison linéaire de cos et sin.
Donc il existe A et B tel que $\cos(a+x) = A\cos x + B\sin x$.
Puis avec les valeurs en $x = 0$, de f et f', on a $A = \cos a$ et $B = -\sin a$
De cet exercice, on déduit un nouveau moyen mnemotechnique pour retenir les formules de Regiomontanus.

Truc & Astuce pour le calcul - Combinaison linéaire en $\cos x$ et $\sin x$
$x \mapsto \cos(a+x)$ est une fonction, combinaison linéaire de $\cos x$ et $\sin x$.
Il existe A, B **indépendant de** x tel que $\cos(a+x) = A\cos x + B\sin x$.
En particulier pour $x = 0$ et $x = \frac{\pi}{2}$: $\cos a = A \times 1 + B \times 0$ et $\cos(a+\frac{\pi}{2}) = -\sin a = A \times 0 + B \times 1$.
Donc pour tout $a, x \in \mathbb{R}$: $\cos(a+x) = \cos a\cos x - \sin a\sin x$.
$x \mapsto \sin(a+x)$ est une fonction, combinaison linéaire de $\cos x$ et $\sin x$.
Il existe C, D **indépendant de** x tel que $\sin(a+x) = C\cos x + D\sin x$.
En particulier pour $x = 0$ et $x = \frac{\pi}{2}$: $\sin a = C \times 1 + D \times 0$ et $\sin(a+\frac{\pi}{2}) =$

$+\cos a = C\times 0 + D\times 1$.

Donc pour tout $a, x \in \mathbb{R}$: $\sin(a+x) = \sin a\cos x + \cos a \sin x$.

Savoir les déduire ou les retrouver.

Proposition - Formules fondamentales (bis)

$$\tan(a+b) = \frac{\tan a + \tan b}{1-\tan a\tan b} \qquad \tan(a-b) = \frac{\tan a - \tan b}{1+\tan a\tan b}$$

$$\sin 2a = 2\sin a\cos a \qquad \cos 2a = \cos^2 a - \sin^2 a = 2\cos^2 a - 1 = 1 - 2\sin^2 a$$

$$\tan 2a = \frac{2\tan a}{1-\tan^2 a}$$

$$\cos^2 a = \frac{1+\cos 2a}{2} \qquad \sin^2 a = \frac{1-\cos 2a}{2}$$

Exercice

Démontrer ces formules

Correction

Quelques unes :

$$\tan(a-b) = \frac{\sin(a-b)}{\cos(a-b)} = \frac{\sin a\cos b - \cos a\sin b}{\cos a\cos b + \sin a\sin b} = \frac{\frac{\sin a\cos b - \cos a\sin b}{\cos a\cos b}}{\frac{\cos a\cos b + \sin a\sin b}{\cos a\cos b}} = \frac{\tan a - \tan b}{1+\tan a\tan b}$$

$\cos(2a) = \cos(a+a) = \cos^2 a - \sin^2 a = \cos^2 a - (1-\cos^2 a) = 2\cos^2 a - 1 = (1-\sin^2 a) - \sin^2 a = 1 - 2\sin^2 a \ldots$

3.2. Produit en somme et réciproquement

Savoir les déduire ou les retrouver.

Proposition - Transformation de produit en somme

$$\cos a\cos b = \frac{1}{2}\big(\cos(a+b) + \cos(a-b)\big)$$

$$\sin a\sin b = \frac{1}{2}\big(\cos(a-b) - \cos(a+b)\big)$$

$$\sin a\cos b = \frac{1}{2}\big(\sin(a+b) + \sin(a-b)\big)$$

Exercice

Comment exploiter les symétries du calcul pour « deviner » les égalités

Correction

On note (par exemple) $\varphi(a,b) = \sin a\sin b$. Donc $\varphi(-a,-b) = \varphi(a,b)$, la formule contient des cos (fonctions paires).

$\varphi(a,0) = 0$, donc il y a une soustraction de $\cos(a+b) = \cos a$ et $\cos(a-b) = \cos a$. $\varphi(a,a) = \sin^2 a = \frac{1}{2}(1-\cos 2a)$ ce qui donne la première formule...

Exercice

Démontrer ces formules

Correction

La démonstration se fait à l'envers. Il faut donc bien intuiter d'où partir....

Par exemple, pour obtenir $\sin a\sin b$, on se souvient que cela s'obtient avec $\cos(a+b)$.

Donc on note : $\cos(a+b) = \cos a\cos b - \sin a\sin b$ et $\cos(a-b) = \cos a\cos b + \sin a\sin b$.

Il faut supprimer les $\cos a\cos b$, on retranche donc :

$$\cos(a+b) - \cos(a-b) = -\sin a\sin b - \sin a\sin b \Longrightarrow \sin a\sin b = \frac{1}{2}(\cos(a-b) - \cos(a+b))$$

Exercice

Comment exploiter les symétries du calcul pour « deviner » les égalités

Correction

Remarque - Notation exponentielle

Avec les notations exponentielles, le résultats sera plus immédiat (on pourra le trouver dans le sens direct).

Pour aller plus loin - Trisection de l'angle

Un problème antique consistait à trouver comment couper un angle en trois parts égales.
La réponse de Viète (1593 - incomplète car elle ne donne pas de construction), consiste à remarquer que $\sin(3\alpha) = 3\sin\alpha - 4\sin^3\alpha$.
Si on connait 3α *et donc* $\sin 3\alpha = S$. *Il s'agit de résoudre :* $4x^3 - 3x + S = 0$.
Or la formule d'Al-Khwarismi donne pour solution à cette équation :

$$x = \sqrt[3]{-\frac{S}{8} + \sqrt{-\frac{S^2}{64} - \frac{1}{4}}} + \sqrt[3]{-\frac{S}{8} - \sqrt{-\frac{S^2}{64} - \frac{1}{4}}}$$

Proposition - Transformation de somme en produit

$$\cos p + \cos q = 2\cos\big(\tfrac{p+q}{2}\big)\cos\big(\tfrac{p-q}{2}\big)$$

$$\cos p - \cos q = -2\sin\big(\tfrac{p+q}{2}\big)\sin\big(\tfrac{p-q}{2}\big)$$

$$\sin p + \sin q = 2\sin\big(\tfrac{p+q}{2}\big)\cos\big(\tfrac{p-q}{2}\big)$$

$$\sin p - \sin q = 2\cos\big(\tfrac{p+q}{2}\big)\sin\big(\tfrac{p-q}{2}\big)$$

Exercice

Démontrer ces formules

Correction

Par exemple :

$$\cos p - \cos q = \cos(\tfrac{p+q}{2} + \tfrac{p-q}{2}) - \cos(\tfrac{p+q}{2} - \tfrac{p-q}{2})$$
$$= \cos(\tfrac{p+q}{2})\cos(\tfrac{p-q}{2}) - \sin(\tfrac{p+q}{2})\sin(\tfrac{p-q}{2}) - \cos(\tfrac{p+q}{2})\cos(\tfrac{p-q}{2}) - \sin(\tfrac{p+q}{2})\sin(\tfrac{p-q}{2})$$
$$= -2\sin(\tfrac{p+q}{2})\sin(\tfrac{p-q}{2})$$

Attention - Remarque

Il n'y a pas de formule générale pour transformer $\cos p \pm \sin q$.
Sauf à exploiter $\sin q = \cos(\frac{\pi}{2} - q)\ldots$

Exemple - Calcul de $\sum_{k=0}^{n} \cos kt$

Soit $t \in]0,\pi]$. On pose $S_n = \sum_{k=0}^{n} \cos kt$.

Calculer $2(\sin\frac{t}{2})S_n$ puis déduire S_n (que l'on exprimera comme produit ou quotient de trois termes sinus ou cosinus).

$$2(\sin\tfrac{t}{2})S_n = 2\sum_{k=0}^{n}\sin\tfrac{t}{2}\cos(kt) = \sum_{k=0}^{n}\Big(\sin(\tfrac{2k+1}{2}t) + \sin(\tfrac{-2k+1}{2}t)\Big) = \sum_{k=0}^{n}\Big(\sin(\tfrac{2k+1}{2}t) - \sin(\tfrac{2k-1}{2}t)\Big)$$

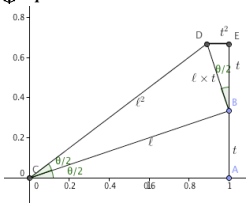
Puis par télescopage :

$$2(\sin\tfrac{t}{2})S_n = \sin(\tfrac{2n+1}{2}t) - \sin(-\tfrac{1}{2}t) = \sin(\tfrac{2n+1}{2}t) + \sin(\tfrac{1}{2}t) = 2\sin(\tfrac{2n+2}{4}t)\cos(\tfrac{2n}{4}t) = 2\sin(\tfrac{n+1}{2}t)\cos(\tfrac{n}{2}t)$$

Ainsi

$$S_n = \frac{\cos\frac{n}{2}t\sin\frac{n+1}{2}t}{\sin\frac{1}{2}t}$$

Représentation - Formules d'addition



3.3. Angle moitié

Proposition - Utilisation de la tangente de l'angle moitié

On note $t = \tan\dfrac{\theta}{2}$. Alors :

$$\sin\theta = \frac{2t}{1+t^2} \qquad \cos\theta = \frac{1-t^2}{1+t^2} \qquad \tan\theta = \frac{2t}{1-t^2}$$

Remarque - Calcul intégral

Ces résultats servent souvent dans le calcul d'intégrale avec des fonctions trigonométriques

Démonstration

Un graphique nous aide là aussi. Mais on peut directement, faire le calcul après avoir rappeler : $1+t^2 = 1+\tan^2\frac{\theta}{2} = \dfrac{1}{\cos^2\frac{\theta}{2}}$:

$$\sin\theta = \sin(2\tfrac{\theta}{2}) = 2\sin\tfrac{\theta}{2}\cos\tfrac{\theta}{2} = 2\tan\tfrac{\theta}{2}\cos^2\tfrac{\theta}{2} = \frac{2t}{1+t^2}$$

$$\cos\theta = \cos(2\tfrac{\theta}{2}) = 2\cos^2\tfrac{\theta}{2} - 1 = \frac{2}{1+t^2} - 1 = \frac{1-t^2}{1+t^2}$$

□

Remarque - Trucs pour ne pas écrire de bêtises…
On peut vérifier que si $\theta = 0$: $t = 0$, $\sin\theta = 0$,
mais aussi $\cos\theta = 1$ et $\sin^2 + \cos^2 = 1$,
ou encore, si $\theta = \frac{\pi}{2}$, $t = 1$ et $\tan\theta = \infty$…, donc le dénominateur de tan s'annule en 1 et −1.
ou toujours, tan = $\frac{\sin}{\cos}$…

Exercice
Exemple d'emploi des notations exponentielles.
Notons α l'argument du complexe $z = 1 + it$.
Calculer z^2, quel est l'argument du complexe z^2 ? En déduire les relations recherchées ?
Sauriez-vous en déduire l'expression de $\cos\theta$ en fonction de $r = \tan\frac{\theta}{2}$?

Correction
$z^2 = (1-t^2) + 2it$, c'est le complexe de module $\sqrt{(1-t^2)^2 + 4t^2} = \sqrt{1+2t^2+t^4} = (1+t^2)$ et d'argument 2α.
Donc $\cos(2\alpha) = \frac{\mathrm{Re}(z^2)}{1+t^2} = \frac{1-t^2}{1+t^2}$ et $\sin(2\alpha) = \frac{\mathrm{Im}(z^2)}{1+t^2} = \frac{2t}{1+t^2}$.
De même $z^3 = [1-3t^2] + i[3t-t^3]$, de module $\sqrt{(1-3t^2)^2 + (3t-t^3)^2} = \sqrt{1+3t^2+3t^4+t^6} = (1+t^2)^{3/2}$ et d'argument 3α.
Donc $\cos(3\alpha) = \frac{1-3t^2}{(1+t^2)^{3/2}}$ et $\sin(3\alpha) = \frac{3t-t^3}{(1+t^2)^{3/2}}$…

Savoir faire - Méthode pour transformer $a\cos t + b\sin t$ en $A\cos(t-\phi)$
On écrit

$$a\cos t + b\sin t = \sqrt{a^2+b^2}\Big(\frac{a}{\sqrt{a^2+b^2}}\cos t + \frac{b}{\sqrt{a^2+b^2}}\sin t\Big)$$

Comme $\left(\frac{a}{\sqrt{a^2+b^2}}\right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 = 1$, il existe $\phi \in \mathbb{R}$ tel que

$$\cos\phi = \frac{a}{\sqrt{a^2+b^2}} \text{ et } \sin\phi = \frac{b}{\sqrt{a^2+b^2}}$$

d'où en posant $A = \sqrt{a^2+b^2}$, on a

$$a\cos t + b\sin t = A\Big(\cos\phi\cos t + \sin\phi\sin t\Big) = A\cos(t-\phi).$$

La fonction $s : t \mapsto a\cos t + b\sin t$ représente donc un signal sinusoïdal d'amplitude A de phase initiale $-\phi$(instant $t = 0$) .

Exercice
Factoriser $\sin\theta + \cos\theta$, $\sqrt{3}\cos x - \sin x$.

Correction
$\sin\theta + \cos\theta = \sqrt{2}\big(\sin\theta\sin\frac{\pi}{4} + \sin\theta\cos\frac{\pi}{4}\big) = \sqrt{2}\cos(\theta - \frac{\pi}{4})$.
Comme $\sqrt{3}^2 + 1 = 4 = 2^2$, on a,

$$\sqrt{3}\cos x - \sin x = 2\Big(\sqrt{3}2\cos x - \frac{1}{2}\sin x\Big) = 2\Big(\cos\frac{-\pi}{6}\cos x + \sin\frac{-\pi}{6}\sin x\Big) = 2\cos(x+\frac{\pi}{6})$$

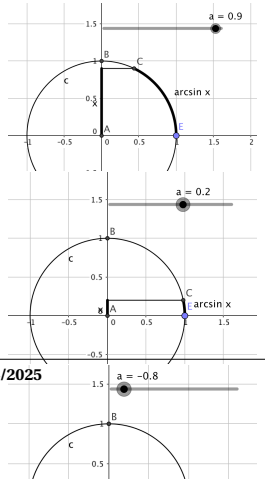
4. Trigonométrie réciproque

4.1. Arcsinus

Définition - Arcsinus
Pour tout $x \in [-1,1]$ il existe un unique $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ vérifiant $x = \sin\theta$. Ce réel θ est appelé arcsinus de x et noté $\arcsin x$ On a donc :

$$\theta = \arcsin x \Leftrightarrow \Big(\sin\theta = x \text{ et } \theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]\Big)$$

Représentation - Quelques valeurs de $\arcsin x$



Attention - Intervalle d'arrivée
De même qu'il a été choisi de prendre l'unique racine positive de a, lorsqu'on écrit $\sqrt{a}$ (et non $-\sqrt{a}$ qui vérifie également $(-\sqrt{a})^2 = a$) ; on choisit ici un résultat dans $[-\frac{\pi}{2}, \frac{\pi}{2}]$, il faut donc penser à ajouter un angle…

$$\sin\theta = x \Longleftrightarrow \theta \equiv \arcsin(x)[2\pi] \text{ ou } \theta \equiv \pi - \arcsin(x)[2\pi]$$

Il faut connaître les valeurs remarquables suivantes :

x	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1
$\arcsin x$					

Exercice
Calculer $\arcsin(\sin\frac{2\pi}{3})$, $\arcsin(\sin\frac{23\pi}{6})$.

Correction
Où est le piège ? dans l'intervalle d'arrivée.
Comme $\frac{2\pi}{3} > \frac{\pi}{2}$, $\arcsin(\sin\frac{2\pi}{3}) = \pi - \frac{2\pi}{3} = \frac{\pi}{3}$. De même $\frac{23\pi}{6} = 4\pi - \frac{\pi}{6}$, $\arcsin(\sin\frac{23\pi}{6}) = -\frac{\pi}{6}$

Histoire - Série arcsin
On trouve chez Wallis *et les mathématiciens anglais pré-newtonien :*
$\arcsin(x) = x + \frac{1}{2}\frac{x^3}{3} + \frac{1\times3}{2\times4}\frac{x^5}{5} + \frac{1\times3\times5}{2\times4\times6}\frac{x^7}{7} + \dots$

Proposition - Composition de fonctions trigonométriques et arcsin
On a :

$$\forall\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}], \quad \arcsin(\sin\theta) = \theta$$

$$\forall x \in [-1,1], \quad \sin(\arcsin x) = x$$

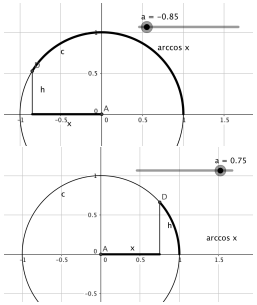
$$\forall x \in [-1,1], \quad \cos(\arcsin x) = \sqrt{1-x^2}$$

Démonstration
Les deux premiers résultats s'obtiennent en appliquant tout simplement la définition.
Comme $\cos^2 = 1 - \sin^2$, on a donc pour $x \in [-1,1]$,

$$\cos^2(\arcsin(x)) = 1 - \sin^2(\arcsin(x)) = 1 - x^2$$

donc $\cos(\arcsin(x)) = \pm\sqrt{1-x^2}$.
Or $\arcsin(x) \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, donc $\cos(\arcsin(x)) \geqslant 0$ et donc $\cos(\arcsin(x)) = +\sqrt{1-x^2}$ □

Représentation - Quelques valeurs de $\arccos x$



4.2. Arccosinus

Définition - Arccosinus
Pour tout $x \in [-1,1]$ il existe un unique $\theta \in [0,\pi]$ vérifiant $x = \cos\theta$. Ce réel θ est appelé arccosinus de x et noté $\arccos x$ On a donc :

$$\theta = \arccos x \Leftrightarrow \Big(\cos\theta = x \text{ et } \theta \in [0,\pi]\Big)$$

Attention - Intervalle d'arrivée
Comme précédemment :

$$\cos\theta = x \Longleftrightarrow \theta \equiv \arccos(x)[2\pi] \text{ ou } \theta \equiv -\arccos(x)[2\pi]$$

Il faut connaître les valeurs remarquables suivantes :

x	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1
$\arccos x$					

Exercice
Calculer $\arccos(\cos\frac{4\pi}{3}), \arccos(\cos\frac{25\pi}{6})$.

Correction
Comme $\frac{4\pi}{3} \in]\pi, 2\pi[$, $\arccos(\cos\frac{2\pi}{3}) = -\frac{4\pi}{3} + 2\pi = \frac{2\pi}{3}$. De même $\frac{25\pi}{6} = 4\pi + \frac{\pi}{6}$, $\arccos(\cos\frac{25\pi}{6}) = \frac{\pi}{6}$

Proposition - Composition de fonctions trigonométriques et arccos
On a :
$$\forall \theta \in [0,\pi], \quad \arccos(\cos\theta) = \theta$$
$$\forall x \in [-1,1], \quad \cos(\arccos x) = x$$
$$\forall x \in [-1,1], \quad \sin(\arccos x) = \sqrt{1-x^2}$$

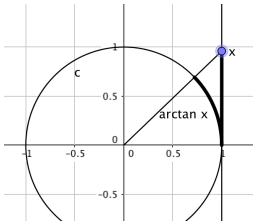
Exercice
Faire la démonstration

Correction
Comme $\sin^2 = 1 - \cos^2$, on a donc pour $x \in [-1,1]$,
$$\sin^2(\arccos(x)) = 1 - \cos^2(\arccos(x)) = 1 - x^2$$
donc $\sin(\arccos(x)) = \pm\sqrt{1-x^2}$.
Or $\arccos(x) \in [0,\pi]$, donc $\sin(\arccos(x)) \geqslant 0$ et donc $\sin(\arccos(x)) = +\sqrt{1-x^2}$

4.3. Arctangente

Définition - Arctangente
Pour tout $x \in \mathbb{R}$ il existe un unique $\theta \in]-\frac{\pi}{2}, \frac{\pi}{2}[$ vérifiant $x = \tan\theta$. Ce réel θ est appelé arctangente de x et noté $\arctan x$ On a donc :
$$\theta = \arctan x \Leftrightarrow \left(\tan\theta = x \text{ et } \theta \in]-\frac{\pi}{2}, \frac{\pi}{2}[\right)$$

Représentation - Quelques valeurs de $\arctan x$



Il faut connaître les valeurs remarquables suivantes :

x	0	$\frac{1}{\sqrt{3}}$	1	$\sqrt{3}$
$\arctan x$				

Proposition - Composition de fonctions trigonométriques et arctan
On a :
$$\forall \theta \in]-\frac{\pi}{2}, \frac{\pi}{2}[, \quad \arctan(\tan\theta) = \theta$$
$$\forall x \in \mathbb{R}, \quad \tan(\arctan x) = x$$
$$\forall x \in \mathbb{R}, \quad \cos(\arctan x) = \frac{1}{\sqrt{1+x^2}}$$
$$\forall x \in \mathbb{R}, \quad \sin(\arctan x) = \frac{x}{\sqrt{1+x^2}}$$

Histoire - Série arctan
On trouve chez GREGORY *et les mathématiciens anglais pré-newtonien :*
$\arcsin(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots$.
Puis, avec, une formule d'approximation de π *:*
$\pi = 16\arctan\frac{1}{5} - 4\arctan\frac{1}{239}$.

Démonstration
On exploite $\cos^2 = \frac{1}{1+\tan^2}$, puis la positivité.
Et $\sin^2 = 1 - \cos^2 = 1 - \frac{1}{1+\tan^2} = \frac{\tan^2}{1+\tan^2} \ldots$ □

Proposition - Relation complexe
Soit $x \in \mathbb{R}$, alors $\arg(1+ix) = \arctan(x)$

Pour aller plus loin - Formule d'approximation de π ***: Formule de Machin (1706)***
$4\arctan\frac{1}{5} - \arctan\frac{1}{239} = \cdots = \arg\left((1+\frac{i}{5})^4(1-\frac{i}{239})\right) = \arg(\frac{114244}{149375}(1+i)) = \frac{\pi}{4}$.
Comme $\arctan(x) \approx x + \frac{1}{6}x^3 + \frac{3}{8}x^5 + \ldots$, *on trouve une excellente approximation de* π.
Cette formule donna la meilleure approximation de π *connue durant tout le XVIII ème siècle.*

Démonstration
Soit $z = 1 + ix$, note $\rho = \sqrt{1+x^2}$ son module et θ sont argument.
$$z = 1 + ix = \rho(\cos\theta + i\sin\theta)$$
Donc a donc $\tan\theta = \frac{\sin\theta}{\cos\theta} = \frac{\rho\sin\theta}{\rho\cos\theta} = \frac{x}{1} = x$.
Ainsi $\arctan x = \theta = \arg(1+ix)$. □

Remarque - Aspect analytique
On étudiera dans un prochain chapitre les aspects analytiques de ces fonctions (dérivées, développement limités...)

5. Bilan

Synthèse

- En géométrie (et physique), nous pratiquons la projection orthogonale, cela consiste à multiplier par $\cos\theta$ (ou $\sin\theta$) la longueur de l'hypoténuse. Différents calculs se présentent à nous : $\cos(a+b)$, $\cos(a)\cos(b)$ ou $\cos a + \cos b$ (et tout ce que l'on peut imaginer de manière équivalente avec sin ou tan). Il existe alors de nombreuses relations calculatoires **à apprendre**!
- Très souvent la question se pose de manière réciproque : étant donné une longueur de quel angle en est-elle le cos? Le problème, la fonction n'est pas injective : on peut avoir $\theta \neq \theta'$ et $\cos\theta = \cos\theta'$. On restreint donc l'intervalle image. On crée ainsi une fonction réciproque arccos à la fonction $\cos_{|[0,\pi]} : [0,\pi] \to [-1,1]$. De même pour les fonctions $\sin_{|[-\frac{\pi}{2},\frac{\pi}{2}]}$ et $\tan_{[-\frac{\pi}{2},\frac{\pi}{2}]}$. Au passage, on trouve une méthode complémentaire (algébrique) dans le simple cas de la racine carrée d'un nombre complexe.

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Cas d'égalité de sinus ou de cosinus
- Truc & Astuce pour le calcul - Exploiter les symétries du calcul
- Truc & Astuce pour le calcul - Combinaison linéaire en $\cos x$ et $\sin x$
- Savoir-faire - Méthode pour transformer $a\cos t + b\sin t$ en $A\cos(t-\varphi)$

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
cos, sin, tan	Fonctions cosinus, sinus et tangentes.	Dans un triangle ABC rectangle en A, $\cos B = \frac{AB}{BC}$, $\sin B = \frac{AC}{BC}$ et $\tan B = \frac{AC}{AB} = \frac{\cos B}{\sin B}$	Tout un chapitre à connaître!
arccos, arcsin, arctan	Fonctions réciproques de $\cos_{|[0,\pi]}^{|[-1,1]}$, $\sin_{|[-\pi/2,\pi/2]}^{|[-1,1]}$, $\tan_{|]-\pi/2,\pi/2[}^{|[-1,1]}$ respectivement.	$\cos(\arccos(x)) = x$ pour tout $x \in [-1,1]$	A savoir maîtriser

Retour sur les problèmes

7. Voir le cours
8. Les formules d'additions de cos et sin restent vraies si les angles sont en degré.
   Pourquoi changer d'unité au lycée?

L'inégalité $\sin x \leqslant x \leqslant \tan x$ est vraie pour x en radian. Pour x en degré, on aurait plutôt : $\sin x \leqslant \frac{\pi}{180} x \leqslant \tan x$.

On trouve alors, en radian : $\cos x \leqslant \dfrac{\sin x}{x} \leqslant 1$ en faisant $x \to 0$: on trouve $\sin'(x) = 1$, puis avec les formules d'addition : $\sin' = -\cos$.
Si les angles sont en degré : il faut un coefficient multiplicatif. C'est donc une relation pénible.
Bilan : si on passe en radian, c'est parce qu'on s'intéresse à propriétés analytiques des fonctions trigonométriques…

9. A apprendre. Mais l'apprendre, c'est toujours plus compliqué.
10. $\cos(n\theta) = \mathrm{Re}((e^{i\theta})^n) = \mathrm{Re}((\cos\theta + i\sin\theta)^n) = \displaystyle\sum_{0\leqslant k\leqslant \frac{n}{2}} \binom{n}{2k} (-1)^k \cos^{n-2k}\theta (1-\cos^2\theta)^k = T_n(\cos\theta)$
11. arcsin et arccos…

Chapitre 3

Fonctions *à la Euler*

Résumé -

Dans ce chapitre, on s'intéresse aux principales fonctions usuelles des mathématiques pré-eulerien (donc, jusqu'à la fonction Γ, exclue).
Nous reprenons les constructions historiques qui conduisent à ces fonctions, en espérant qu'ainsi, les propriétés caractéristiques de chacune seront mieux mémorisées.
Pour préparer le cours sur la dérivation des fonctions usuelles, nous donnerons une série d'inégalités localisées suffisantes pour calculer les dérivées.
Enfin, nous terminons ce chapitre en donnant une liste d'évaluations numériques des fonctions usuelles sous forme de somme infinies (convergentes). Nous en reparlerons (beaucoup) plus tard.

— *Kahn Académy - Qu'est-ce qu'une fonction exponentielle ?. https ://www.youtube.com/watch ?v=pBeGfLoId4I*
— *Micmath - Merveilleux logarithmes. https ://www.youtube.com/watch ?v=rWfl7Pw8YVE*

Sommaire

1. Problèmes 38
2. Généralités sur les fonctions 38
2.1. Définition et représentation d'une fonction 38
2.2. Opérations sur les fonctions 39
2.3. Vocabulaire d'analyse de fonctions 40
2.4. Bijections et réciproques 42
2.5. Etude des branches infinies en ∞ 43
3. Fonctions trigonométriques 45
3.1. Fonctions circulaires 45
3.2. Fonctions circulaires réciproques 46
4. Fonctions polynomiales et puissances rationnelles 48
4.1. Fonction puissance entière relative 48
4.2. Fonctions polynomiales 50
4.3. Fonction puissance rationnelle 51
5. Exponentielles et logarithmes 52
5.1. ExponentielleS 52
5.2. LA fonction exponentielle 54
5.3. LogarithmeS 56
5.4. Retour sur les fonctions puissances, avec un exposant non rationnel 57
5.5. Croissances comparées 58
5.6. Fonctions hyperboliques directes 58
6. Sommes numériques infinies 59
7. Bilan 60

1. Problèmes

Histoire - Evolution de la notion de fonction
Pour Leibniz puis Euler, qui a été le premier à utiliser le mot de « fonction » et pour les mathématiciens du XVIII-ième siècle, l'idée de relation fonctionnelle était plus ou moins assimilée à l'existence d'une formule mathématique simple exprimant la nature exacte de cette relation. Cette conception s'est révélée trop étroite pour les exigences de la physique mathématique, et l'idée de fonction, ainsi que la notion de limite qui lui est associée, ont subi un long processus de clarification et de généralisation.
Par exemple : $x \mapsto \begin{cases} 1 & si\ x \leqslant 1 \\ x^2 & si\ x > 1 \end{cases}$ *n'est pas une fonction pour Euler; mais pour nous (et vous?) c'est bien une fonction!*

Problème 12 - Comment calculer π^e ?
Pour l'étude des fonctions usuelles, il est très important pour chacun d'être en mesure de savoir comment faire le calcul des valeurs, sans raccourci avec la calculatrice.
Il faudra néanmoins faire ces calculs pour les nombres rationnels (et pour les nombres réels, on verra plus loin...).
Les nombres π et e sont des nombres réels bien définis.
Comment faire ce calcul? Les nombres réels sont approchés par des nombres rationnels.
On va donc commencer par essayer de calculer $\left(\frac{22}{7}\right)^{\frac{8}{3}}$, puis de manière générale de r^z où $r, z \in \mathbb{Q}$.
Deux temps d'analyse :

1. On fixe $z \in \mathbb{Q}$ et on étudie $t \mapsto t^z$, pour $t \in \mathbb{R}$. Ce sont les fonctions puissances.
2. On fixe $r \in \mathbb{Q}$ puis $r \in \mathbb{R}$ et on étudie $t \mapsto r^t$, pour $t \in \mathbb{R}$. Ce sont les fonctions exponentielles.

Problème 13 - Interpolation de la suite géométrique
Existe-t-il une fonction simple (polynomiale) qui interpole la suite géométrique de raison $r (= 2$ par exemple)?
Comment l'étudier?

Problème 14 - De la multiplication à l'addition
Additionner deux nombres de tailles n se fait en gros en $2n$ calculs. Pour les multiplier l'algorithme classique nécessite n^2 multiplications de chiffres, puis une addition de n nombres...
Peut-on trouver un moyen simple qui transmute les multiplications en additions? Une fonction telle que : $f(a \times b) = f(a) + f(b)$?

2. Généralités sur les fonctions

2.1. Définition et représentation d'une fonction

Définition - Fonction
Une *fonction* d'une variable réelle, à valeurs réelles, est un "procédé" qui à chaque élément x d'un sous-ensemble $\mathscr{D}$ de $\mathbb{R}$ associe un réel $f(x)$ parfaitement déterminé. Une telle fonction est notée

$$\begin{array}{rcl} f : & \mathscr{D} & \to \mathbb{R} \\ & x & \mapsto f(x) \end{array}$$

$f(x)$ est appelé *image* de x par f.
Si $y \in \mathbb{R}$, tout élément x de $\mathscr{D}$ vérifiant $f(x) = y$ est appelé un *antécédent* de y.

Remarque - Ensemble de définition
Le fait d'écrire $f : \mathscr{D} \to \mathbb{R}$ sous-entend que $f(x)$ est parfaitement défini si $x \in \mathscr{D}$.
Il est toutefois fréquent en pratique que l'ensemble $\mathscr{D}$ ne soit pas connu a priori. A partir de l'expression de $f(x)$, il faut déterminer l'ensemble des réels x pour lesquels elle a un sens. Cet ensemble est appelé *domaine de définition* de f (généralement noté $\mathscr{D}_f$). Il est souvent constitué d'une réunion d'intervalles.

Définition - Graphe d'une fonction
$\mathscr{C} = \{(x, f(x)); x \in \mathscr{D}_f\}$ s'appelle le *graphe* de f, le plan étant muni d'un repère $(O, \vec{i}, \vec{j})$, on appelle *représentation graphique* ou *courbe représentative de* f la représentation de cet ensemble dans le plan. La courbe représentative a pour équation $y = f(x)$.

Définition - Image de $\mathscr{D}$ par une fonction. Fonction restreinte
Si $\mathscr{D}' \subset \mathscr{D}_f$ ($\mathscr{D}'$ sous ensemble de $\mathscr{D}_f$), on note $f(\mathscr{D}')$ l'ensemble des images des éléments de $\mathscr{D}'$: $f(\mathscr{D}') = \{f(x); x \in \mathscr{D}'\}$. $f(\mathscr{D}')$ s'appelle *l'ensemble image (ou image directe)* de $\mathscr{D}'$ par f.
Soit $f : \mathscr{D}_f \to \mathbb{R}$ une fonction et I un intervalle inclus dans $\mathscr{D}_f$. On appelle *restriction* de f à I la fonction g définie sur I par : $\forall x \in I, g(x) = f(x)$. On la note $f_{|I}$.

Définition - Ensemble des applications
Soit I un intervalle de $\mathbb{R}$, non vide et non réduit à un point.
On note $\mathscr{F}(I, \mathbb{R})$ l'ensemble des fonctions définies sur I à valeurs dans $\mathbb{R}$ (on parle aussi d'applications de I dans $\mathbb{R}$)

Savoir faire - Transformation sur le graphe
Soient $f : \mathscr{D}_f \to \mathbb{R}$ et $a \in \mathbb{R}$.
Comment obtient-on les domaines de définition ainsi que les graphes (ou représentations graphiques) des fonctions $x \mapsto f(x) + a$, $x \mapsto f(x+a)$, $x \mapsto f(a-x)$, $x \mapsto af(x)$?
$x \mapsto f(x) + a : \mathscr{D}_1 = \mathscr{D}$ et translation de $a\vec{j}$,
$x \mapsto f(x+a) : \mathscr{D}_2 = \{x \mid x + a \in \mathscr{D}\} = \mathscr{D} - a$ et translation de $-a\vec{i}$,
$x \mapsto f(a-x) : \mathscr{D}_3 = \{x \mid a - x \in \mathscr{D}\}$ (ex : si $\mathscr{D} = [c, d[$, alors $\mathscr{D}_3 =]a-d, a-c]$) et reflexion (symétrie) d'axe d'équation $x = \frac{a}{2}$ $x \mapsto af(x)$: $\mathscr{D}_4 = \mathscr{D}$ et homothétie-axiale de rapport a et de « centre » l'axe des abscisses.

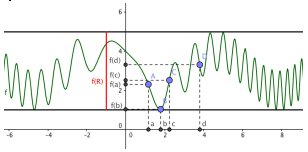
Exercice
Montrer qu'une suite (u_n) est également une fonction

Correction
Il s'agit d'une application de $\mathbb{N}$ dans $\mathbb{R}$, avec $u : n \mapsto u_n$

2.2. Opérations sur les fonctions

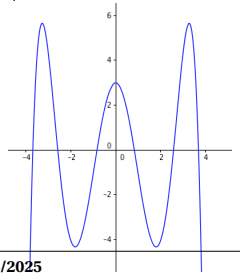
Définition - Opérations classiques
Dans $\mathscr{F}(I, \mathbb{R})$ on définit les opérations suivantes :
— Addition : si $(f, g) \in \mathscr{F}(I, \mathbb{R})^2$, la fonction $f + g$ est définie sur I par
$$\forall x \in I, (f+g)(x) = f(x) + g(x)$$
— Multiplication par un réel : si $f \in \mathscr{F}(I, \mathbb{R})$ et $\lambda \in \mathbb{R}$, la fonction λf est définie sur I par
$$\forall x \in I, (\lambda f)(x) = \lambda f(x)$$

Représentation - Fonction



Pour tracer on commence bien par tous les points en noir : $x_i, f(x_i)$, on en déduit $A_i(x_i, f(x_i))$. Puis on relie tous ces points A_i, une courbe apparait!
L'image de f est ici donné en rouge : c'est le segment $[1,5]$.

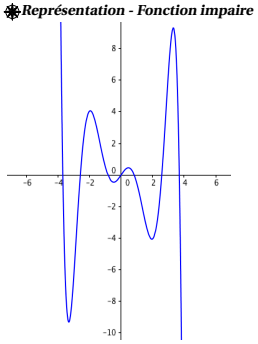
Représentation - Fonction paire



— Produit de deux fonctions : si $(f, g) \in \mathscr{F}(I, \mathbb{R})^2$, la fonction fg est définie sur I par
$$\forall x \in I, (fg)(x) = f(x) \times g(x)$$
— Valeur absolue d'une fonction : si $f \in \mathscr{F}(I, \mathbb{R})$ la fonction $|f|$ est définie sur I par
$$\forall x \in I, |f|(x) = |f(x)|$$

Remarque - Lois internes...
Addition et multiplication de deux applications sont des lois internes sur $\mathscr{F}(I, \mathbb{R})$, commutatives, associatives, l'application nulle est élément neutre pour l'addition et toute application f admet un opposé : l'application $-f$, l'application constante égale à 1 est élément neutre pour la multiplication, la multiplication est distributive par rapport à l'addition. (On parle d'anneau pour décrire un ensemble ayant deux telles lois internes).

Représentation - Fonction impaire

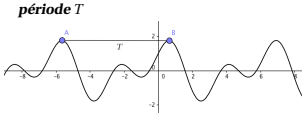


Définition - Composée
Soient $f : I \to \mathbb{R}$, $g : J \to \mathbb{R}$ vérifiant $f(I) \subset J$. On définit la composée $g \circ f : I \to \mathbb{R}$ par
$$\forall x \in I, (g \circ f)(x) = g(f(x)).$$

En général, même lorsque les deux fonctions $g \circ f$ et $f \circ g$ ont un sens, elles sont différentes.
Exercice
Définir proprement les deux composées (si cela est possible) des fonctions suivantes (ou de leurs restrictions) :
$$f : \begin{array}{l}\mathbb{R} \to \mathbb{R} \\ x \mapsto x^2 - 1\end{array} \quad \text{et} \quad g : \begin{array}{l}\mathbb{R} \setminus \{0\} \to \mathbb{R} \\ x \mapsto \frac{1}{x}\end{array}$$

Correction
$f \circ g : \begin{array}{l}\mathbb{R}^* \to \mathbb{R} \\ x \mapsto \frac{1}{x^2} - 1\end{array}$ et $g \circ f : \begin{array}{l}\mathbb{R} \setminus \{-1, 1\} \to \mathbb{R} \\ x \mapsto \frac{1}{x^2-1}\end{array}$

Représentation - Fonction périodique de période T



2.3. Vocabulaire d'analyse de fonctions

Parité, périodicité

Définition - Vocabulaire (et propriétés)
Soit $f : \mathscr{D}_f \to \mathbb{R}$ une fonction
• On dit que f est *paire* si
$$\forall x \in \mathscr{D}_f, -x \in \mathscr{D}_f \text{ et } f(-x) = f(x)$$
$\mathscr{C}_f$ est alors symétrique par rapport à Oy
• On dit que f est *impaire* si
$$\forall x \in \mathscr{D}_f, -x \in \mathscr{D}_f \text{ et } f(-x) = -f(x)$$
$\mathscr{C}_f$ est alors symétrique par rapport à O.
• $f \in \mathscr{F}(\mathbb{R}, \mathbb{R})$ est dite périodique s'il existe $T > 0$ tel que
$$\forall x \in D_f, x + T \in D_f, x - T \in D_f \text{ et } f(x+T) = f(x).$$
T est une période de f. $\mathscr{C}_f$ est alors invariante par translation de vecteur $T\vec{i}$.

On laisse les démonstrations au lecteur.

Fonctions monotones

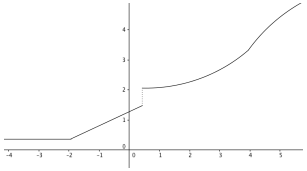
Définition - Fonction croissante, décroissante et monotone
On dit qu'une fonction f
- est croissante sur I si $\forall (x,y)\in I^2,\ x\leqslant y \Rightarrow f(x)\leqslant f(y)$.
- est décroissante sur I si $\forall (x,y)\in I^2,\ x\leqslant y \Rightarrow f(x)\geqslant f(y)$.
- est monotone sur I si elle est croissante sur I ou décroissante sur I.
- est *strictement* croissante sur I si $\forall (x,y)\in I^2,\ x<y \Rightarrow f(x)<f(y)$.
- est *strictement* décroissante sur I si $\forall (x,y)\in I^2,\ x<y \Rightarrow f(x)>f(y)$.

Proposition - Composition et monotonie
La composée de deux applications monotones de même sens de variation (respectivement de sens contraire) est une application croissante (respectivement décroissante).

La démonstration est simple…

Démonstration
Supposons que f et g sont décroissants.
Soit $x\leqslant y\in\mathscr{D}_{g\circ f}$, alors :
$f(x)\geqslant f(y)$
$(g\circ f)(x)\leqslant (g\circ f)(y)$.
Donc $g\circ f$ est décroissante…□

Représentation - Fonction strictement croissante



Fonction (a priori) croissante (et non dérivable!).

Fonctions convexes/concaves

Définition - Fonction convexe, concave
On dit qu'une fonction f
- est convexe sur I si
  $\forall (x,y)\in I^2, \forall\ \lambda\in[0,1]\ \ f(\lambda x+(1-\lambda)y)\leqslant \lambda f(x)+(1-\lambda)f(y)$.
- est strictement convexe sur I si
  $\forall (x,y)\in I^2, \forall\ \lambda\in]0,1[\ f(\lambda x+(1-\lambda)y)< \lambda f(x)+(1-\lambda)f(y)$.
- est concave sur I si
  $\forall (x,y)\in I^2, \forall\ \lambda\in[0,1]\ \ f(\lambda x+(1-\lambda)y)\geqslant \lambda f(x)+(1-\lambda)f(y)$.
- est strictement concave sur I si
  $\forall (x,y)\in I^2, \forall\ \lambda\in]0,1[\ f(\lambda x+(1-\lambda)y)> \lambda f(x)+(1-\lambda)f(y)$.

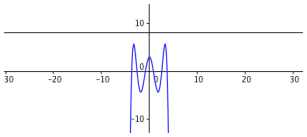
Pour aller plus loin - Fonctions convexes
Nous étudierons tout particulièrement les fonctions convexes dans un prochain chapitre

Fonctions (ou applications) bornées

Définition - Fonctions majorées, minorées, bornées
On dit qu'une fonction f :
- est majorée s'il existe $M\in\mathbb{R}$ tel que $\forall x\in\mathscr{D}_f,\ f(x)\leqslant M$.
- est minorée s'il existe $m\in\mathbb{R}$ tel que $\forall x\in\mathscr{D}_f,\ m\leqslant f(x)$.
- est bornée si elle est majorée et minorée.

Proposition - Bilan
Une application $f: I\to\mathbb{R}$ est bornée
si et seulement si il existe $M>0$ tel que $\forall x\in I,\ |f(x)|\leqslant M$.

Représentation - Fonction majorée, minorée?



Fonction (a priori) majorée et non minorée, donc non bornée.

Extremums

Définition - Maximum, minimum et extremum
On dit que $M\in\mathbb{R}$ est un maximum sur I de f si
- $\forall x\in I,\ f(x)\leqslant M$
- et il existe $a\in I$ tel que $f(a)=M$
  on dit que f présente un maximum en a.

On dit que $m\in\mathbb{R}$ est un minimum sur I de f si
- $\forall x\in I,\ f(x)\geqslant m$
- et il existe $a\in I$ tel que $f(a)=m$
  on dit que f présente un minimum en a.

On parle d'extremum lorsque l'on a un maximum ou un minimum. On note
$$M=\max_{x\in I} f(x) \text{ et } m=\min_{x\in I} f(x)$$

Définition - Maximum local
On dit que $M=f(a)$ est un *maximum local* (maximum ou minimum)
s'il existe $\epsilon>0$ tel que pour tout $x\in]a-\epsilon,a+\epsilon[\cap D_f,\ f(x)\leqslant f(a)$.
On parle de *maximum strict*, lorsque pour $x\in]a-\epsilon,a+\epsilon[\cap D_f$ et $x\neq a$, $f(x)<f(a)$.

Remarque - Voisinage de a (dans $\mathbb{R}$
Pour décrire un tel ensemble V, on parle souvent de voisinage de a.
Ainsi la restriction de f à $V=]a-\epsilon,a+\epsilon[\cap D_f$ présente en a un extremum (stricte) respectivement).

Remarque - Extension de définition
La définition s'étend à minimum local et minimum local strict et à maximum local et maximum local strict.

Représentation - Exemple
Sur la représentation de la fonction majorée non minorée, on peut voir trois maximums (maxima) locaux, tous stricts et deux sont aussi maximum global…

2.4. Bijections et réciproques

On commence par rappeler ce qu'est une fonction bijective avant de voir le rôle joué ici par la dérivée.

Bijection

Définition - Bijection
Soit f une fonction définie sur un sous-ensemble D de $\mathbb{R}$ à valeurs dans $\mathbb{R}$ et $J\subset\mathbb{R}$.
On dit que f est bijective de D sur J (ou réalise une bijection de D sur J)
- si tout élément de D a son image dans J
- et si tout élément de J admet un unique antécédent par f dans D

Formellement :
$$\forall x\in D,\ f(x)\in J \quad \text{et} \quad \forall y\in J, \exists! x\in D,\ y=f(x).$$

Remarque - Si, par convention $J=f(D)$
Si l'on pose $J=f(D)=\{f(x);x\in D\}=\{y\in\mathbb{R}\mid \exists x\in D, y=f(x)\}$,
alors f est une bijection de D sur $J=f(D)$ si et seulement si $\forall y\in J, \exists! x\in D,\ y=f(x)$.

Exemple - Application exponentielle
L'application exponentielle est une bijection de $\mathbb{R}$ sur $\mathbb{R}_+^*$

Définition - Application (bijection) réciproque
Si f est bijective de D sur J, on définit une fonction g par
$$\begin{array}{rll} g: & J\to D & \\ & y\mapsto x & \mid y=f(x) \text{ (unique antécédent de } y \text{ par } f)\end{array}$$

Cette fonction g est elle-même bijective et appelée bijection réciproque de f, et notée f^{-1}.

Exemple - Application logarithmique
L'application logarithmique (naturelle) est une bijection de $\mathbb{R}_+^*$ sur $\mathbb{R}$. C'est la bijection réciproque de la fonction exponentielle.

Proposition - Application directe
Si f est une bijection de D sur J, on a

$$\forall x \in D, (f^{-1} \circ f)(x) = x;$$

$$\forall y \in J, (f \circ f^{-1})(y) = y;$$

$$y = f(x) \Leftrightarrow x = f^{-1}(y).$$

Théorème - Réciproque et représentation graphique
Soit $f : I \to J$ une bijection et $f^{-1} : J \to I$ sa bijection réciproque. Alors
- dans un repère orthonormé, $\mathscr{C}_f$ et $\mathscr{C}_{f^{-1}}$ sont symétriques par rapport à la première bissectrice (droite d'équation $y = x$).
- Si f est monotone sur I alors f^{-1} est monotone sur J, de même sens de variations.

On verra des exemples plus loin.

Démonstration
Pour montrer la symétrie dans le graphique, il nous faut alors montrer l'équivalence entre :
$M(x,y) \in \mathscr{C}_f$ et $M'(y,x) \in \mathscr{C}_{f^{-1}}$.
Or
$$M' \in \mathscr{C}_{f^{-1}} \Leftrightarrow f^{-1}(y) = x \Leftrightarrow y = f(x) \Leftrightarrow M \in \mathscr{C}_f$$
Concernant la monotonie, supposons que f soit croissante, :
considérons $x \leqslant y \in J$,
si $f^{-1}(x) > f^{-1}(y)$, alors par croissance de f : $x > y$. Absurde.
donc, nécessairement : $f^{-1}(x) \leqslant f^{-1}(y)$ et f^{-1} est croissante.
De même si f^{-1} est croissante, alors sa réciproque, i.e. f est également croissante.
Le cas décroissant est laissé en exercice.□

On admet les théorèmes qui suivent et qui seront démontrés ultérieurement :

Théorème - Théorème de la bijection
Soit f une fonction définie sur I, continue, strictement monotone sur I (intervalle de $\mathbb{R}$),
alors f est bijective de I sur $J = f(I)$.
Sa bijection réciproque f^{-1} est continue sur J.

2.5. Etude des branches infinies en ∞

Le but est de préciser l'allure de la courbe représentative de f au voisinage de (+ ou -) l'infini.

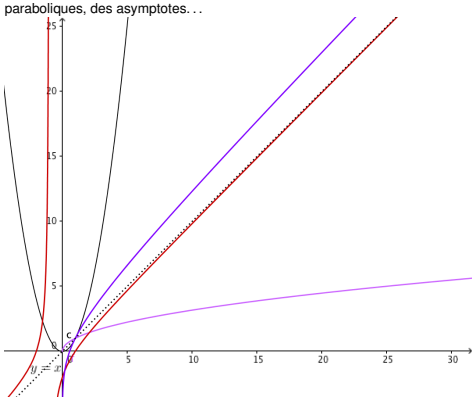
Savoir faire - Etude des branches infinies (et définition)
Soit f une fonction définie au voisinage de $\pm\infty$.
1. si $\lim\limits_{x\to\infty} f(x) = \ell$ avec $\ell \in \mathbb{R}$, la courbe admet une **asymptote horizontale** d'équation $y = \ell$.
2. si $\lim\limits_{x\to\infty} f(x) = \infty$, on calcule $\dfrac{f(x)}{x}$.
   (a) si $\lim\limits_{x\to\infty} \dfrac{f(x)}{x} = 0$, il y a une **branche parabolique horizontale** (ou de direction Ox).
   (b) si $\lim\limits_{x\to\infty} \dfrac{f(x)}{x} = \infty$, il y a une **branche parabolique verticale** (ou de direction Oy).
   (c) si $\lim\limits_{x\to\infty} \dfrac{f(x)}{x} = a$, $a \in \mathbb{R}^*$, il faut calculer $f(x) - ax$.
      i. si $\lim\limits_{x\to\infty} f(x) - ax = b \in \mathbb{R}$, la courbe admet une **asymptote oblique** d'équation $y = ax + b$.
      ii. si $\lim\limits_{x\to\infty} f(x) - ax = \infty$ il y a une **branche parabolique oblique de direction** $y = ax$.

Exercice
Énoncer des fonctions présentant :
1. une asymptote horizontale (on donnera l'équation de cette asymptote)
2. une branche parabolique horizontale
3. une branche parabolique verticale
4. une asymptote oblique (on donnera l'équation de cette asymptote)
5. une branche parabolique oblique (on donnera la direction), mais pas d'asymptote oblique

Correction

1. $y = \arctan(x)$ admet une asymptote horizontale : $y = \frac{\pi}{2}$
2. $y = \sqrt{x}$ admet une branche parabolique horizontale
3. $y = x^2$ admet une branche parabolique verticale
4. $y = \dfrac{2x^2+x-2}{x+1} (= 2x - 1 - \frac{1}{x+1})$ admet une asymptote oblique d'équation $y = 2x - 1$
5. $y = 3x + \ln x$ admet une branche parabolique oblique d'équation $y = 3x$.

Exercice
Indiquer sous chacun des quatre graphiques suivants lesquels présentent des branches paraboliques, des asymptotes...



Correction
En noir : branche parabolique verticale, en bleu une branche parabolique oblique d'équation $y = x$, en rouge un courbe avec asymptote d'équation $y = x$ et en violet une courbe avec une direction parabolique horizontale.

Remarque - Courbe asymptote
Plus généralement on dit que la courbe représentative de f admet au voisinage de $+\infty$ (ou $-\infty$ ou un réel a) admet pour courbe asymptote la courbe d'équation $y = g(x)$ si $\lim\limits_{x\to+\infty} f(x) - g(x) = 0$.

3. Fonctions trigonométriques

On reprend, de manière analytique (où le paramètre x devient une variable) les fonctions trigonométriques vues précédemment.

3.1. Fonctions circulaires

Proposition - Aspect analytique
Les fonctions sinus et cosinus sont 2π-périodiques.
sin est une fonction impaire alors que cos est une fonction paire.

Savoir faire - Transférer un problème trigonométrique « en a », vers « en 0 »
Il faut exploiter les formules trigonométriques : $\sin(a+h) = \sin a \cos h + \cos a \sin h$ et $\cos(a+h) = \cos a \cos h - \sin a \sin h$, à connaître par coeur.

Analyse - Inégalité fondamentale
On termine cette partie par une observation essentielle :
Rappelons que θ est la longueur de l'angle
(on peut aussi comparer l'aire du triangle BCA', égale à $\frac{1\times CA}{2} = \frac{1}{2}\sin\theta$
à l'aire (plus grande) de la portion du disque BCA égale à $\frac{\theta}{2\pi}\times\pi 1^2 = \frac{1}{2}\theta$.)
Pour la seconde inégalité, on calcule deux aire :
— l'aire de la portion du disque BAC : elle vaut $\frac{\theta}{2}R^2 = \frac{\theta}{2}$ car $R=1$
— l'aire du triangle rectangle $BA'C'$: elle vaut $\frac{1}{2}BA'A'C' = \frac{\tan\theta}{2}$.
« Clairement » la seconde aire est plus petite que la première.

Proposition - Inégalité
On a pour tout $x\in]-\frac{\pi}{2},\frac{\pi}{2}[$,

$$|\sin x| \leqslant |x| \leqslant |\tan x| = \frac{|\sin x|}{\cos x}$$

Et en particulier $\lim\limits_{x\to 0}\dfrac{\sin x}{x} = 1$

Démonstration
On a vu (dans l'analyse) que pour $x\in]0,\frac{\pi}{2}[$, $\sin x \leqslant x \leqslant \tan x$.
Puis en multipliant par $-1<0$: $-\sin x \geqslant -x \geqslant -\tan x$.
et par imparité si $x_-\in]-\frac{\pi}{2},0[$: $\sin(x_-) = -\sin(-x_-) \geqslant -(-x_-) \geqslant -\tan(-x_-) = \tan(x_-)$.
Ainsi pour $x\in]-\frac{\pi}{2},\frac{\pi}{2}[$: $|\sin(x)| \leqslant |x| \leqslant |\tan(x)| = \dfrac{|\sin x|}{\cos x}$
Donc en divisant par $|x|$ et en séparant en deux inégalités :

$$\left|\frac{\sin x}{x}\right| \leqslant 1 \qquad \text{et} \qquad \cos x \leqslant \left|\frac{\sin x}{x}\right|$$

Par encadrement : $\dfrac{\sin x}{x} \xrightarrow[x\to 0]{} 1$.
Ainsi sin est dérivable en 0 de dérivée égale à 1. □

Exemple - Calculatrice. Calculer $\sin(0,01234)$
On obtient $\sin(0,01234) = 0,01233968682$

Exercice
En majorant le module de $e^{ix}-1$, montrer que pour tout $x\in\mathbb{R}$, $\sin^2 x + (\cos x + 1)^2 \leqslant x^2$.

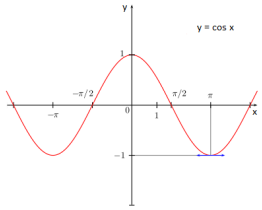
Correction
Soit $x\in\mathbb{R}$, la factorisation par l'angle moitié donne : $e^{ix}-1 = e^{i\frac{x}{2}}(2i\sin\frac{x}{2})$, donc

$$|e^{ix}-1| = 1\times 2|\sin\frac{x}{2}| \leqslant |x|$$

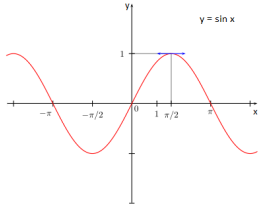
Si on élève au carré :

$$(\cos x - 1)^2 + \sin^2 x \leqslant x^2$$

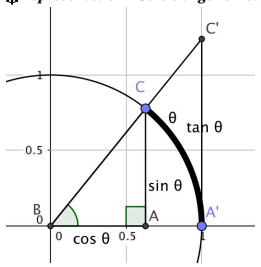
Représentation - Fonction cosinus



Représentation - Fonction sinus

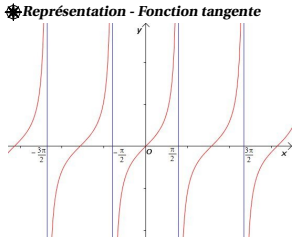


Représentation - Cercle trigonométrique



Proposition - Fonction tangente - Aspect analytique
La fonction tangente est ainsi définie sur $\mathbb{R}\setminus\{\frac{\pi}{2}+k\pi; k\in\mathbb{Z}\}$ ($\mathbb{R}$ privé des points de la forme $\frac{\pi}{2}+k\pi$ avec $k\in\mathbb{Z}$).
tan est impaire, π-périodique

Représentation - Fonction tangente



Démonstration
Il s'agit de la division de deux fonctions dérivables. Sur $\mathbb{R}\setminus\{\frac{\pi}{2}+k\pi; k\in\mathbb{Z}\}$ (le cosinus ne s'annule pas) : □

Exercice
Etudier et représenter la fonction tan

Correction
La fonction tan est définie sur $\mathscr{D} = \{x\in\mathbb{R} \mid \cos\theta\neq 0\} = \mathbb{R}\setminus\{\frac{\pi}{2}+k\pi; k\in\mathbb{Z}\}$.
La fonction tan est π-périodique d'après la formule trouvée plus haut.
On peut l'étudier sur $]-\frac{\pi}{2},\frac{\pi}{2}[$, puis exploiter des translations de vecteurs $\pi\vec{\imath}$.
Par division de deux fonctions dérivables, tan est dérivable sur son ensemble de définition.

$$\forall\, x\in\mathscr{D},\qquad \tan'(x) = \frac{\cos^2(x)+\sin^2(x)}{\cos^2(x)} = 1+\tan^2(x) = \frac{1}{\cos^2(x)}$$

La fonction tan est donc strictement croissante sur les intervalles de la forme $]\frac{-\pi}{2},\frac{-\pi}{2}[$ et à valeurs dans $]-\infty,\infty[$.
$\tan(0) = 0$ et la pente de la tangente au point 0a pour pente : $\tan'(k\pi) = \dfrac{1}{\cos(k\pi)} = 1$.
Enfin, comme $\frac{1}{\cos^2}$ est croissante sur $[0,\frac{\pi}{2}[$, tan est convexe sur $[0,\frac{\pi}{2}[$ et $\frac{1}{\cos^2}$ est décroissante sur $]-\frac{\pi}{2},0]$, tan est concave sur $]-\frac{\pi}{2},0]$.
On obtient la représentation graphique suivante :

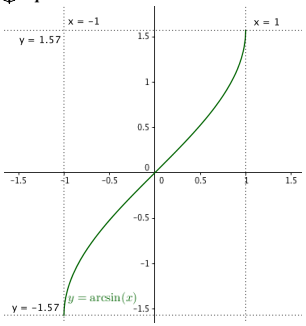
3.2. Fonctions circulaires réciproques

Fonction arcsin

Définition - Arcsinus
La fonction sinus est continue et strictement croissante sur $[-\frac{\pi}{2},\frac{\pi}{2}]$ donc réalise une bijection de $[-\frac{\pi}{2},\frac{\pi}{2}]$ sur $[-1,1]$.
La bijection réciproque s'appelle arcsinus, $\arcsin : [-1,1]\to[-\frac{\pi}{2},\frac{\pi}{2}]$.
Elle est impaire, strictement croissante. On a donc :

$$t = \arcsin x \Leftrightarrow \left(\sin t = x \text{ et } t\in[-\frac{\pi}{2},\frac{\pi}{2}]\right)$$

***Représentation - Fonction* arcsin**



Proposition - Rappels
On a :
— $\forall x\in[-\frac{\pi}{2},\frac{\pi}{2}]$, $\arcsin(\sin x) = x$
— $\forall x\in[-1,1]$, $\sin(\arcsin x) = x$
— $\forall x\in[-1,1]$, $\cos(\arcsin x) = \sqrt{1-x^2}$
— $\forall x\in]-1,1[$, $\tan(\arcsin x) = \frac{x}{\sqrt{1-x^2}}$

Analyse - Questions
Comment démontrer tout cela?
Il faut connaître les valeurs remarquables suivantes :

x	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\arcsin x$	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$

Exercice
Comparer $\arcsin x$ et x, à partir de la double inégalité fondamentale du sinus.

Correction
On a vu pour tout $x \in]-\frac{\pi}{2}, \frac{\pi}{2}[$, $|\sin x| \leqslant |x| \leqslant |\tan x|$.
Posons $x = \arcsin u$, pour $u \in]-1,1[$; donc $x \in]-\frac{\pi}{2}, \frac{\pi}{2}[$.

$$|u| \leqslant |\arcsin u| \leqslant |\tan(\arcsin u)| = \frac{|u|}{\sqrt{1-u^2}}.$$

Fonction arccos

Définition - Arccosinus
La fonction cosinus est continue et strictement décroissante sur $[0,\pi]$ donc réalise une bijection de $[0,\pi]$ sur $[-1,1]$.
La bijection réciproque s'appelle arccosinus, $\arccos : [-1,1] \to [0,\pi]$.
Elle est strictement décroissante et on a donc :

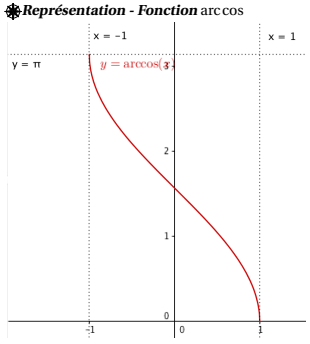
$$t = \arccos x \Leftrightarrow \Big(\cos t = x \text{ et } t \in [0,\pi]\Big)$$

Proposition - Rappels
On a :
- $\forall x \in [0,\pi]$, $\arccos(\cos x) = x$
- $\forall x \in [-1,1]$, $\cos(\arccos x) = x$
- $\forall x \in [-1,1]$, $\sin(\arccos x) = \sqrt{1-x^2}$
- $\forall x \in [-1,1], x \neq 0$, $\tan(\arccos x) = \frac{\sqrt{1-x^2}}{x}$
- $\forall x \in [-1,1]$, $\arcsin x + \arccos x = \frac{\pi}{2}$

Il faut connaître les valeurs remarquables suivantes :

x	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\arccos x$	$\frac{\pi}{2}$	$\frac{\pi}{3}$	$\frac{\pi}{4}$	$\frac{\pi}{6}$	0

Représentation - Fonction arccos



Fonction arctan

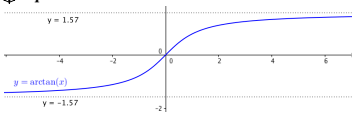
Définition - Arctangente
La fonction tangente est continue et strictement croissante sur $]-\frac{\pi}{2}, \frac{\pi}{2}[$ donc réalise une bijection de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ sur $\mathbb{R}$.
La bijection réciproque s'appelle arctangente, $\arctan : \mathbb{R} \to]-\frac{\pi}{2}, \frac{\pi}{2}[$.
Elle est impaire, strictement croissante et on a donc :

$$t = \arctan x \Leftrightarrow \Big(\tan t = x \text{ et } t \in]-\frac{\pi}{2}, \frac{\pi}{2}[\Big)$$

Proposition - Rappels
On a :
- $\forall x \in]-\frac{\pi}{2}, \frac{\pi}{2}[$, $\arctan(\tan x) = x$
- $\forall x \in \mathbb{R}$, $\tan(\arctan x) = x$
- $\forall x \in \mathbb{R}$, $\cos(\arctan x) = \frac{1}{\sqrt{1+x^2}}$
- $\forall x \in \mathbb{R}$, $\sin(\arctan x) = \frac{x}{\sqrt{1+x^2}}$

- $\forall x \in \mathbb{R}$, $\arctan x + \arctan \frac{1}{x} = \begin{cases} \frac{\pi}{2} & \text{si } x > 0 \\ -\frac{\pi}{2} & \text{si } x < 0 \end{cases}$

Représentation - Fonction arctan



Il faut connaître les valeurs remarquables suivantes :

x	0	$\frac{1}{\sqrt{3}} = \frac{\sqrt{3}}{3}$	1	$\sqrt{3}$
$\arctan x$	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$

4. Fonctions polynomiales et puissances rationnelles

On reprend, de manière analytique (où le paramètre x devient une variable) les fonctions puissances et polynomiales vues précédemment.

Pour aller plus loin - Besoin d'inégalités
Pour étudier les limites variées (à l'infini, ou calculer des dérivées), on a ***toujours*** *besoin d'encadrement.*
Dans chaque partie, on trouvera des inégalités importantes

4.1. Fonction puissance entière relative

Définition

Définition - Puissance entière > 0
Soit $n \in \mathbb{N}^*$, on qualifie de fonction puissance entière l'application $x \mapsto x^n$, i.e. définie par récurrence par $x \mapsto x \times x^{n-1}$ et $x^0 = 1$.
Son ensemble de définition est $\mathbb{R}$. C'est une fonction continue (nous le verrons plus tard).
Cette application est paire si n est pair, et impaire si n est impair.

Histoire - Notation des puissances et puissances négatives
Cette notation émerge petit à petit chez Bombelli (1572), Simon Stevin (1585), Descartes puis Newton.

Il faut savoir représenter ces fonctions.

Définition - Puissance entière < 0
Soit $m \in \mathbb{Z}_-$, on qualifie de fonction puissance entière négative l'application $x \mapsto x^m = \frac{1}{x^{-m}}$, i.e. définie par récurrence par $x \mapsto \frac{1}{x} \times x^{m+1}$ et $x^0 = 1$.
Son ensemble de définition est $\mathbb{R}^*$. C'est une fonction continue sur $\mathbb{R}_+^*$ et sur $\mathbb{R}_-^*$.
Cette application est paire si n est pair, et impaire si n est impair.

Il faut savoir représenter ces fonctions, en particulier l'hyperbole $\mathscr{C}$ associé à $x \mapsto \frac{1}{x}$ $(m = -1)$.

Proposition - Morphisme
On a pour tout $m, n \in \mathbb{Z}$ et $x \in \mathbb{R}^*$, $x^m \times x^n = x^{m+n}$.
Vrai également en $x = 0$, si $n, m > 0$.

Exercice
A démontrer

Correction
On fixe $m \in \mathbb{Z}$, et on fait une récurrence sur $n \in \mathbb{N}$.
Puis, on étudie le cas $n < 0$, avec $-m \in \mathbb{Z}$: $x^{-m} \times x^{-n} = x^{-m+-n}$...

Inégalités de croissance

Fixons $n \in \mathbb{N}$.
Pour la croissance de $x \mapsto x^n$, on exploite le binôme de Newton, par exemple :

Proposition - Binôme de Newton. Croissance
Soit $n \in \mathbb{N}$. Pour tout $a \in \mathbb{R}$, $(a+x)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} x^k$.
Avec $a, x > 0$, on a donc $x < x' \Rightarrow x^n < x'^n$, soit la croissance de $x \mapsto x^n$ sur $\mathbb{R}_+$.

Démonstration
$a = x' - x > 0$, $x'^n = x^n + \underbrace{\sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} x^k}_{>0} > x^n$. □

Exercice
Faire la démonstration par récurrence.
On fera bien attention aux variables fixées et celles qui sont libres

Correction
On peut fixer x et x' dans $\mathbb{R}_+$, par exemple : $0 \leqslant x < x'$.
Posons, pour tout entier $n \in \mathbb{N}^*$, $\mathscr{P}_n$: « $0 \leqslant x^n < x'^n$. »
— $\mathscr{P}_1$ est vraie par hypothèse.
— Soit $n \in \mathbb{N}^*$. Supposons que $\mathscr{P}_n$ est vraie.
Comme $x \geqslant 0$: $x^{n+1} = x^n \times x \leqslant x'^n \times x$, d'après $\mathscr{P}_n$.
Puis comme $x < x'$ et $x'^n > 0$: $x'^n \times x < x'^n \times x' = x'^{n+1}$.
Donc $\mathscr{P}_{n+1}$ est vraie.
La récurrence est démontrée : $\forall\, n \in \mathbb{N}^*$, $0 \leqslant x^n < x'^n$.
Ceci est vraie pour tout $0 \leqslant x < x'$, on a donc :
$\forall\, (x, x', n) \in \mathbb{R}_+ \times \mathbb{R}_+^* \times \mathbb{N}^*$ tel que $x < xt$: $x^n < x'^n$,
On a donc encore : $\forall\, n \in \mathbb{N}^*$, $\forall\, 0 \leqslant x < x'$, $x^n < x'^n$, donc $t \mapsto t^n$ est strictement croissante sur $\mathbb{R}_+$.
Peut-on se passer de $0 \leqslant$ *dans l'écriture de* $\mathscr{P}_n$ *?*

Inégalités de Bernoulli

Proposition - Inégalités de Bernoulli
Soit $x \in]-1, +\infty[$, pour tout $n \in \mathbb{N}^*$, $(1+x)^n \geqslant 1 + nx$.
Pour $x \in]-1, \frac{1}{n}[$, pour tout $n \in \mathbb{N}$, $(1+x)^n \leqslant \dfrac{1}{1-nx}$

Démonstration
Par récurrence, on note $\mathscr{P}_n$: « $\forall\, x > -1$, $(1+x)^n \geqslant 1 + nx$ et $\forall\, x \in [-1, \frac{1}{n}]$, $(1+x)^n \leqslant \dfrac{1}{1-nx}$ ».
— Le résultat est vrai pour $n = 0$ (et $n = 1$ (immédiat)).
Donc $\mathscr{P}_0$ est vraie.
— Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}_n$ est vraie.
Soit $x > -1$. On a donc $(1+x)^{n+1} = (1+x)^n \times (1+x) \leqslant (1+nx)(1+x) = 1 + (n+1)x + nx^2$,
car : $1 + x > 0$ et $nx^2 \geqslant 0$.
De même si $x \in]-1, \frac{1}{n+1}[\subset]-1, \frac{1}{n}[$, $(1+x)^{(n+1)} = (1+x) \times (1+x)^n \leqslant \dfrac{1+x}{1-nx}$ car $1 + x > 0$.
Or $(1+x)(1-(n+1)x) = 1 - nx - (n+1)x^2 \leqslant 1 - nx$ car $(n+1)x^2 \geqslant 0$.
Ainsi, en divisant par $(1-(n+1)x)(1-nx) \geqslant 0$: $(1+x)^{(n+1)} \leqslant \dfrac{1+x}{1-nx} \leqslant \dfrac{1}{1-(n+1)x}$
Donc $\mathscr{P}_{n+1}$ vraie.
On obtient ainsi la première et la troisième inégalité (en composant par $t \mapsto \frac{1}{t}$ décroissante sur $\mathbb{R}+$).
□

L'exercice suivant permet de montrer la continuité des fonctions puissances.
Exercice
On fixe $n \in \mathbb{N}$.Montrer que $\lim_{x \to 0+} (1+x)^n = 1$, puis la continuité à droite de $t \mapsto t^n$ en 1 et en tout $x \in \mathbb{R}$.

Correction
Soit n fixé. Pour tout $x \in [0, \frac{1}{n}[$,

$$1 + nx \leqslant (1+x)^n \leqslant \frac{1}{1-nx}$$

Par encadrement : même limite à gauche et à droite, pour $x \to 0^+$, on a donc $(1+x)^n \underset{x \to 0^+}{\longrightarrow} 1$. Soit $a \in \mathbb{R}$ et $h > 0$, alors $(a+h)^n = a^n(1+\frac{h}{a})^n$, ainsi si $0 \leqslant \frac{h}{a} \leqslant \frac{1}{2}$,
on a : $a^n(1+n\frac{h}{a}) \leqslant (a+h)^n = a^n(1+\frac{h}{a})^n \leqslant a^n(1+2n\frac{h}{a})$.
Là encore, pour $h \to 0^+$, on a donc $(a+h)^n \to a^n$, ce qui conduit à la continuité à droite de $t \mapsto t^n$.

4.2. Fonctions polynomiales

Définition - Fonction polynomiale
On appelle fonction polynomiale une fonction de la forme :

$$f : x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{k=0}^{n} a_k x^k$$

où $\forall\, k \in [\![0, n]\!]$, $a_k \in \mathbb{R}$ (ou $\mathbb{C}$) ;
Il s'agit d'une combinaison linéaire finie de puissances entières de la variable x. On parle de polynôme simple ou de polynôme à une variable.
On dit que $f(x) = b$ est une équation polynomiale si f est une fonction polynomiale.

Remarque - Notations
On remarque que les lettres de fin d'alphabet sont en générale associées à des inconnues. Les lettres de début d'alphabet aux variables connues.
On comprend pour les inconnues : on ne peut pas faire autrement. Mais pourquoi associer des lettres à des nombres connus?
Par propriétés calculatoires sur $\mathbb{R}$ ou $\mathbb{C}$:

Proposition - Propriété de l'ensemble des fonctions polynomiales
Si f et g sont deux fonctions polynomiales, alors :
— $f + g$ est une fonction polynomiale
— $f \times g$ est une fonction polynomiale
— $f \circ g$ est une fonction polynomiale.

Démonstration
Il suffit d'écrire les calculs. Cela est lié aux propriétés des anneaux $\mathbb{R}$ et $\mathbb{C}$.
Pour la composition, c'est plus subtile. On note que, par récurrence, grâce au résultat sur les produits :
Pour tout g, polynomiale, tout $k \in \mathbb{N}^*$: $g^k = g^{k-1} \times g$ est également polynomiale.
puis d'après le résultat sur la somme, par récurrence : $\sum_{k=0}^{n} a_k g^k(x) = f \circ g$ est polynomiale.
□

Rappelons :

Théorème - Factorisation multiple
Soit f une fonction polynomiale de degré n. Soit $p \leqslant n$
Si $x_1, x_2, \ldots x_p$, p solutions différentes de l'équation $f(x) = 0$ (racines de f).
Alors il existe g_p, fonction polynomiale de degré $n - p$ tel que

$$\forall\, x \in \mathbb{K}, \qquad f(x) = (x - x_1)(x - x_2)\ldots(x - x_p) \times g_p(x)$$

Corollaire - Nombre maximal de solution
Une équation polynomiale de degré n admet au plus n solutions différentes

4.3. Fonction puissance rationnelle

Définition

Analyse - Bijection de $x \mapsto x^n$ sur $\mathbb{R}_+$
Pour tout $n \in \mathbb{N}^*$, $x \mapsto x^n$ est strictement croissante sur $I = \mathbb{R}_+$ et à valeurs dans $J = \mathbb{R}_+$.
Elle est continue et donc admet une application réciproque de $J = \mathbb{R}_+$ sur $I = \mathbb{R}_+$.
Dans le cas où n est impair, on peut élargir la définition de $I = \mathbb{R}$ sur $J = \mathbb{R}$.

Définition - Racine n-ième
On note $\sqrt[n]{.}$ la bijection réciproque de $x \mapsto x^n$.
On a donc :

$$\begin{array}{lll} \text{si } n \text{ est pair} & \sqrt[n]{x} = & x^{1/n} \quad \text{pour } x \geqslant 0 \\ \text{si } n \text{ est impair} & \sqrt[n]{x} = & \begin{cases} x^{1/n} & \text{pour } x \geqslant 0 \\ -|x|^{1/n} = -(-x)^{1/n} & \text{pour } x \leqslant 0 \end{cases} \end{array}$$

Pour n impair on a donc $\sqrt[n]{-x} = -\sqrt[n]{x}$.

Définition - Puissance rationnelle
Soit $r = \frac{p}{q} \in \mathbb{Q}^*$ (avec $q \in \mathbb{N}^*$, $p \in \mathbb{Z}$), on qualifie de fonction puissance rationnelle l'application $x \mapsto x^r$ où x^r vérifie $(x^r)^q = x^p$.
Son ensemble de définition est $\mathbb{R}_+^*$. C'est une fonction croissante et continue (nous l'admettons à ce stade).

Exemple - $5^{2/3}$
Il s'agit du nombre y tel que $y^3 = 5^2 = 25$. (Existe-t-il un et un seul nombre y qui vérifie cette équation $y^3 = 25$?).
Par dichotomie (et croissance) : $2^3 = 8$ et $3^3 = 27$, donc $y \in]2,3[$. Et l'on peut chercher à préciser...
$2{,}9^3 = 24{,}389$. Donc $y \in]2{,}9;3[$...

Inégalités complémentaires

Analyse - Image de $[0,1[$ et image de $]1,+\infty[$ par $x \mapsto x^r$
Si $x > 1$, alors pour $n, m \in \mathbb{N}$: $x^n > 1$.
Et pour tout $y < 1$, $y^m < 1$.
Et nécessairement y tel que $y^m = x^n > 1$ vérifie $y > 1$.

Proposition - Comparaison des fonctions puissances
Soient $r < r' \in \mathbb{Q}$.
Alors pour tout $x > 1$, $x^r < x^{r'}$. Et si $x < 1$, $x^r > x^{r'}$

Démonstration
La soustraction $r' - r = r''$ donne un nombre rationnel, positif.
On a alors, par positivité de x^r :
$x^r < x^{r'} \iff x^{r''} = x^{r'-r} > 1$.
Or $x > 1$ et $r'' \in \mathbb{Q}^+$, donc $x^{r''} > 1$.
Si $x < 1$, on raisonne avec $\frac{1}{x} > 1$.
□

Attention - Ne pas confondre les variables x et n
Dès maintenant, on fait bien attention lorsqu'on compare à x fixé x^r et x^s,
et lorsqu'on compare à r fixé x^r et x'^r.

5. Exponentielles et logarithmes

Heuristique - Histoire
Les mathématiciens ont d'abord rencontrer les fonctions logarithmiques (Stevin, Briggs, Neper) au XVIeme siècle.
Ils cherchaient un processus pour transformer multiplication (complexe) en addition (plus simple).
Il s'agissait d'interpoler la réciproque des suites géométriques : $n \mapsto a^n$, vérifiant $a^{n+m} = a^n \times a^m$.
Pour faciliter les démonstrations du cours, nous remonterons l'histoire (d'abord exponentielles avant logarithmes).

5.1. ExponentielleS

Heuristique - Equation fonctionnelle
Soit $a \in \mathbb{R}$, si $n, m \in \mathbb{N}$, $a^{n+m} = a^n \times a^m$.
Cette relation est centrale si l'on s'intéresse à $x \mapsto a^x$.
Considérons donc $f : \mathbb{R} \to \mathbb{R}$ vérifiant pour tous nombres réels $x, y \in \mathbb{R}$: $f(x+y) = f(x) \times f(y)$.
Est-ce qu'une telle relation est suffisante pour définir parfaitement aucune (non car $t \mapsto 2^t$ semble bien aller, au moins pour $t \in \mathbb{Q}$), une fonction f, ou plusieurs? Et dans ce cas, que rajouter pour différencier ces différentes fonctions?

On notera le pluriel :

Définition - Fonctions exponentielles
On qualifie de fonctions exponentielles les applications $f : \mathbb{R} \to \mathbb{R}$, non nulles vérifiant :
$\forall\, x, y \in \mathbb{R} : f(x+y) = f(x) \times f(y)$.

Proposition - Propriété commune à toutes les exponentielles
Si f est une fonction vérifiant : $f(x+y) = f(x) \times f(y)$, alors f est à valeurs dans $\mathbb{R}_+$.
Puis : ou bien $f : x \mapsto 0$, ou bien $f(0) = 1$.
Donc une fonction exponentielle est à valeurs dans $\mathbb{R}_+$ et $f(0) = 1$.

Démonstration
Pour tout $x \in \mathbb{R}$, $f(x) = f(\frac{x}{2} + \frac{x}{2}) = \left(f(\frac{x}{2})\right)^2 \geqslant 0$.
$f(x) = f(0+x) = f(0) \times f(x)$.
Si il existe x tel que $f(x) \neq 0$, alors en divisant par $f(x)$: $f(0) = 1$.
Sinon, pour tout $x \in \mathbb{R}$, $f(x) = 0$ et on a bien (réciproquement) $f(x+y) = 0 = f(x) \times f(y)$. □

Proposition - Base
Si f est une fonction exponentielle non nulle, alors il existe un nombre $a \in \mathbb{R}_+$, tel que pour tout $x \in \mathbb{Q}$, $f(x) = a^x$

Savoir faire - Etude d'une équation fonctionnelle de $\mathbb{N}$ à $\mathbb{R}$
L'étude d'une équation fonctionnelle se fait souvent de la façon suivante :

1. Par récurrence, en étudiant $f(sn)$ pour $n \in \mathbb{N}$ et s quelconque.
2. Par imparité/parité (ou autre symétrie), on étudie $f(sm)$ pour $m \in \mathbb{Z}$.
3. On retrouve ensuite le résultat pour $m \in \mathbb{Q}$.
4. Ensuite, on exploitera (plus tard) un argument de continuité ou bien un argument de croissance

Démonstration
Considérons une fonction exponentielle, non nulle.
Soit $s \in \mathbb{R}$, fixé.
Posons, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$: « $f(sn) = (f(s))^n$.
— Le résultat est vraie pour $n = 0$ (car $f(s)^0 = 1 = f(0)$) et $n = 1$.
— Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}_n$ est vraie.
Alors $f(s(n+1)) = f(sn+s) = f(sn) \times f(s) = (f(s))^{n+1}$ d'après $\mathscr{P}_n$.
Soit $t \in \mathbb{R}$, $f(t+(-t)) = f(0) = 1 = f(t) \times f(-t)$, donc $f(-t) = \dfrac{1}{f(t)}$.
Ainsi, pour $t \leftarrow sn$, alors $f(s\times(-n)) = \dfrac{1}{f(sn)} = \dfrac{1}{(f(s))^n} = (f(s))^{-n}$ Ainsi, $s \leftarrow 1$ et $a = f(1) > 0$,
on a pour tout $m \in \mathbb{Z}$, $f(m) = f(1m) = f(1)^m = a^m$.
Considérons, alors $r = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.
on a $f(qr) = f(p) = a^p$ et $f(qr) = f(r)^q$ avec $s \leftarrow r$ et $n \leftarrow q$.
on a donc, en prenant la racine q-ième : $f(r) = a^{\frac{p}{q}} = a^r$ □

Proposition - Variations
Soi f une fonction exponentielle est non nulle,
f est strictement croissante sur $\mathbb{Q}$ si $f(1)(= a) > 1$
et elle est décroissante sur $\mathbb{Q}$ si $f(1)(= a) < 1$

Démonstration
Supposons que $f(1) = a > 1$. Soient $r_1, r_2 \in \mathbb{Q}$, avec $r_1 \leqslant r_2$. Notons $r = r_2 - r_1 \in Q \cap]0, +\infty[$
$f(r_2) = f(r_1 + r) = f(r_1) \times f(r)$. Or $f(r) = a^r > 1$ car $a > 1$.
Donc $f(r_2) > f(r_1)$, ainsi f est croissante sur $\mathbb{Q}$.
De même si $f(1) < 1$.
□

Analyse - Comment définir $f(x)$ pour $x \in \mathbb{R}$
Il reste à étendre la définition pour des nombres $x \in \mathbb{R}$.
Considérons le développement décimal de x, il existe (on le démontrera plus tard) une suite d_n tel que pour tout $n \in \mathbb{N}$, $d_n \leqslant x < d_n + 10^{-n}$ avec $(d_n)_n$ croissante et $(d_n + 10^{-n})_n$ décroissante de limite x.
Supposons que $a > 1$.
La suite $(a^{d_n})_{n\in\mathbb{N}}$ est une suite croissante, majorée par a^{d_0+1}, elle converge.
On note $f(x) = a^x$, cette limite.
Exercice
On note $a = f(1)$. Montrer que pour tout $x \in \mathbb{R}$ et $r \in \mathbb{Q}$, $f(rx) = f(x)^r$.
Quelle formule obtient concernant les puissances de a ?

Correction
En reprenant pour $m \in \mathbb{Z}$, $f(mx) = (f(x))^m$, puis pour $r \in \mathbb{Q}$, $f(rx) = f(x)^r$.
On a donc $a^{rx} = (a^x)^r$. Puis en passant à la limite pour $(r_n) \to x'$: $a^{xx'} = (a^x)^{x'}$.

On résume et admet les derniers résultats (il nous manque la continuité) :

Pour aller plus loin - Suite décimale
Prenons un exemple pour mieux comprendre ici.
Considérons le nombre π, on a alors $\pi = 3,1415\ldots$.
Dans ce cas : $d_0 = 3$, $d_1 = 3,1$, $d_2 = 3,14$, $d_3 = 3,141\ldots$

Pour aller plus loin - Définition de a^x
Il faudrait démontrer que cette valeur ne dépend pas de la suite (d_n) choisie, convergente vers x.

Théorème - Fonctions exponentielles. Bilan
Les fonctions exponentielles non nulles sont continues.
Elles vérifient : $f(0) = 1$ et pour tout $x, y \in \mathbb{R}$, $f(x+y) = f(x) \times f(y)$ et $f(x \times y) = f(x)^y$.
Il existe $a(= f(1)) \in \mathbb{R}$ tel que $f(x) = a^x$ (par définition de a^x si $x \in \mathbb{R} \setminus \mathbb{Q}$).
Si $a > 1$, alors f est strictement croissante sur $\mathbb{R}$, avec $\lim\limits_{-\infty} f = 0$ et $\lim\limits_{+\infty} f = +\infty$.
Si $a < 1$, alors f est strictement décroissante sur $\mathbb{R}$, avec $\lim\limits_{-\infty} f = +\infty$ et $\lim\limits_{+\infty} f = 0$.

5.2. LA fonction exponentielle

Nous verrons que ces fonctions sont dérivables. L'une a la propriété essentielle de vérifier $f'(0) = 1$. C'est LA fonction exponentielle avec $a = e$ (LE « e »).
Prenons un autre définition.

Pour aller plus loin - Critère de convergence pour une suite réelle
Nous verrons, sans cercle vicieux, que toute suite de nombres réelles, majorée et croissante (à partir d'un certain rang) est convergente.
C'est une propriété caractéristique de $\mathbb{R}$.

Définition - La fonction exponentielle naturelle
Soit $x \in \mathbb{R}$. La suite $(x_n) = ((1 + \frac{x}{n})^n)$ est majorée, croissante à partir d'un certain rang, donc convergente.
Notons $\exp(x)$ la limite de (x_n).

Il faut démontrer la convergence de la suite :

Démonstration
• Positivité à partir d'un certain rang.
Pour tout réel x, notons que $\frac{x}{n} \to 0$ pour $n \to +\infty$.
Donc à partir d'un certain rang N_x tel que $\forall\, n \geqslant N_x$, $-\frac{1}{2} \leqslant \frac{x}{n} \leqslant \frac{1}{2}$.
Ainsi, pour tout $n \geqslant N_x$, $x_n > 0$. On notera plus simplement que ce rang N_x est $\max(0, \lceil -x \rceil)$.
• Croissance (à partir d'un certain rang)
On peut utiliser le critère d'une suite positive (à partir d'un certain rang) : par comparaison relative à 1).

$$\frac{x_{n+1}}{x_n} = \left(1+\frac{x}{n}\right)\left(\frac{\frac{n+1+x}{n+1}}{\frac{n+x}{n}}\right)^{n+1} = \left(\frac{n+x}{n}\right)\left(\frac{n^2+nx+n}{n^2+nx+n+x}\right)^{n+1}$$

$$\frac{x_{n+1}}{x_n} = \left(\frac{n+x}{n}\right)\left(1-\frac{x}{(n+1)(n+x)}\right)^{n+1}$$

Rappelons l'inégalité de Bernoulli : $(1+a)^m \leqslant 1 + ma$ si $a > -1$ et $m \in \mathbb{N}^*$.
Prenons alors $m \leftarrow n+1 (\in \mathbb{N}^*)$ et $a \leftarrow -\dfrac{x}{(n+1)(n+x)}$.
On a bien : $a > -1$, car :
• si $x \leqslant 0$, $x < n+x$ donc $x < (n+1)(n+x)$ dès que $n > 0$.
• si $x < 0$, $-x > 0$ et $(n+1)(n+x) > 0$ dès que $n > -x$, i.e. $n \in N_x$.
Donc :

$$\left(1-\frac{x}{(n+1)(n+x)}\right)^{n+1} \leqslant 1 + (n+1)\frac{-x}{(n+1)(n+x)} = \frac{n}{n+x}$$

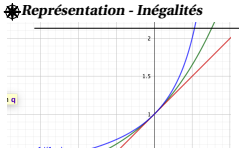
Enfin, comme $\dfrac{n+x}{n} \leqslant 0$, le sens de l'inégalité est inchangé :

$$\frac{x_{n+1}}{x_n} \leqslant \frac{n+x}{n} \times \frac{n}{n+x} = 1$$

• Majoration.
Soit $s = \lfloor |x| \rfloor + 1 \in \mathbb{N}$, donc $\frac{x}{sn} \in]-\frac{1}{n}, \frac{1}{n}[$.

$$x_{sn} = \left(\left(1+\frac{x}{sn}\right)^n\right)^s \leqslant \left(\frac{1}{1-n\frac{x}{sn}}\right)^s = \left(\frac{s}{s-x}\right)^s \text{ (constante en } n).$$

(La fonction $t \mapsto t^s$ est croissante sur $\mathbb{R}_+$.)
Soit $m \geqslant \max(N_x, N'_x)$, et $n = \lfloor \frac{m}{s} \rfloor + 1$
on a $n \geqslant \frac{m}{s}$, donc $N'_x \leqslant m \leqslant ns$.
puis par croissance de (x_n) pour tout $m \geqslant N'_x$: $x_m \leqslant x_{ns} \leqslant \left(\dfrac{s}{s-x}\right)^s$ □

Représentation - Inégalités


Proposition - Inégalités

On a pour tout $x \in]-1,1[$, $1+x \leqslant \exp x \leqslant \dfrac{1}{1-x}$.

Remarque - Elargissement de l'intervalle

En fait, le résultat est vrai pour tout $x \in \mathbb{R}$ pour la première inégalité et sur $]-\infty,1[$ pour la seconde.
Mais en réalité, elles nous serviront surtout pour x proche de 0, où les trois termes valent 1…

Démonstration

On applique les inégalités de Bernoulli, à partir d'un certain rang, puisque $\frac{x}{n} \to 0$ ($\frac{x}{n} < \frac{1}{n}$) :

$$1+x = 1+n\frac{x}{n} \leqslant \left(1+\frac{x}{n}\right)^n = x_n \leqslant \frac{1}{1-n\frac{x}{n}} = \frac{1}{1-x}$$

On passe ensuite à la limite : à gauche et à droite les termes sont constants. Au centre, la suite converge vers e^x. □

Théorème - exp est une fonction exponentielle.

La fonction $x \mapsto \exp x$ est une fonction exponentielle appellée LA fonction exponentielle.

On a donc pour tout $x \in \mathbb{R}$, $\exp(x) = e^x$ où $e = \exp(1) = \lim\limits_{n\to+\infty}\left(1+\dfrac{1}{n}\right)^n$

Elle vérifie donc : $\forall\, x, y \in \mathbb{R}$, $\exp(x+y) = e^{x+y} = e^x e^y = \exp(x) \times \exp(y)$ et $\exp(x \times y) = e^{xy} = (e^x)^y = (\exp(x))^y$.

Démonstration

Plus compliqué. Soient $x, y \in \mathbb{R}$.
Notons $x_n = \left(1+\frac{x}{n}\right)^n$, $y_n = \left(1+\frac{y}{n}\right)^n$ et $z_n = \left(1+\frac{x+y}{n}\right)^n$.

Alors $\dfrac{x_n y_n}{z_n} = \dfrac{\left(1+\frac{x}{n}+\frac{y}{n}+\frac{xy}{n^2}\right)^n}{\left(1+\frac{x+y}{n}\right)^n} = \left(1+\dfrac{t_n}{n}\right)^n$,

avec $t_n = \dfrac{xy}{n+x+y} \to 0$ pour $n \to +\infty$.

Il existe donc une valeur N tel que pour tout $n \geqslant N$, $t_n \in [-\frac{1}{2}, \frac{1}{2}]$, donc $\frac{t_n}{n} \in \subset [-\frac{1}{n}, \frac{1}{n}] \subset [-1, \frac{1}{n}[$
On a alors $1+t_n \leqslant \dfrac{x_n y_n}{z_n} \leqslant \dfrac{1}{1-t_n}$ et donc par unicité des limites : $\dfrac{\exp(x)\exp(y)}{\exp(x+y)} = \lim \dfrac{x_n y_n}{z_n} = 1$.
Donc $\exp(x+y) = \exp(x)\exp(y)$.
exp est une fonction exponentielle. □

Application - Evaluation approchée de $(1+\frac{1}{30})^{100}$

Si l'on considère $n = 100$ proche de l'infini, on a donc

$$\left(1+\frac{1}{30}\right)^{100} = \left(1+\frac{\frac{10}{3}}{100}\right)^{100} \approx \exp\left(\frac{10}{3}\right)$$

On vérifie à la calculatrice : $\exp\frac{10}{3} = 28,03162$ et $(1+\frac{1}{30})^{100} = 26,548739$.

Analyse - Binôme de Newton pour $(1+\frac{1}{n})^n$ et une approximation d'Euler

L'argument d'Euler, à partir du binôme de Newton donne :

$$\begin{aligned}(1+\frac{1}{n})^n &= \sum_{k=0}^{n}\binom{n}{k}\frac{1}{n^k} = 1+\frac{n}{n}+\frac{n(n-1)}{2!n^2}+\frac{n(n-1)(n-2)}{3!n^3}+\dots\\ &= 1+1+\frac{1(1-\frac{1}{n})}{2!}+\frac{1(1-\frac{1}{n})(1-\frac{2}{n})}{3!}+\dots\end{aligned}$$

Euler ajoute : « *si n est un nombre plus grand qu'aucune quantité assignable, la fraction $\frac{n-1}{n}$ égalera l'unité* » et conclue par $e = 1+1+\frac{1}{2!}+\frac{1}{3!}+\dots$.
La méthode laisse à désirer, mais le résultat est juste :

Histoire - D'où vient la notation e ?

Leonard EULER *(1707-1783) est le mathématicien le plus prolixe de l'histoire (avec Cauchy?).*
C'est un calculateur de génie, doté d'une mémoire prodigieuse (hypemnésique).



Proposition - Formules d'Euler (1746)

$$e = \lim_{n\to+\infty}\left(1+\frac{1}{n}\right)^n = \sum_{k=0}^{+\infty}\frac{1}{k!}$$

Et pour tout $x \in \mathbb{R}$,

$$e^x = \lim_{n\to+\infty}\left(1+\frac{x}{n}\right)^n = \sum_{k=0}^{+\infty}\frac{x^k}{k!}$$

5.3. LogarithmeS

Les fonctions exponentielles non constante égale à 0 ou 1 sont continues et strictement monotone, elles admettent donc une fonction réciproque.

Histoire - Neper

L'écossais John Napier (1550-1617) (ou Neper) cherche au XV siècle une fonction qui faciliterait les calculs : elle transformerait le produit (compliqué car beaucoup de calculs) en addition (moins de calculs).
Il trouve le logarithme.
On a donc $\ln(ab) = \ln a + \ln b$.
L'histoire peut être un moyen mnémotechnique.



Définition - Fonctions logarithmes

On appelle fonctions logarithmes toute fonctions g réciproques de fonctions exponentielles f non constantes.
Si cette dernière est $x \mapsto a^x$ (avec $a \notin \{0,1\}$), alors la fonction logarithme est qualifiée « de base a ». On note souvent $g = \log_a$ ou $\ln_a$.
Elle est définie sur $\mathbb{R}_+$, à valeurs dans $\mathbb{R}$ et vérifie alors

$\forall\, x, y \in \mathbb{R}_+$, $g(x \times y) = g(x) + g(y)$.

Exemple - Différents logarithmes bien connus

Le logarithme en base 10 est un classique de la physique.
Il indique en gros la taille en nombre de chiffres.
Le logarithme en base 2 est un classique de l'informatique.

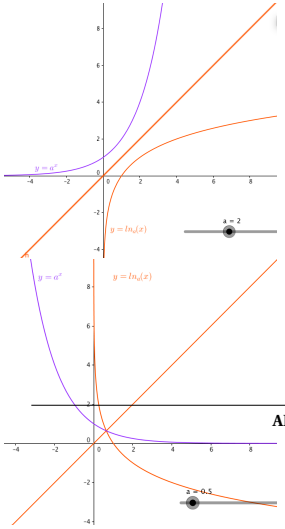
Démonstration

L'existence de g est liée à la bijectivité de f.
f étant à valeurs dans $\mathbb{R}_+$, on a pour tout $X = f(x) \in \mathbb{R}_+$ (x existe bien, c'est $g(X)$) et $Y = f(y) \in \mathbb{R}_+$: $g(X \times Y) = g(f(x) \times f(y)) = g(f(x+y)) = x+y = g(X) + g(Y)$. □

Théorème - Fonctions logarithmes. Bilan

Les fonctions logarithmes sont continues, définies sur $\mathbb{R}_+^*$, à valeurs dans $\mathbb{R}$.
Elles vérifient : $g(1) = 0$ et pour tout $x, y, t \in \mathbb{R}_+$, $g(x \times y) = g(x) + g(y)$ et $g(x^t) = t \times g(x)$.
Il existe $a (= f(1)) \in \mathbb{R}$ tel que $g(a) = 1$.
Si $a > 1$, alors g est strictement croissante sur $\mathbb{R}$, avec $\lim\limits_{0} g = -\infty$ et $\lim\limits_{+\infty} g = +\infty$.
Si $a < 1$, alors g est strictement décroissante sur $\mathbb{R}$, avec $\lim\limits_{0} g = +\infty$ et $\lim\limits_{+\infty} f = -\infty$.

Représentation - Exponentielles et logarithmes selon la valeur de a



Démonstration

Faisons juste la démonstration de $g(x^t)$:
On sait, pour $X = g(x)$ que : $f(t \times X) = f(X)^t$, i.e. $f(t \times g(x)) = x^t$. Puis en composant par g : $t \times g(x) = g(x^t)$. □

Savoir faire - Calculer « à la main » le logarithme en base a de x ?

On n'a pas d'autre solution (pour le moment) mais cela est suffisant (compte-tenu de la contrainte que l'on s'est donné) de procéder par dichotomie.
On regarde la suite (a^n) et l'on trouve $n \in \mathbb{N}$ tel que $a^n \leqslant x < a^{n+1}$.
Puis, on sélectionne $a_0 = n$ et $b_0 = n+1$. Puis on peut (par exemple), considérer $c = \frac{a_0+b_0}{2} \in \mathbb{Q}$, évaluer a^c.
Si $a^c < x$, on prend $a_1 = c$ et $b_1 = b_0$, sinon on prend $a_1 = a_0$ et $b_1 = c$…

On a deux suites adjacentes (a_n) et (b_n) convergente vers y avec $a^y = x$, donc $y = \log_a(x)$.

Définition - Le logarithme naturel
La fonction logarithme réciproque de la fonction exponentielle, donc le logarithme en base $e = \exp 1$ est appelé logarithme naturel.
On le note ln.
ln est définie, continue et croissante sur $\mathbb{R}_+$, à valeurs dans $\mathbb{R}$.
Numériquement : $\ln(1) = 0$, $\ln e = 1$, $\lim_0 \ln = -\infty$ et $\lim_{+\infty} \ln = +\infty$.
On a les propriétés algébrique : $\ln(ab) = \ln a + \ln b$, $\ln(a^b) = b \ln a \ldots$
On a pour tout $u \in \mathbb{R}_+^*$, $\ln u \leqslant u - 1$.

Histoire - Logarithme naturel
Il y a un abus historique ici.
On a démontré historiquement qu'il s'agit bien du logarithme naturel en le définissant comme primitive de $x \mapsto \frac{1}{x}$ (primitive dont on a démontré qu'il s'agissait d'un logarithme (Fermat - 1636)). C'est le naturel car $\ln'(1) = 1$.
La définition donnée ici vient de Euler (un siècle plus tard)

Tout est immédiat, sauf l'inégalité qu'on démontre :

Démonstration
On sait que pour tout $x \in]-1, +\infty[\subset \mathbb{R}$, $1 + x \leqslant \exp(x)$.
En composant par ln, croissante : $\ln(1 + x) \leqslant x$.
Posons $u = 1 + x \in \mathbb{R}_+^*$: $\ln u \leqslant u - 1$
□

Proposition - Ecriture en fonction du logarithme naturel
Soit g la fonction logarithme de base a, réciproque de $f : x \mapsto a^x$.
Alors on a :
$$\forall\, x \in \mathbb{R},\ f(x) = a^x = \exp(x \times \ln a) \qquad \forall\, x \in \mathbb{R}_+,\ g(x) = \frac{\ln x}{\ln a}$$

Démonstration
Comme ln est un logarithme : $\exp(x \ln a) = \exp(\ln a^x) = a^x$, car ln est réciproque de exp.
Puis, $G : x \mapsto \frac{\ln x}{\ln a}$ est une fonction logarithme
$$G(x \times y) = \frac{\ln(xy)}{\ln a} = \frac{\ln x + \ln y}{\ln a} = G(x) + G(y)$$
de base a, car $G(a) = \frac{\ln a}{\ln a} = 1$. Donc $G = g$ □

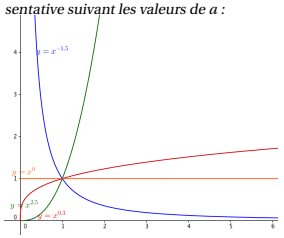
5.4. Retour sur les fonctions puissances, avec un exposant non rationnel

Définition - Fonction puissance réelle
Pour $\alpha \in \mathbb{R}$, on définit sur $]0, +\infty[$ la fonction puissance α par :
$$\begin{array}{rccc} g_\alpha : &]0,+\infty[& \to & \mathbb{R} \\ & x & \mapsto & x^\alpha = \exp(\alpha \ln x) \end{array}$$

Proposition - Fonction puissance réelle
Elle vérifie les propriétés suivantes :
$\forall (x, y) \in]0, +\infty[^2$, $\forall (\alpha, \beta) \in \mathbb{R}^2$,
- $(xy)^\alpha = x^\alpha y^\alpha$
- $x^{\alpha+\beta} = x^\alpha x^\beta$
- $(x^\alpha)^\beta = x^{\alpha\beta}$
- Si $\alpha = 0$, g_α est constante égale à 1.
- Si $\alpha > 0$, g_α est croissante et $\lim_{x \to 0^+} g_\alpha(x) = 0$
- Si $\alpha < 0$, g_α est décroissante et $\lim_{x \to 0^+} g_\alpha(x) = +\infty$

Pour $\alpha > 0$, on étudie l'existence d'une demi-tangente en 0 :
- Si $\alpha < 1$, la courbe $y = g_\alpha(x)$ admet une tangente verticale en 0.
- Si $\alpha = 1$, la courbe $y = g_\alpha(x)$ admet une tangente de pente 1 en 0.
- Si $\alpha > 1$, la courbe $y = g_\alpha(x)$ admet une tangente horizontale en 0.

Représentation - Fonctions puissances réelles (différentes valeurs de α)
On en déduit les variations et la courbe représentative suivant les valeurs de a :



5.5. Croissances comparées

Heuristique - Logarithme comme nombre de chiffres
Commençons par une remarque, avec $x = 10^n$, on a $\frac{\ln(x)}{x} = n10^{-n} \ln 10 \underset{n \to +\infty}{\longrightarrow} 0$.
Notons que $\ln 10 \approx 2{,}302$, donc $\ln x = \ln(10) \times \log_{10}(x)$ et que $\log_{10}(x)$ est en première approximation le nombre de chiffres de x, alors pour x grand, $\ln x$ est le nombre de chiffres de x multiplié par un peu plus de 2.
Exemple : $\ln(123456789) \approx 2{,}3 \times \log(1{,}23 \times 10^9) = 2{,}3 \times (9 + \ln(1{,}23)) \approx 20$, ce qui est petit

Il s'agit, a priori, de formes indéterminées. Elles sont levées :

Théorème - Croissance comparée
Soient a et b deux réels strictement positifs. On a
$$\lim_{x \to +\infty} \frac{(\ln x)^b}{x^a} = 0; \quad \lim_{x \to 0^+} x^a |\ln x|^b = 0;$$
$$\lim_{x \to +\infty} \frac{e^{ax}}{x^b} = +\infty; \quad \lim_{x \to -\infty} |x|^b e^{ax} = 0.$$

Démonstration
On commence par lever l'indétermination de $\frac{\ln(x)}{x}$ en $+\infty$. Tout en découlera…
Commençons par une remarque, avec $x = 10^n$, on a $\frac{\ln(x)}{x} = n10^{-n} \ln 10 \underset{n \to +\infty}{\longrightarrow} 0$.
On sait que pour tout $x > 0$, $\ln x \leqslant x - 1 < x$,
en particulier $\frac{1}{2} \ln x = \ln(\sqrt{x}) < \sqrt{x}$.
Donc, pour $x > 1$: $0 < \frac{\ln x}{x} < \frac{2\sqrt{x}}{x} = \frac{2}{\sqrt{x}}$. Par encadrement : $\lim_{x \to +\infty} \frac{\ln x}{x} = 0$.
Pour $a, b > 0$,
$$\frac{(\ln x)^b}{x^a} = \left(\frac{\frac{b}{a} \ln(x^{a/b})}{x^{a/b}} \right)^b \underset{x \to +\infty}{\longrightarrow} 0$$
par composition de limites : avec $u = x^{a/b}$, puis $v \mapsto v^b$.
Avec cette nouvelle limite, en composant avec $x : t \mapsto \frac{1}{t}$,
$$x^a |\ln x|^b = \frac{|-\ln t|^b}{t^a} \underset{\substack{t \to +\infty \\ x \to 0}}{\longrightarrow} 0$$
Avec la première limite, en composant avec $x : t \mapsto \ln(t)$ i.e. $t = e^x$,
$$\frac{e^{ax}}{x^b} = \frac{t^a}{(\ln t)^b} \underset{\substack{t \to +\infty \\ x \to +\infty}}{\longrightarrow} +\infty$$
Avec la deuxième limite, en composant avec $x : t \mapsto \ln(t)$ i.e. $t = e^x$,
$$|x|^b e^{ax} = |\ln t|^b t^a \underset{\substack{t \to 0 \\ x \to -\infty}}{\longrightarrow} 0$$
□

Exercice
Fixons $a, b \in \mathbb{R}_+^*$.
Montrer que pour x grand : $e^{\frac{a}{b+1}x} \geqslant \frac{a}{b+1} x$, en déduire $\frac{e^{ax}}{x^b} \geqslant \left(\frac{a}{b+1} \right)^{b+1} x$.
Conclure sur la valeur de $\lim_{x \to +\infty} \frac{e^{ax}}{x^b}$.

Correction

5.6. Fonctions hyperboliques directes

Définition - Fonctions hyperboliques
Les fonctions ch (cosinus hyperbolique), sh (sinus hyperbolique) et th (tangente hyperbolique) sont définies sur $\mathbb{R}$ par :

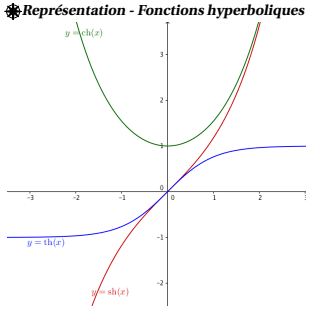
$$\operatorname{ch} x = \frac{e^x + e^{-x}}{2}, \quad \operatorname{sh} x = \frac{e^x - e^{-x}}{2}, \quad \operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x} = \frac{e^x - e^{-x}}{e^x + e^{-x}}.$$

Proposition - Fonctions hyperboliques
La fonction ch est paire, les fonctions sh et th sont impaires.

$\operatorname{ch}(-x) = \operatorname{ch} x$ $\quad$ $\operatorname{sh}(-x) = -\operatorname{sh} x$
$\operatorname{ch}^2 x - \operatorname{sh}^2 x = 1$
$\operatorname{ch} x + \operatorname{sh} x = e^x$ $\quad$ $\operatorname{ch} x - \operatorname{sh} x = e^{-x}$
$\operatorname{ch}(a+b) = \operatorname{ch} a \operatorname{ch} b + \operatorname{sh} a \operatorname{sh} b$ $\quad$ $\operatorname{sh}(a+b) = \operatorname{sh} a \operatorname{ch} b + \operatorname{ch} a \operatorname{sh} b$
$\operatorname{th}(a+b) = \frac{\operatorname{th} a + \operatorname{th} b}{1 + \operatorname{th} a \operatorname{th} b}$

Démonstration
$\operatorname{ch}^2(x) - \operatorname{sh}^2(x) = \frac{1}{4}(e^{2x} + 2 + e^{-2x} - e^{2x} + 2 - e^{-2x}) = 1.$
$\operatorname{ch} x + \operatorname{sh} x = \frac{1}{2}(e^x + e^{-x} + e^x - e^{-x}) = e^x$ et $\operatorname{ch} x - \operatorname{sh} x = \frac{1}{2}(e^x + e^{-x} - e^x + e^{-x}) = e^{-x}$
$\operatorname{ch} a \operatorname{ch} b + \operatorname{sh} a \operatorname{sh} b = \frac{1}{4}((e^a + e^{-a})(e^b + e^{-b}) + (e^a - e^{-a})(e^b - e^{-b})) = \frac{1}{4}(e^{a+b} + e^{a-b} + e^{-a+b} +$
$e^{-a-b} + e^{a+b} - e^{a-b} - e^{-a+b} + e^{-a-b}) = \frac{1}{2}\left(e^{a+b} + e^{-(a+b)}\right) = \operatorname{ch}(a+b).$ □

Représentation - Fonctions hyperboliques



6. Sommes numériques infinies

On commence par une extension de notation :

Définition - Extension du coefficient binomial
Pour $\alpha \in \mathbb{R}$ et $k \in \mathbb{N}$, on note :

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!}$$

La section suivante donne des résultats connus pour l'essentiel depuis le XVIII siècle, au moins.
Mais les démonstrations satisfaisantes sont plus tardives (ABEL et successeurs du XIX).
Pour vous, elles auront officiellement lieu l'année prochaine lorsque vous verrez le cours sur les séries entières.

Proposition - Egalités sommatoires
On a les égalités suivantes :

$x \in ?$	fonction	somme	Auteur (Année)
$\mathbb{R}$	$\sin(x)$	$= \sum_{k=0}^{+\infty} \frac{(-1)^k}{(2k+1)!} x^{2k+1}$	NEWTON(1669), LEIBNIZ(1691)
$\mathbb{R}$	$\cos(x)$	$= \sum_{k=0}^{+\infty} \frac{(-1)^k}{(2k)!} x^{2k}$	NEWTON(1669), LEIBNIZ(1691)
$\mathbb{R}$	$\tan(x)$	$= x + \frac{1}{3}x^3 + \frac{2}{5}x^5 + \frac{17}{315}x^7 + \dots$	JAC. BERNOULLI(1702)
$[-1,1]$	$\arctan(x)$	$= \sum_{k=0}^{+\infty} \frac{(-1)^k}{2k+1} x^{2k+1}$	GREGORY(1671), LEIBNIZ(1674)
$[-1,1]$	$\arcsin(x)$	$= x + \frac{1}{2}\frac{x^3}{3} + \frac{1\cdot 3}{2\cdot 4}\frac{x^5}{5} + \dots$	NEWTON(1669)
$\mathbb{R}$	$(1+x)^n$	$= \sum_{k=0}^{n} \binom{n}{k} x^k$	PASCAL(1654)
$]-1,1[$	$(1+x)^\alpha$	$= \sum_{k=0}^{+\infty} \binom{\alpha}{k} x^k$	NEWTON(1666)
$\mathbb{R}$	$\exp(x)$	$= \sum_{k=0}^{+\infty} \frac{1}{k!} x^k$	EULER(1748)
$]-1,1[$	$\ln(1+x)$	$= \sum_{k=1}^{+\infty} \frac{(-1)^{k-1}}{k} x^k$	MERCATOR(1668)
$\mathbb{R}$	$\operatorname{sh}(x)$	$= \sum_{k=0}^{+\infty} \frac{1}{(2k+1)!} x^{2k+1}$	EULER(1748)
$\mathbb{R}$	$\operatorname{ch}(x)$	$= \sum_{k=0}^{+\infty} \frac{1}{(2k)!} x^{2k}$	EULER(1748)

Pour aller plus loin - Produit infini
Euler démontre également (1748) :

$$\forall\, x \in \mathbb{R}, \sin x = x \prod_{k=1}^{+\infty} \left(1 - \frac{x^2}{k^2\pi^2}\right)$$

Exercice
Donner l'expression formalisée de $\arcsin(x)$.

Correction
$\arcsin(x) = \sum_{k=0}^{+\infty} \frac{(2k)!}{2^{2k}k!^2} \frac{x^{2k+1}}{2k+1}$

Exercice
On rappelle la formule de MACHIN : $\frac{\pi}{4} = 4\arctan\frac{1}{5} - \arctan\frac{1}{239}$.
Combien de calcul pour obtenir 10 décimales de π satisfaisantes ? Faites les à la calculatrice

Correction
$\frac{1}{5} = 0.2$, et donc $\left(\frac{1}{5}\right)^n = 2^n \times 10^{-n}$.
Avec $n = 10$, on a $2^10 \approx 10^3$ et donc $\left(\frac{1}{5}\right)^n \approx 10^{3-10} = 10^{-7}$.
Avec $n = 14$, cela doit être suffisant…

7. Bilan

Synthèse

- ⇝ On s'intéresse aux fonctions dont le domaine est dans $\mathbb{R}$. Beaucoup de définitions : images, restrictions, ou additions, multiplications et compositions de fonctions. Des adjectifs pour les fonction : périodiques, paires ou impaires, majorées, minorées, bornées, monotone, strictement croissante…
- ⇝ Plusieurs fonctions de référence sont à connaître : exponentielle(s) et logarithme(s) en toute base ; les fonctions puissances ; les fonctions circulaires (sin, arccos…) et hyperboliques directes. On doit savoir

comment comparer ces fonctions lorsqu'elles sont en compétition au voisinage de point problématique.

⇝ Les fonctions complexes de la variables réelles s'étudient de la même façon (même si la représentation est plus complexe). En fait, ce qui compte, c'est la nature de la variable « de départ ».

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Transférer un problème logarithme « en a », vers « en 1 »
— Savoir-faire - Transférer un problème trigonométrique « en a », vers « en 0 »
— Savoir-faire - Etude d'une équation fonctionnelle de $\mathbb{N}$ à $\mathbb{R}$
— Savoir-faire - Calculer « à la main » le logarithme en base a de x ?

Retour sur les problèmes

12. C'est l'application $x \mapsto 2^x u_0 = u_0 e^{x\ln 2}$
13. Les seules applications de cette forme sont les applications $x \mapsto A\ln(x)$ (où A est constante).
Elles sont définie sur $\mathbb{R}_+$. Peut-on les étendre sur $\mathbb{R}$ en entier?
Si $x > 0$, $\ln(-x) = \ln(e^{i\pi}x) = \ln x + i\pi[2\pi]\ldots$
14. On vient de terminer ce chapitre en répondant à cette question.

Chapitre 4

Ensemble des nombres complexes

Résumé -

Dans ce chapitre, nous reprenons des résultats de lycée sur les nombres complexes et leur lien avec la géométrie du plan. Ce sont des bons outils pour reprendre les propriétés trigonométriques!
Comme, ces nombres ont été inventés/découverts pour résoudre tout type d'équation polynomiale, il est normal que ce chapitre soit associé à la recherche des solutions de $x^n = 1$, i.e. la recherche des racines de l'unité.
Puis nous nous intéressons aux transformations géométriques du plan. Lorsque l'espace géométrique étudié est de dimension 2 (plan $\mathbb{R}^2$), les nombres complexes sont de parfaits outils pour faire cette étude. En effet, ces nombres ont un lien fort avec la géométrie (revue au chapitre suivant) : addition de complexes = translation et multiplication de complexes = homothétie et rotation (similitude)…

- *Micmath - La conjugaison complexe est un automorphisme de corps. https ://www.youtube.com/watch ?v=AVDMpnwsztg*
- *Les maths en finesse - Racines nieme de l'unité. https ://www.youtube.com/watch ?v=aZLGdnktO8k*
- *Exo7Math - Nombres complexes part.4 : géométrie .https ://www.youtube.com/watch ?v=ej9zpQYsQs8*
- *AEV - Nombres complexes / Applications à la géométrie. https ://www.youtube.com/watch ?v=HfxqAQ1SiGo*

Sommaire

1. Problèmes 64
2. EULER : manipulateur des nombres du diable 64
2.1. Racine de polynômes 64
2.2. Calcul algébrique 65
2.3. Représentation graphique (addition et longueur) . . 67
2.4. Inégalités 67
3. Le visionnaire : GAUSS et la multiplication complexe . . . 68
3.1. Les complexes de module 1 68
3.2. Notation exponentielle 69
3.3. Formules d'Euler et de de Moivre 71
3.4. Argument, forme trigonométrique 73
4. Racines d'un nombre complexe 74
4.1. Recherche de racines carrées 74
4.2. Racines n-ièmes de l'unité 75
4.3. Racines n-ièmes d'un nombre complexe 76
5. $\mathbb{R}^2 = \mathbb{C} = \mathscr{P}$ 77
5.1. Regard géométrique sur le plan complexe 77
5.2. Lignes de niveau 78
5.3. Transformations du plan (point de vue complexe) . 80

6. Bilan 84

1. Problèmes

Problème 15 - Multiplication de nombres

Que représente la multiplication complexe $Z = z \times z'$ pour des points $M(z)$ et $M'(z')$.
En particulier, existe-t-il un algorithme géométrique pour tracer cette multiplication?
On pourra dans un premier temps, considérer que $z \in \mathbb{R}$, $z \in \mathbb{U}$

Problème 16 - Théorème de Napoléon

En exploitant les nombres complexes, démontrer le théorème de Napoléon :
Si nous construisons trois triangles équilatéraux à partir des côtés d'un triangle quelconque, tous à l'extérieur ou tous à l'intérieur, les centres de ces triangles équilatéraux forment eux-mêmes un triangle équilatéral.
Beaucoup de problèmes (théorème de Ptolémée, théorème de Cotes…), du plan se démontre par *calculs* avec des nombres complexes.

Problème 17 - Transformation du plan

A l'aide des nombres complexes, comment trouver toutes les transformations du plan qui conserve les longueurs et/ou les angles?

Problème 18 - Application en physique

On connait beaucoup d'applications en physique des nombres complexes (notés j), en particulier en électricité ou pour l'étude de Fourier.
La loi de Snell-Descartes donne pour la réfraction entre deux milieux d'indices n_1 et n_2 : $n_1 \sin\theta_1 = n_2 \sin\theta_2$.
Lorsque $n_1 > n_2$ et θ_1 proche de 0 (donc $\sin\theta_1$ proche de 1), on trouve $\sin\theta_2 = \dfrac{n_1}{n_2}\sin\theta_1 > 1$, et donc $\cos\theta_2 \in \mathbb{C}$.
Avec ce nombre complexe, Augustin FRESNEL unifiait en une seule formule ce qui se présentait jusqu'alors sous deux formes. Quelle est cette formule?

2. EULER : manipulateur des nombres du diable

2.1. Racine de polynômes

Histoire - Citation

« Au reste tant les vrayes racines que les fausses ne sont pas tousiours reelles ; mais quelques seulement imaginaires ; c'est à dire qu'on peut bien touiours en imaginer autant que iay dit en chasque Equation ; mais qu'il n'y a quelquefois aucune quantité, qui corresponde a celles qu'on imagine. » DESCARTES *(1637)*

Analyse - Problème de Cardan (1545)

Un segment de longueur 10 est coupé en deux parties de longueur a et b. De quelle manière le faire, de sorte que l'aire du rectangle dont chaque côté vaut a et b puisse valoir 40?
On a les équations $a+b=10$ et $a \times b = 40$, donc $a^2 - 10a = a(a-10) = a \times b = 40$.
Les racines de cette équation $x^2 - 10x - 40 = 0$ est $5+\sqrt{-15}$ et $5-\sqrt{-15}$.
Evidemment cela est problématique (racine d'un nombre négatif) sauf que

- $(5+\sqrt{-15}) + (5-\sqrt{-15}) = 10$

— $(5+\sqrt{-15})\times(5-\sqrt{-15}) = 5^2-(-15) = 25+15 = 40$

La solution fonctionne avec ces nouveaux nombres, à condition de garder les même règles de calcul qu'avec les nombres classiques…
Les règles de calcul sont donnés par Raphaël Bombelli (1572), dans son algebra. Pendant deux siècles les mathématiciens se querellent quant à leur existence et à leurs emplois.

Exercice
On reprend un exercice historique de Bombelli.
En reprenant les règles classiques de calcul, évaluer $(2+\sqrt{-1})^3$.
En employant les formules de Cardan, trouver les racines de $x^3 = 15x+4$.

Correction
Binôme de Newton : $(2+\sqrt{-1})^3 = 2^3+3\sqrt{-1}\times 2^2+3(\sqrt{-1})^2\times 2+(\sqrt{-1})^3 = 8+12\sqrt{-1}-6-\sqrt{-1} = 2+11\sqrt{-1}$.

2.2. Calcul algébrique

Euler invente la notation i bien pratique et les manipule avec précision. Il écrit à Diderot : « $e^{i\pi} = -1$ donc Dieu existe ».

Remarque - Unicité
Un complexe est un « nombre » z qui s'écrit $z = a+ib$ où a et b sont des réels et i vérifie $i^2 = -1$. Cette écriture est unique et s'appelle la forme algébrique de z.

Comme la construction de $\mathbb{C}$ n'est pas donnée, il n'est pas possible de démontrer l'unicité de l'écriture de z, ni la justification des règles de calcul. Nous les admettons alors. Ce n'est pas rien…

Pour aller plus loin - Construction de $\mathbb{C}$
Rassurons nous : nous construirons bien $\mathbb{C}$ *par la suite, selon la méthode proposée par Cauchy (avec des classes d'équivalence).*

Définition - Notation de nombre complexe (1748)
Soit $z = a+ib$ un complexe (a et b sont des réels).
$a = \mathrm{Re}\, z$ s'appelle la **partie réelle** de z.
$b = \mathrm{Im}\, z$ s'appelle la **partie imaginaire** de z ;
z est dit **imaginaire pur** *($z \in i\mathbb{R}$) si sa partie réelle est nulle.*
$\overline{z} = a-ib$ s'appelle le **conjugué** de $z = a+ib$.
$|z| = \sqrt{a^2+b^2}$ s'appelle le **module** de z.

Notons tout de suite comment se comportent les calculs habituelles addition et multiplication sur $\mathbb{C}$ (il s'agit presque de définition ici…)

Définition - (et proposition ?) $\mathbb{C}$ est un corps
Pour tout $(z,z') \in \mathbb{C}^2$, $\lambda, \lambda' \in \mathbb{R}$,
— $\mathrm{Re}(\lambda z+\lambda' z') = \lambda \mathrm{Re}(z)+\lambda' \mathrm{Re}(z')$ (*la partie réelle est $\mathbb{R}$-linéaire sur $\mathbb{C}$*)
— $\mathrm{Im}(\lambda z+\lambda' z') = \lambda \mathrm{Im}(z)+\lambda' \mathrm{Im}(z')$ (*la partie imaginaire est $\mathbb{R}$-linéaire sur $\mathbb{C}$*)
— si $z = a+ib$ et $z' = a'+ib'$, alors $z\times z' = (aa'-bb')+i(ab'+a'b)$
En particulier $z\times\overline{z} = a^2+b^2 = |z|^2 = |\overline{z}|^2$, donc $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$.

Remarque - Importance du conjugué
Le fait que $z\overline{z}$ est un nombre réel (pur) explique l'importance de la notion de conjugué.

Démonstration
Comme
$$\lambda z+\lambda' z' = (\lambda a+i\lambda b)+(\lambda' a'+i\lambda' b') = (\lambda a+\lambda' a')+i(\lambda b+\lambda' b')$$
Donc
$$\mathrm{Re}(\lambda z+\lambda' z') = \lambda \mathrm{Re}(z)+\lambda' \mathrm{Re}(z') \quad \text{et} \quad \mathrm{Im}(\lambda z+\lambda' z') = \lambda \mathrm{Im}(z)+\lambda' \mathrm{Im}(z')$$
Puis :
$$z\times z' = (a+ib)\times(a'+ib') = (aa'+iab'+iba'+i^2bb' = (aa'+bb')+i(ab'+a'b)$$
□

On a alors

Proposition - Conjugaison
On a les propriétés du conjugué :
$$\forall (z,z') \in \mathbb{C}^2,\ \forall a \in \mathbb{R},\quad \overline{\overline{z}} = z \qquad \overline{z+z'} = \overline{z}+\overline{z'}$$
$$\overline{zz'} = \overline{z}\,\overline{z'} \qquad \overline{\left(\frac{1}{z}\right)} = \frac{1}{\overline{z}}$$
$$\mathrm{Re}\, z = \frac{z+\overline{z}}{2} \qquad \mathrm{Im}\, z = \frac{z-\overline{z}}{2i}$$

Démonstration
Supposons que $z = a+ib$ et $z' = a'+ib'$. Alors
$$\overline{\overline{z}} = \overline{a-ib} = a+ib = z$$
$$\overline{z+z'} = \overline{(a+ib)+(a'+ib')} = \overline{(a+a')+i(b+b')} = (a+a')-i(b+b') = (a-ib)+(a'-ib') = \overline{z}+\overline{z'}$$
$$\overline{z\times z'} = \overline{(a+ib)\times(a'+ib')} = \overline{(aa'-bb')+i(ab'+a'b)} = (aa'-bb')-i(ab'+a'b) = (a-ib)\times(a'-ib') = \overline{z}\times\overline{z'}$$
$$\frac{1}{z} = \frac{1}{|z|^2}\overline{z} = \frac{1}{|\overline{z}|^2}\overline{\overline{z}} = \frac{1}{\overline{z}}\left(= \frac{z}{|z|^2}\right)$$
$$\frac{z+\overline{z}}{2} = \frac{2a+i0}{2} = a = \mathrm{Re}(z) \qquad \frac{z-\overline{z}}{2i} = \frac{0+2ib}{2i} = b = \mathrm{Im}(z)$$
□

Proposition - Puissance et conjugaison
On définit les puissances d'un nombre complexe par
$$\begin{cases} z^0 = 1 \\ \forall n \in \mathbb{N},\ z^{n+1} = z^n z \end{cases}$$
On a alors $\forall n \in \mathbb{N},\ \overline{z^n} = \overline{z}^n$.
Pour $z \neq 0$ et $n \in \mathbb{N}$, on pose $z^{-n} = \dfrac{1}{z^n} = (z^n)^{-1}$, on a alors $\forall n \in \mathbb{Z},\ \overline{z^n} = \overline{z}^n$.

Exercice
Faire la démonstration

Correction
Il faut faire une récurrence

Exercice
Démontrer la formule de Moivre (1707) : $(\cos a+i\sin a)^n = \cos(na)+i\sin(na)$.
(Il est compliqué de comprendre comment il a cette idée, au. hasard ?)

Correction
On le fait par récurrence.
Pour $n = 0$, on a bien $(\cos a+i\sin a)^0 = 1 = \cos 0+i\sin 0$.
Supposons que le résultat est vrai au rang n quelconque.
$(\cos a+i\sin a)^{n+1} = (\cos(na)+i\sin(na))(\cos a+i\sin a) = (\cos(na)\cos a-\sin(na)\sin a)+i(\cos(na)\sin a+\sin(na)\cos a)) = \cos((n+1)a)+i\sin((n+1)a)$

Proposition - Propriétés du module
On a les propriétés du module :
$$\forall (z,z') \in \mathbb{C}^2,\quad |z| = \sqrt{z\overline{z}} \qquad |zz'| = |z|\,|z'|$$
$$|z| = |\overline{z}| = |-z| \qquad \left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}\ (\text{si } z' \neq 0)$$

Démonstration
Les deux premiers résultats ont été démontrés. Puis
$$|zz'| = \sqrt{(zz')\overline{(zz')}} = \sqrt{zz'\overline{z}\overline{z'}} = \sqrt{z\overline{z}}\sqrt{z'\overline{z'}} = |z||z'|$$
$$|z| = \left|z'\times\frac{z}{z'}\right| = |z'|\times\left|\frac{z}{z'}\right|$$
Il ne reste plus qu'à diviser par $|z'|$. □

Remarque - Valeur absolue et module
Pour un réel, valeur absolue et module coïncident !

2.3. Représentation graphique (addition et longueur)

On munit le plan d'un repère orthonormé direct $(0,\vec{u},\vec{v})$. Le point M de coordonnées (a,b), caractérisé par $\overrightarrow{OM} = a\vec{u} + b\vec{v}$, peut alors être représenté par le complexe $z = a + ib$.

Définition - Affixe d'un point. Affixe d'un vecteur
$z = a+ib$ est alors appelé **affixe** du point $M(a,b)$, on peut noter $z = \text{Aff}(M)$.
Réciproquement, le point M est appelé (point) image de z.
De même, si $\vec{w}$ est un vecteur de coordonnées (a,b), $a+ib$ est appelé affixe de $\vec{w}$ (noté $\text{Aff}(\vec{w})$), lui-même appelé (vecteur) image du complexe $a+ib$.

Remarque - Axes
Les points de l'axe des abscisses correspondent aux points d'affixe réelle.
Les points de l'axe des ordonnés correspondent aux points d'affixe imaginaire pure.

Proposition - Opération complexe et correspondance sur le plan géométrique
Si z est l'affixe de M alors $\overline{z}$ est l'affixe du symétrique de M par rapport à l'axe des abscisses.
Si $z = \text{Aff}(M)$ alors $|z|$ est égal à la distance OM.
Si $z = \text{Aff}(M)$ et $z_0 = \text{Aff}(M_0)$, alors $\text{Aff}(\overrightarrow{M_0M}) = z - z_0$ et $|z - z_0| = M_0M$

Histoire - John* WALLIS *(1616-1703)



Il semble que John Wallis ait imaginé représenter les nombres complexes dans un plan. Certainement, avait-il compris comment additionner les nombres complexes ; mais l'essentiel : il n'avait pas compris le rôle géométrique de la multiplication.
Wallis est par ailleurs un grand manipulateur de l'infini.

2.4. Inégalités

Théorème - Inégalités
Pour $(z,z') \in \mathbb{C}^2$, on a les inégalités suivantes :

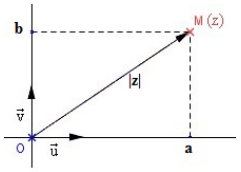
$$\text{Re}\, z \leqslant |z| \text{ avec égalité si et seulement si } z \in \mathbb{R}^+$$

$$\text{Im}\, z \leqslant |z| \text{ avec égalité si et seulement si } z \in i\mathbb{R}^+$$

$$\big||z| - |z'|\big| \leqslant |z+z'| \leqslant |z| + |z'| \textbf{ (Inégalité triangulaire)}$$

avec égalité dans l'inégalité de droite
si et seulement si $z' = 0$ ou il existe $\lambda \in \mathbb{R}^+$ tel que $z = \lambda z'$ (z, z' positivement liés).

Représentation - Affixe d'un point (ou d'un vecteur)



Attention - Module ou valeur absolue ?
Il y a des modules et des valeurs absolues partout ici

Analyse - Interprétation de l'inégalité triangulaire
Si A, B, C sont trois points tels que $z = \text{Aff}(\overrightarrow{AB})$ et $z' = \text{Aff}(\overrightarrow{BC})$, alors

$$|z+z'| \leqslant |z| + |z'| \text{ avec égalité si et seulement si } z, z' \text{ positivement liés}$$

signifie que $AC \leqslant AB + BC$ avec égalité si et seulement si A, B, C sont alignés et B entre A et C.

Démonstration
Avec les notations habituelles,

$$|z|^2 = a^2 + b^2 \geqslant a^2 \Longrightarrow |z| \geqslant |a| = |\text{Re}(z)|$$

Il y a égalité si et seulement si $b = 0$, i.e. $\text{Im}(z) = 0$.
Pour l'inégalité triangulaire, réécrivons les calculs (au carrés) pour mieux voir comment comparer :

$$|z+z'|^2 = (a+a')^2 + (b+b')^2 = a^2 + b^2 + a'^2 + b'^2 + 2aa' + 2bb' = |z|^2 + |z'|^2 + 2\text{Re}(z\overline{z'})$$

$$(|z| + |z'|)^2 = |z|^2 + |z'|^2 + 2|zz'| = |z|^2 + |z'|^2 + 2|z\overline{z'}|$$

Or comme on a vu que $|z\overline{z'}| \geqslant \text{Re}(z\overline{z'})$, on a l'égalité attendue ;
la condition équivalente à l'égalité est $\text{Im}(z\overline{z'}) = 0$ et $\text{Re}(z\overline{z'}) > 0$
i.e. $ab' - a'b = 0$ et $aa' + bb' > 0$ i.e. $z' = \lambda z$ avec $\lambda = \frac{a'}{a} = \frac{b'}{b} > 0$
Enfin, en supposant $|z| \geqslant |z'|$, en considérant $Z = z + z'$ et $Z' = -z'$, on a

$$|z| = |Z + Z'| \leqslant |Z| + |Z'| = |z+z'| + |z'| \quad \Longrightarrow \quad \big||z| - |z'|\big| = |z| - |z'| \leqslant |z+z'|$$

□

Par récurrence :

Proposition - Inégalités
Pour n complexes $z_1, \ldots, z_n$ on a

$$|z_1 + \cdots + z_n| \leqslant |z_1| + \cdots + |z_n|.$$

Proposition - Caractérisation des complexes remarquables

$$z = 0 \Leftrightarrow |z| = 0 \Leftrightarrow \text{Re}\, z = \text{Im}\, z = 0$$

$$z \in \mathbb{R} \Leftrightarrow \text{Im}\, z = 0 \Leftrightarrow \overline{z} = z \Leftrightarrow |z|^2 = (\text{Re}\, z)^2$$

$$z \in i\mathbb{R} \Leftrightarrow \text{Re}\, z = 0 \Leftrightarrow \overline{z} = -z \Leftrightarrow |z|^2 = (\text{Im}\, z)^2$$

3. Le visionnaire : GAUSS et la multiplication complexe

3.1. Les complexes de module 1

En 1800, les mathématiciens manipulent les nombres complexes, mais ces nombres manquent de légitimité.
C'est Gauss qui les justifie géométriquement sur $\mathbb{R}^2$ (Argand et Wessel semblent, chacun de leur côté, avoir eu la même idée).

Le groupe unitaire $\mathbb{U}$

Définition - Groupe unitaire
On note $\mathbb{U}$ l'ensemble des complexes de module 1, c'est aussi le cercle unité de $\mathbb{C}$, ensemble des affixes des points du cercle trigonométrique

$$\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}.$$

Proposition - Conjugaison sur $\mathbb{U}$
$\forall (z,z') \in \mathbb{U}^2,\ zz' \in \mathbb{U}, \qquad \forall z \in \mathbb{U},\ \overline{z} = \dfrac{1}{z} \in \mathbb{U}.$
On dit que l'ensemble $\mathbb{U}$ muni de l'opération multiplication est un groupe commutatif.

Démonstration
$|zz'| = |z| \times |z'| = 1 \times 1 = 1$, donc $zz' \in \mathbb{U}$.
On a vu $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2} = \overline{z}$ car $|z| = 1$. □

Interprétation géométrique du calcul $u \times z$ pour $u \in \mathbb{U}$ et $z \in \mathbb{C}$

Analyse - Géométrique

Soit $u \in \mathbb{U}\setminus\{1\}$ et $z \in \mathbb{C}$. Considérons les 4 points du plan $A(1)$, $B(u) \neq A$, $C(z)$ et $D(u\times z)$.
Alors $AC = |z-1|$ et $BD = |uz-u| = |u| \times |z-1| = AC$.
On a vu (raisonnement analyse-synthèse) alors que :

si (AB) et (CD) ne sont pas parallèles, il existe une unique rotation r du plan tel que $r(A) = B$ et $r(C) = D$.

C'est la rotation dont le centre Ω est à l'intersection des médiatrices de $[AB]$ et $[CD]$ et d'angle $\widehat{\overrightarrow{\Omega A}, \overrightarrow{\Omega B}}$. Or $OA = OB = 1$ et $OC = |z| = |u||z| = |uz| = OD$. Donc O est à l'intersection des médiatrices, par unicité de ce point : $O = \Omega$.
Ainsi, $r(C) = D$, où r est la rotation de centre $O(0)$ et d'angle $\widehat{\overrightarrow{OA}, \overrightarrow{OB}}$).

On montrera plus loin que $(AB)//(CD) \iff \dfrac{z_D - z_C}{z_B - z_A} \in \mathbb{R} \iff z \in \mathbb{R}$.

Or dans ce cas, on peut appliquer directement le théorème de Thalès : pour les triangles OAB et OCD semblables.

On retrouve donc le résultat précédent.

Définition - Argument de $u \in \mathbb{U}$, de $z \in \mathbb{C}$
Soit $u \in \mathbb{U}$. On note I, le point du plan d'affixe 1 et M celui d'affixe u.
On appelle argument de $u \in \mathbb{U}$ noté $\text{Arg}(u)$, l'angle (principal) $(\overrightarrow{OI}, \overrightarrow{OM}) \in]-\pi, \pi]$.
Dans un premier temps, on note $\measuredangle\theta$ ce nombre complexe de module 1 et d'argument θ.
On a alors $u = \cos\theta + i\sin\theta$, pour $\theta = \text{Arg}(u)$.

Remarque - Angle aigu
Le résultat se conçoit bien pour $\theta \in [0, \frac{\pi}{2}]$, mais il reste vrai pour toute mesure d'angle (dans $\mathbb{R}$), par propriété de parité (cos), imparité (sin) et 2π-périodicité.

Démonstration
Si on note X, le point d'affixe $\text{Re}(u)$, alors le triangle OXM est rectangle en X.
Son hypothénuse a une longueur égale à $OM = |u| = 1$, donc comme $\theta \equiv (\overrightarrow{OI}, \overrightarrow{OM})[2\pi]$,
on a $OX = \cos\theta = \text{Re}(u)$ et $XM = \sin\theta = \text{Im}(u)$.
Ainsi $u = \cos\theta + i\sin\theta$. □

Pour aller plus loin - Le problème est en fait lié à la relation d'égalité…
Nous allons essayer de faire avec, au mieux. Mais lorsqu'on aura proprement défini ce que sont des relations d'équivalence, cela sera plus simple…

Proposition - Multiplication par $u \in \mathbb{U}$
Soit $z \in \mathbb{C}$ et $u \in \mathbb{U}\setminus\{1\}$.
Notons $\theta = \arg(u)$.
Alors $u \times z$ est l'affixe du point obtenu par rotation de centre 0 et d'angle θ, à partir du point d'affixe z

La démonstration a été faite plus haut (dans l'analyse).

Attention - Mauvaise définition de l'argument…
La définition donnée ici est peu satisfaisante ; avec un argument principal, on n'a pas nécessairement $\text{Arg}zz' = \text{Arg}z + \text{Arg}z'$, mais seulement des congruences.

3.2. Notation exponentielle

Argument ou argument (classe d'équivalence)

Corollaire - Propriété de $\measuredangle\cdot$
Pour tout $\theta, \theta' \in \mathbb{R}$, $\measuredangle\theta \times \measuredangle\theta' = \measuredangle(\theta + \theta')$

Démonstration
$\measuredangle\theta \times \measuredangle\theta'$ est l'affixe du point M' obtenu à partir de M d'affixe $\measuredangle\theta'$ par rotation d'angle θ.
Il s'agit donc du point de $\mathbb{U}$ d'argument $\theta + \theta'$.
A noter qu'on peut « dépasser » π… □

Analyse - Non injectivité
Mais pour revenir à la question de l'argument, i.e. de $z = \measuredangle\theta$ à $\theta = \text{Arg}z$, on a un soucis de non bijectivité (en fait de non injectivité) de $\measuredangle : \measuredangle\theta = \measuredangle\theta' \not\Rightarrow \theta = \theta'$.
On doit considérer la classe d'équivalences de θ :

$$\overline{\theta} = \{\alpha \mid \exists\, k \in \mathbb{Z}, \alpha = \theta + 2k\pi\}$$

Notons donc $\theta \equiv \theta'[2\pi]$ pour exprimer : $\exists\, k \in \mathbb{Z}$ tel que $\theta' - \theta = 2k\pi$.

Définition - et Propriété. Argument de z
Pour tout $z \in \mathbb{U}$, on note $\arg z = \{\text{Arg}z + 2k\pi, k \in \mathbb{Z}\}$, on le considère *comme* un nombre.
Pour $z, z' \in \mathbb{U}$: $\arg(z \times z') = \arg z + \arg z'$ ou (de manière équivalente) : $\text{Arg}(z \times z') \equiv \text{Arg}z + \text{Arg}z'\ [2\pi]$.

Démonstration
Notons $\theta = \text{Arg}z$ et $\theta' = \text{Arg}z'$. On a $\theta, \theta' \in]-\pi, \pi]$, donc $\theta + \theta' \in]-2\pi, 2\pi]$
Alors $zz' = \measuredangle\theta \times \measuredangle\theta' = \measuredangle(\theta + \theta')$.
• Si $\theta + \theta' \in]-\pi, \pi]$, alors $\text{Arg}zz' = \theta + \theta' \mathit{rime} = \text{Arg}z + \text{Arg}z'$.
• Si $\theta + \theta' \in]\pi, 2\pi]$, alors $\theta + \theta' - 2\pi \in]-\pi, 0] \subset]-\pi, \pi]$ et $\text{Arg}zz' = \theta + \theta' - 2\pi$.
• Si $\theta + \theta' \in]-2\pi, -\pi]$, alors $\theta + \theta' + 2\pi \in]0, \pi] \subset]-\pi, \pi]$ et $\text{Arg}zz' = \theta + \theta' + 2\pi$.
Par conséquent, dans tous les cas : $\text{Arg}zz' \equiv \text{Arg}z + \text{Arg}z'[2\pi]$. □

Pour aller plus loin - Une vraie démonstration
Euler a bien démontré cette démonstration ; il ne s'agit pas d'une simple notation. Il faut donc voir qu'ici, :
— *il s'agit bien du nombre $e = 2,718281\ldots$*
— *il s'agit bien d'une puissance complexe*

Notation d'Euler

Définition - Notation d'Euler
Nous verrons que dans le cas réel, on appelle exponentielle les fonctions qui vérifient $f(a+b) = f(a) \times f(b)$.
Elles s'écrivent (dans le cas réel) sous la forme $x \mapsto A^x$ où $A = f(1)$.
Par uniformité de notation, suivant L. Euler, on notera maintenant $e^{i\theta} = \measuredangle\theta = \cos\theta + i\sin\theta$

On a alors, plus globalement :

Théorème - Propriétés
Soient $(\theta, \theta') \in \mathbb{R}^2$. On a :

$$e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'} \qquad \overline{e^{i\theta}} = e^{-i\theta} = \frac{1}{e^{i\theta}}$$

$$e^{i\frac{\pi}{2}} = i \qquad e^{i\pi} = -1$$

$$e^{i\theta} = 1 \Leftrightarrow \theta \equiv 0[2\pi] \Leftrightarrow \theta \in 2\pi\mathbb{Z} \qquad e^{i\theta} = e^{i\theta'} \Leftrightarrow \theta \equiv \theta'[2\pi]$$

Histoire - D'où vient la notation e ?
Ce n'est pas le e d'exponentielle, mais bien le e du suisse Leonard Euler
La formule d'Euler $e^{i\theta} = \cos\theta + i\sin\theta$ a été obtenue à partir du développement sous forme infinie de exp, cos *et* sin *(chapitre précédent), mais Euler n'a pas compris les propriétés géométriques du produit de complexes.*

Démonstration
On a alors $1 = e^{i0} = e^{i(\theta-\theta)} = e^{i\theta}e^{-i\theta}$, donc $e^{-i\theta} = \dfrac{1}{e^{i\theta}} = \overline{e^{i\theta}}$, car $e^{i\theta} \in \mathbb{U}$.
Le reste s'obtient facilement… □

Corollaire - Formule d'additions trigonométriques
Soient $a, b \in \mathbb{R}$,
$\cos(a+b) = \cos a \cos b - \sin a \sin b$ et $\sin(a+b) = \sin a \cos b + \cos a \sin b$

Démonstration
$\cos(a+b) + i\sin(a+b) = e^{i(a+b)} = e^{ia} \times e^{ib} = (\cos a + i \sin a)(\cos b + i \sin b)$
$= (\cos a \cos b - \sin a \sin b) + i(\sin a \cos b + \cos a \sin b)$
Reste à identifier les parties réelles et imaginaires. □

Exercice
En déduire les formules donnant $\cos(a-b)$ et $\sin(a-b)$.

Correction
Par parité de cos et imparité de sin, en faisant $b \mapsto -b$:
$\cos(a-b) = \cos a \cos b + \sin a \sin b$ et $\sin(a-b) = \sin a \cos b - \cos a \sin b$

3.3. Formules d'Euler et de de Moivre

Formules

Proposition - Formules d'Euler
$$\cos\theta = \mathrm{Re}(e^{i\theta}) = \frac{e^{i\theta}+e^{-i\theta}}{2} \quad , \quad \sin\theta = \mathrm{Im}(e^{i\theta}) = \frac{e^{i\theta}-e^{-i\theta}}{2i}.$$

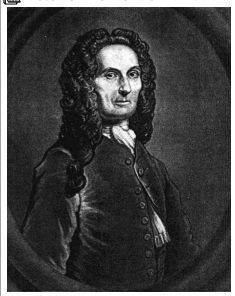
Exercice
Calculer $\frac{1}{3}+\frac{1}{4}$, en déduire une expression de $\cos\frac{7\pi}{12}$ et $\sin\frac{7\pi}{12}$.
On exploitera ces résultats plus tard.

Correction
$\frac{1}{3}+\frac{1}{4} = \frac{7}{12}$, donc
$$e^{i\frac{7\pi}{12}} = e^{i\frac{1}{3}\pi + i\frac{1}{4}\pi} = (\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}) \times (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$$
$$= (\frac{1}{2} + i\frac{\sqrt{3}}{2}) \times (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = \frac{\sqrt{2}-\sqrt{6}}{4} + i\frac{\sqrt{2}+\sqrt{6}}{4}$$
Donc : $\cos\frac{7\pi}{12} = \frac{\sqrt{2}-\sqrt{6}}{4}$ et $\sin\frac{7\pi}{12} = \frac{\sqrt{2}+\sqrt{6}}{4}$

Proposition - Formule de Moivre
$\forall\, n \in \mathbb{Z}$, $(e^{i\theta})^n = e^{in\theta}$
$\forall\, n \in \mathbb{Z}$, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i \sin n\theta$

Démonstration
Par récurrence. On note pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$: « $(e^{i\theta})^n = e^{in\theta}$ ».
— $(e^{i\theta})^0 = 1 = e^{i0\theta}$, donc $\mathscr{P}_0$ est vraie.
— Soit $n \in \mathbb{N}$, supposons que $\mathscr{P}_n$ est vraie.
On a donc $(e^{i\theta})^{n+1} = (e^{i\theta})^n \times e^{i\theta} = e^{in\theta}e^{i\theta}$ d'après $\mathscr{P}_n$.
puis $e^{i\theta})^{n+1} = e^{i(n+1)\theta}$, donc $\mathscr{P}_{n+1}$ est alors vérifiée.
La récurrence fonctionne bien et le résultat est démontrée pour tout n entier naturel.
Puis si $m \in \mathbb{Z}$ avec $m < 0$, alors en notant $n = -m$
$$(e^{i\theta})^m = (e^{i\theta})^{-n} = \frac{1}{(e^{i\theta})^n} = \frac{1}{e^{in\theta}} = e^{-in\theta} = e^{im\theta}$$
La seconde formule de Moivre est la notation algébrique de la précédente. □

Histoire - De Moivre



Abraham De MOIVRE (1667, 1754), mathématicien d'origine française, mais qui du vivre en Angleterre. Hormis la formule de de Moivre (1707), il est connu pour son ouvrage sur les probabilités : the Doctrine of chances

Angle moitié (pour factoriser)

Truc & Astuce pour le calcul - Factorisation de l'angle moitié
Lorsqu'on rencontre un expression de la forme $e^{ia} \pm e^{ib}$ (a, b réels), il faut toujours penser à factoriser par la moitié :
$$a = \frac{a+b}{2} + \frac{a-b}{2} \quad , \quad b = \frac{a+b}{2} - \frac{a-b}{2}$$

Cela donne :
$$e^{ia} \pm e^{ib} = e^{i\frac{a+b}{2}}\left(e^{i\frac{a-b}{2}} \pm e^{-i\frac{a-b}{2}}\right)$$
Et on applique les formules d'Euler

Exercice
Factoriser $1+e^{i\theta}$ et $1-e^{i\theta}$. (Re)trouver les formules donnant $1 \pm \cos\theta$

Correction
$1+e^{i\theta} = e^{i\theta/2}(e^{-i\theta/2}+e^{i\theta/2}) = 2\cos\frac{\theta}{2}e^{i\theta/2}$, $1-e^{i\theta} = e^{i\theta/2}(e^{-i\theta/2}-e^{i\theta/2}) = -2i\sin\frac{\theta}{2}e^{i\theta/2}$
En prenant les parties réelles :
$$1+\cos\theta = 2\cos^2\frac{\theta}{2} \qquad 1-\cos\theta = 2\sin^2\frac{\theta}{2}$$

Exercice
Nouveau calcul de $\sum_{k=0}^{n}\cos kt$ et $\sum_{k=0}^{n}\sin kt$

Correction
On fait un seul calcul, la partie réelle donnera le premier résultat, la partie imaginaire le second.
$$S_n = \sum_{k=0}^{n} e^{ikt} = \sum_{k=0}^{n}(e^{it})^k = 1\frac{1-(e^{it})^{n+1}}{1-e^{it}} = \frac{1-e^{i(n+1)t}}{1-e^{it}} = \frac{e^{i(n+1)t/2}(-2i\sin\frac{(n+1)t}{2})}{e^{it/2}(-2i\sin\frac{t}{2})} = e^{int/2}\frac{\sin(n+1)t/2}{\sin t/2}$$
Formule d'Euler+ de Moivre + série géométrique + angle moitié +...
Donc
$$\sum_{k=0}^{n}\cos kt = \mathrm{Re}(S_n) = \frac{\cos(nt/2)\sin(n+1)t/2}{\sin t/2} \quad , \quad \sum_{k=0}^{n}\sin kt = \mathrm{Im}(S_n) = \frac{\sin(nt/2)\sin(n+1)t/2}{\sin t/2}$$

Linéarisation

Savoir faire - Linéarisation
Il s'agit d'exprimer $\cos^n\theta$ ou $\sin^n\theta$ sous forme d'une somme de $\cos k\theta$ ou $\sin k\theta$
(il ne doit plus y avoir de puissances ni de produits de cosinus ou sinus).
— Ecrire $\cos^n\theta = \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)^n$.
— Développer avec la formule du binôme.
— Regrouper les termes conjugués pour faire apparaître des cosinus ou des sinus.
Si il n'y a pas de faute de calculs, vous devez obtenir un nombre réel : **donc simplification des i...**

Exercice
Linéariser $\cos^3\theta$, $\sin^4\theta$.

Correction
$$\cos^3\theta = \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)^3 = \frac{e^{3i\theta}+3e^{i\theta}+3e^{-i\theta}+e^{3i\theta}}{8} = \frac{1}{4}\cos(3t) + \frac{3}{4}\cos(t)$$
$$\sin^4\theta = \left(\frac{e^{i\theta}-e^{-i\theta}}{2i}\right)^4 = \frac{e^{4i\theta}-4e^{2i\theta}+6-4e^{-2i\theta}+e^{4i\theta}}{16} = \frac{1}{8}\cos(4t) - \frac{1}{2}\cos(2t) + \frac{3}{8}$$

Pour aller plus loin - Polynôme de Tchebychev
Les polynômes de Tchebychev (env. 1860) sont définis par récurrence par :
$$T_0(x) = 1, T_1(x) = x$$
$$T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x)$$
Ils vérifient alors $\forall\, n \in \mathbb{N}$, $\forall\, \theta \in \mathbb{R}$,
$$T_n(\cos\theta) = \cos(n\theta)$$

Savoir faire - Expressions de $\cos(nt)$ et $\sin(nt)$ en fonction de $\cos t$ et $\sin t$
— Ecrire $\cos(nt) = \mathrm{Re}(e^{int}) = \mathrm{Re}[(e^{it})^n]$ ou $\sin(nt) = \mathrm{Im}[(e^{it})^n]$.
— Utiliser la formule du binôme pour calculer $(e^{it})^n = (\cos t + i\sin t)^n$.
— Récupérer la partie réelle (ou imaginaire) en séparant les indices pairs des indices impairs.

Exercice
Ecrire $\cos 3t$ en fonction des puissances de $\cos t$, $\sin 3t$ comme le produit de $\sin t$ et d'une expression contenant des puissances de $\cos t$. Faire de même avec $\cos 5t$ et $\sin 5t$.

Correction
Là encore, on fait les deux questions en même temps, puis on prend la partie réelle et imaginaire.

$$\cos(3t)+i\sin(3t)=(e^{it})^3=(\cos t+i\sin t)^3=\cos^3 t+3i\cos^2 t\sin t-3\cos t\sin^2 t-i\sin^3 t$$

$$\cos(3t)=\cos^3 t-3\cos t\sin^2 t=\cos^3 t-3\cos t(1-\cos^2 t)=4\cos^3 t-3\cos t$$

$$\sin(3t)=3\cos^2 t\sin t-\sin^3 t=3(1-\sin^2 t)\sin t-\sin^3 t=3\sin t-4\sin^3 t$$

$$\cos(5t)+i\sin(5t)=(e^{it})^5=(\cos t+i\sin t)^5=\cos^5 t+5i\cos^4 t\sin t-10\cos^3 t\sin^2 t-10i\cos^2 t\sin^3 t+5\cos t\sin^4 t+i\sin^5 t$$

$$\cos(5t)=\cos^5 t-10\cos^3 t\sin^2 t+5\cos t\sin^4 t=16\cos^5 t-20\cos^3 t+5\cos t$$

$$\sin(5t)=5\cos^4 t\sin t-10\cos^2 t\sin^3 t+\sin^5 t=16\sin^5 t-20\sin^3 t+5\sin t$$

3.4. Argument, forme trigonométrique

Définition - Argument
Soit $z\in\mathbb{C}$, $z\neq 0$, on a $\dfrac{z}{|z|}\in\mathbb{U}$ donc il existe $\theta\in\mathbb{R}$ tel que $\dfrac{z}{|z|}=e^{i\theta}$.
On dit que θ est un argument de z. On note $\theta=\arg z$.
L'écriture $z=re^{i\theta}$ où $r=|z|$ est appelée forme trigonométrique de z.

Pour aller plus loin - Moins loin...
Rappelons qu'on a dit précédemment que l'argument était plutôt à considérer comme un ensemble de valeurs; une classe d'équivalence.

L'argument est une fonction logarithmique (qui vérifie $f(ab)=f(a)+f(b)$), mais multivariée (à plusieurs valeurs).

Proposition - Arithmétique de la congruence
Si $(z,z')\in(\mathbb{C}^*)^2$, on a

$$\arg\overline{z}\equiv-\arg z\ [2\pi]$$
$$\arg\frac{1}{z}\equiv-\arg z\ [2\pi]$$
$$\arg(zz')\equiv(\arg z+\arg z')\ [2\pi]$$
$$\arg\left(\frac{z}{z'}\right)\equiv(\arg z-\arg z')\ [2\pi]$$

Attention - Pas d'unicité
Il n'y a pas unicité de l'argument, il est défini à 2π près. On peut imposer l'unicité de l'argument en le choisissant dans un intervalle de longueur 2π (en géneral $]-\pi,\pi]$ ou $[0,2\pi[$).

Remarque - Géométriquement
Soit z un complexe non nul et M le point d'affixe z. Toute mesure de l'angle orienté $(\vec{u},\overrightarrow{OM})$ est un argument de z.
Il faut savoir caractériser les complexes non nuls réels (resp. réels positifs, resp. réels négatifs, resp. imaginaires purs) par leur argument.

Proposition - Relation arg et arctan
Soit $x\in\mathbb{R}$, alors $\arg(1+ix)\equiv\arctan x\ [2\pi]$.
Soit $z\in\mathbb{C}$, alors $\arg z\equiv\arctan\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\ [\pi]$. Précisément :

$$\arg z\equiv\begin{cases}\arctan\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\ [2\pi] & \text{si } \mathrm{Re}(z)>0\\ \pi+\arctan\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}\ [2\pi] & \text{si } \mathrm{Re}(z)>0\end{cases}$$

Démonstration
Soit $z=1+ix$, on note $\rho=\sqrt{1+x^2}$ son module et θ son argument principal.

$$z=1+ix=\rho\cos\theta+i\rho\sin\theta$$

On peut identifier :

$$x=\frac{x}{1}=\frac{\rho\sin\theta}{\rho\cos\theta}=\tan\theta\Longleftrightarrow\theta=\arctan x$$

□

4. Racines d'un nombre complexe

4.1. Recherche de racines carrées

On dit que $Z\in\mathbb{C}$ est une racine carrée de $z\in\mathbb{C}$ si $Z^2=z$. On dispose de deux méthodes pour chercher les racines carrées de z.

Résolution trigonométrique (la meilleure!)

Truc & Astuce pour le calcul - Racine carrée. Exploitation de la forme trigonométrique
On considère un complexe non nul z écrit sous forme trigonométrique $z=|z|e^{i\alpha}$, et on cherche Z sous forme trigonométrique $Z=\rho e^{i\theta}$ où $\rho>0$.
On a alors $Z^2=\rho^2e^{2i\theta}$, on fait ensuite une sorte d'identification entre les modules et les arguments (mais attention...).

Exercice
Trouver les racines carrées de $z=\dfrac{1-i}{\sqrt{3}-i}$.
On rappelle que $\cos\frac{7\pi}{12}=\frac{\sqrt{2}-\sqrt{6}}{4}$ *et* $\sin\frac{7\pi}{12}=\frac{\sqrt{2}+\sqrt{6}}{4}$

Correction
Il faut écrire z sous forme trigonométrique, on multiplie le dénominateur par la quantité conjuguée (non nécessaire) :

$$z=\frac{(1-i)(\sqrt{3}+i)}{3+1}=\frac{(1+\sqrt{3})+i(1-\sqrt{3})}{4}$$
$$|z|^2=\frac{1}{16}((1+\sqrt{3})^2+(1-\sqrt{3})^2)=\frac{1}{2}\quad\Longrightarrow|z|=\frac{1}{\sqrt{2}}$$

Si $\arg(z)=\theta$, alors $\cos\theta=\frac{\sqrt{2}}{4}(1+\sqrt{3})=\sin\frac{7\pi}{12}$ et $\sin\theta=\frac{\sqrt{2}}{4}(1-\sqrt{3})=\cos\frac{7\pi}{12}$.
Donc $\theta=\frac{\pi}{2}-\frac{7\pi}{12}=\frac{-\pi}{12}$ Les racines carrées de z sont alors : $Z_1=\frac{1}{2^{1/4}}e^{-i\theta/24}$ et $Z_2=-\frac{1}{2^{1/4}}e^{-i\theta/24}$.

La méthode-algorithmique précédente nous permet d'affirmer :

Proposition - Deux racines complexes
Tout complexe non nul possède exactement deux racines carrées complexes (opposées).

Résolution algébrique

Truc & Astuce pour le calcul - Racine carrée. Exploitation de la forme algébrique
On considère donc un complexe non nul z écrit sous forme algébrique $z=x+iy$, et on cherche Z sous forme algébrique $Z=X+iY$.
Le principe est d'écrire l'égalité des modules, des parties réelles et imaginaires de z et Z^2 pour se ramener à une résolution simple de système

donnant X^2, Y^2 et le signe de XY.

$$Z^2 = z \Leftrightarrow \begin{cases} X^2+Y^2 = \sqrt{x^2+y^2} \\ X^2-Y^2 = x \\ 2XY = y \end{cases}$$

On résout le système formée par les deux premières équations, la troisième donne le signe de XY.

Exercice

Déterminer les racines carrées de $2-3i$.

Correction

On considère $Z = X+iY$ avec $Z^2 = 2-3i$.
Donc $|Z|^2 = X^2+Y^2 = |Z^2| = \sqrt{4+9} = \sqrt{13}$.
Puis $\mathrm{Re}(Z^2) = X^2-Y^2 = 2$.
On a donc $X^2 = \frac{2+\sqrt{13}}{2}$ et $Y^2 = -1+\frac{\sqrt{13}}{2}$.
Et comme $\mathrm{Im}(Z^2) = 2XY = -3 < 0$, X et Y sont de signe opposé.
Ainsi $Z = \pm\left(\sqrt{1+\frac{\sqrt{13}}{2}} - i\sqrt{-1+\frac{\sqrt{13}}{2}}\right)$

Equation du second degré

Le théorème suivant a déjà été vu. Mais ici, on insiste sur le fait que les coefficients peuvent être des nombres complexes.

Proposition - Nombre de racines et degré
L'équation $az^2+bz+c=0$, avec $(a,b,c) \in \mathbb{C}^3$, $a \neq 0$, admet deux solutions complexes (éventuellement confondues) $z_1 = \dfrac{-b-\delta}{2a}$ et $z_2 = \dfrac{-b+\delta}{2a}$ où δ est une racine carrée complexe de b^2-4ac.

Remarque - Bien connu...
On retrouve le résolution déjà connue d'une équation du second degré à coefficients réels.

Proposition - Théorème de Viète
Soient $(S,P) \in \mathbb{C}^2$. Les solutions du système

$$\begin{cases} z_1+z_2 = S \\ z_1 \times z_2 = P \end{cases}$$

sont exactement (à permutation près) les solutions de $z^2-Sz+P=0$

Exercice

Résoudre dans $\mathbb{C}$ le système d'équation $\begin{cases} z_1+z_2 = 3 \\ z_1 \times z_2 = 1-3i \end{cases}$.

Correction

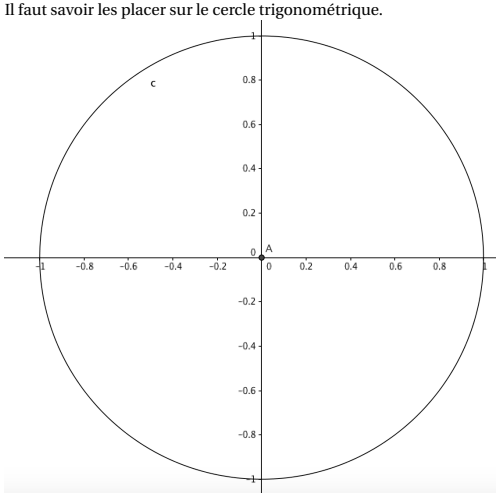
Il faut trouver les solutions de l'équation $z^2-3z+1-3i=0$.
Le discriminant est $\Delta = 9-4+12i = 5+12i$.
On cherche $\delta = a+ib$ tel que $\delta^2 = \Delta$, donc
$|\delta|^2 = a^2+b^2 = |\delta^2| = |\Delta| = \sqrt{25+144} = \sqrt{169} = 13$.
$\Re(\delta^2) = a^2-b^2 = \Re(\Delta) = 5$.
Donc $a^2 = \dfrac{13+5}{2} = 9$ et $b^2 = 4$.
Enfin, comme $2ab = \Im(\delta^2) = \Im(\Delta) = 12 > 0$, on a donc $\delta = 3+2i$ ou $\delta = -3-2i$.
Et par conséquent, les racines de l'équations sont (à permutation près) :
$z_1 = \dfrac{3+3+2i}{2} = 3+i$ et $z_2 = \dfrac{3-3-2i}{2} = -i$.

4.2. Racines n-ièmes de l'unité

Pour aller plus loin - Groupes $(\mathbb{U}_n, \times)$
L'ensemble $\mathbb{U}_n$ des racines n-ieme de l'unité, avec la loi de multiplication $\times$ en fait un groupe.
Nous reprendrons son étude plus précisément, dans quelques semaines.

Théorème - Les n solutions de $z^n=1$
Soit $n \in \mathbb{N}^*$. Les n racines n-ièmes de l'unité, c'est à dire les solutions de l'équation $z^n=1$, sont les n nombres $e^{\frac{2ik\pi}{n}}$ avec $k \in \{0,1,\dots,n-1\}$.
On note $\mathbb{U}_n = \left\{e^{\frac{2ik\pi}{n}}; k \in \{0,1,\dots,n-1\}\right\}$

On obtient donc pour
$n=2$: 1 et -1 ;
$n=3$: 1, $j = e^{\frac{2i\pi}{3}} = \exp\frac{2i\pi}{3}$ et $j^2 = \overline{j} = e^{\frac{4i\pi}{3}} = \exp\frac{4i\pi}{3}$;
$n=4$: $1, i, -1$ et $-i$.
Il faut savoir les placer sur le cercle trigonométrique.



Proposition - Somme des racines n-ième
Soit $n \in \mathbb{N}$, $n \geqslant 2$. La somme des racines n-ièmes de l'unité est nulle.
En particulier $1+j+j^2=0$.

Démonstration
On peut identifier dans le développement polynomiale ou faire le calcul :
$\sum_{k=0}^{n-1} e^{\frac{2ik}{n}\pi} = \sum_{k=0}^{n-1} (e^{\frac{2i\pi}{n}})^k = 1\dfrac{1-e^{2in\pi/n}}{1-e^{2i\pi/n}} = 0$ □

4.3. Racines n-ièmes d'un nombre complexe

Théorème - Racines n-ièmes de z_0
Soient $z_0 \in \mathbb{C}^*$ et $n \in \mathbb{N}^*$. Alors z_0 a exactement n racines n-ièmes (solutions de $z^n = z_0$).
Si $z_0 = |z_0|e^{i\alpha}$, alors ce sont les

$$z_k = |z_0|^{1/n} e^{i\left(\frac{\alpha}{n}+\frac{2k\pi}{n}\right)} \text{ où } k \in \{0,1,\dots,n-1\}.$$

Exercice

Déterminer les racines n-ièmes de $\frac{1+\sqrt{3}i}{1-i}$.

On rappelle que $\cos\frac{7\pi}{12} = \frac{\sqrt{2}-\sqrt{6}}{4}$ *et* $\sin\frac{7\pi}{12} = \frac{\sqrt{2}+\sqrt{6}}{4}$

Correction

On note $z = \frac{1+\sqrt{3}i}{1-i} = \frac{(1+\sqrt{3}i)(1+i)}{(1-i)(1+i)} = \frac{(1-\sqrt{3})+i(1+\sqrt{3})}{2} = \sqrt{2}\times(\frac{\sqrt{2}-\sqrt{6}}{4}) + i\frac{\sqrt{2}+\sqrt{6}}{4}) = \sqrt{2}e^{i\frac{7\pi}{12}}$.

Ainsi, les racines n-ièmes de z sont les nombres $\rho\epsilon_k$, pour $k \in \{0,1,\dots n-1\}$, avec $\rho = 2^{1/2n}$ et $\epsilon_k = e^{i\frac{7\pi}{12n} + \frac{2k\pi}{n}}$.

Exercice

Résoudre dans $\mathbb{C}$ l'équation $(z-1)^6 + (z+1)^6 = 0$.

Correction

On a donc $\left(\frac{z-1}{z+1}\right)^6 = -1$. Puis $\frac{z-1}{z+1}$, racine 6-ième de $-1 = e^{i\pi}$.

Donc $\frac{z-1}{z+1} = \epsilon_k$, avec $k \in \{0,1,\dots,5\}$ et $\epsilon_k = e^{i(2k+1)\pi/6}$.

Et ensuite $z-1 = \epsilon_k(z+1)$ donc $(1-\epsilon_k)z = 1+\epsilon_k$, donc $z_k = \frac{1+\epsilon_k}{1-\epsilon_k}$.

En factorisant par l'angle moitié : $z_k = \frac{\cos(\frac{2k+1}{12}\pi)}{-i\sin(\frac{2k+1}{12}\pi)} = \frac{i}{\tan(\frac{2k+1}{12}\pi)}$

On voit bien sur ces exemples qu'il est préférable d'exploiter la forme géométrique lorsqu'on cherche des racines de nombres complexes…

5. $\mathbb{R}^2 = \mathbb{C} = \mathscr{P}$

5.1. Regard géométrique sur le plan complexe

Proposition - Identification

On munit le plan $\mathscr{P}$ d'un repère orthonormé $(O,\vec{i},\vec{j})$.
Soient A, B, A', B' quatre points du plan. On a alors (*mesure des angles orientés de vecteurs*) :

$$|z_A| = OA$$
$$AB = |z_B - z_A|$$
$$\arg z_A \equiv (\vec{i},\overrightarrow{OA})[2\pi] \qquad \text{et plus généralement : } \arg(z_B - z_A) \equiv (\vec{i},\overrightarrow{AB})[2\pi]$$
$$\arg\left(\frac{z_{B'} - z_{A'}}{z_B - z_A}\right) \equiv (\overrightarrow{AB},\overrightarrow{A'B'})[2\pi]$$

Le dernier résultat, essentiel, mérite une démonstration

Démonstration
Il s'agit d'angle orienté :

$$(\overrightarrow{AB},\overrightarrow{A'B'}) = (\vec{i},\overrightarrow{A'B'}) - (\vec{i},\overrightarrow{AB}) = \arg(z_{B'} - z_{A'}) - \arg(z_B - z_A) = \arg\left(\frac{z_{B'} - z_{A'}}{z_B - z_A}\right)$$

□

Analyse - Le nombre $Z = z' \times \overline{z}$

Etant donné deux vecteurs $\overrightarrow{AB}$ d'affixe $z(= z_B - z_A)$ et $\overrightarrow{A'B'}$ d'affixe $z'(= z_{B'} - z_{A'})$, alors le dernier calcul pour trouver l'angle entre les deux vecteurs conduit à nous intéresser au nombre complexe :

$$Z = z' \times \overline{z}$$

Son argument donne l'angle (orienté) entre ces deux vecteurs.

Définition - Le complexe Z

Soient A, B, A', B' quatre points du plan d'affixe z_A, z_B, $z_{A'}$ et $z_{B'}$ respectivement.
On note $Z = (z_{B'} - z'_A) \times \overline{(z_B - z_A)}$.

Alors

$$\arg Z \equiv (\overrightarrow{AB},\overrightarrow{A'B'})[2\pi] \quad \text{et} \quad |Z| = \|\overrightarrow{AB}\| \times \|\overrightarrow{A'B'}\|$$

où $\|\vec{u}\| = \sqrt{x^2+y^2}$ est par définition la norme (longueur) du vecteur $\vec{u}(x,y)$.
Et donc

$$Z = \|\overrightarrow{AB}\|\|\vec{A'B'}\|\left[\cos(\overrightarrow{AB},\overrightarrow{A'B'}) + i\sin(\overrightarrow{AB},\overrightarrow{A'B'})\right]$$

Le calcul donne :

Proposition - Partie réelle et imaginaire de Z

Avec les mêmes notations et en notant $\vec{u} = \overrightarrow{AB}$ d'affixe $z = z_B - z_A = x + iy$ et $\vec{u'} = \overrightarrow{A'B'}$ d'affixe $z' = z_{B'} - z_{A'} = x' + iy'$.
On rappelle que $Z = z' \times \overline{z}$. On a alors :

$$\mathrm{Re}(Z) = \|\overrightarrow{AB}\|\|\vec{A'B'}\|\cos(\overrightarrow{AB},\overrightarrow{A'B'}) = xx' + yy'$$

$$\mathrm{Im}(Z) = \|\overrightarrow{AB}\|\|\vec{A'B'}\|\sin(\overrightarrow{AB},\overrightarrow{A'B'}) = xy' - x'y$$

Démonstration
Il s'agit juste de vérifier l'égalité avec les parties réelles et imaginaires de z et z'.

$$Z = z \times \overline{z'} = (x+iy)\times(x'-iy') = (xx'+yy') + i(xy'-x'y)$$

□

5.2. Lignes de niveau

Une droite est un ensemble de points alignés. Pour définir une (équation de) droite, on exploite donc les deux points de vue sur l'alignement.

Théorème - Utilisation des complexes - Droite

1. La droite (AB) privée des points A et B (d'affixes respectives a et b) est l'ensemble des points M d'affixe z vérifiant
$$\arg\left(\frac{z-b}{z-a}\right) \equiv 0[\pi].$$
2. La droite (AB) privée du point A est l'ensemble des points M d'affixe z vérifiant
$$\frac{z-b}{z-a} = \overline{\left(\frac{z-b}{z-a}\right)}$$
3. La droite (AB) est l'ensemble des points M d'affixe z vérifiant
$$(z-b)(\overline{z-a}) = (\overline{z-b})(z-a).$$

Démonstration
Notons $\mathscr{D}$, la droite (AB) privées des points A et B (pour avoir un dénominateur non nul dans le calcul).

$$M(z) \in \mathscr{D} \iff (\overrightarrow{AM},\overrightarrow{BM}) \equiv 0[\pi] \iff \arg\left(\frac{z-b}{z-a}\right) \equiv 0[\pi]$$

Et

$$M(z) \in \mathscr{D} \iff \mathrm{Im}((b-z)\overline{(a-z)}) = 0 \iff (b-z)\overline{(a-z)} \in \mathbb{R} \iff (z-b)(\overline{z-a}) = \overline{(z-b)(\overline{z-a})}$$

$$\iff (z-b)(\overline{z-a}) = (\overline{z-b})(z-a) \iff \frac{z-b}{z-a} = \overline{\left(\frac{z-b}{z-a}\right)}$$

□

niveau circu-

"affixe z véri-

infinie si $\theta \equiv$ privé de ces

suivant les démonstration information ce cercle se trice de $[AB]$ gle au centre e...).

Exercice

Donner l'équation de la droite (complexe) qui passe par les points $A(1+i)$ et $B(2-i)$.

Correction

$M(z) \in (AB) \iff (z-(1+i))(\overline{z-(2-i)}) = (\overline{z-(1+i)})(z-(2-i)) \iff z\overline{z}-(2+i)z-(1+i)\overline{z}+(1+3i) = z\overline{z}-(1+i)z-(2-i)\overline{z}+1-3i$

$\iff (1+2i)z-(1-2i)\overline{z}-6i = 0$

On peut vérifier que A et B appartiennent bien à la droite :

$(1+2i)(1+i)-(1-2i)(1-i) = 2i\text{Im}((1+2i)(1+i)) = 6i$ et $2i\text{Im}((1+2i)(2-i)) = 6i$.

Théorème - Ligne de niveau - Cercle

Soient A, B, C trois points distincts d'affixes respectives a, b et c.

1. $(AB) \perp (AC) \Leftrightarrow \arg\left(\dfrac{c-a}{b-a}\right) \equiv \dfrac{\pi}{2}[\pi]$
2. L'ensemble des points M d'affixe z vérifiant
$$\arg\left(\frac{z-b}{z-a}\right) \equiv \frac{\pi}{2}[\pi]$$
est le cercle de diamètre $[AB]$ privé des points A et B.
3. L'ensemble des points M d'affixe z vérifiant
$$\frac{z-b}{z-a} = -\left(\overline{\frac{z-b}{z-a}}\right)$$
est le cercle de diamètre $[AB]$ privé du point A.
4. L'ensemble des points M d'affixe z vérifiant $(z-b)\overline{(z-a)} = -\overline{(z-b)}(z-a)$ est le cercle de diamètre $[AB]$.

Démonstration

Le premier point découle d'une proposition précédente.

Nous allons procéder en deux temps (double inclusion d'ensemble).

On note $\mathscr{E} = \left\{M(z) \in \mathbb{C} \mid \arg\dfrac{z-b}{z-c} \equiv \dfrac{\pi}{2}[\pi]\right\}$ et $\mathscr{C}$ le cercle de diamètre $[AB]$.

Il allons de montrer, par double inclusion, que $\mathscr{E} = \mathscr{C} \setminus \{A, B\}$.

— Le centre du cercle $\mathscr{C}$ est K d'affixe $k = \dfrac{a+b}{2}$ et de rayon $r = \dfrac{1}{2}|AB| = \dfrac{|b-a|}{2}$

$$z \in \mathscr{C} \setminus \{A, B\} \iff z = k + re^{i\theta} \text{ avec } \theta \neq \theta_0[\pi]$$

où $\theta_0 = \arg(a-b) = (\vec{i}, \overrightarrow{BA})$, donc $a - b = 2re^{i\theta_0}$.

Or

$$\frac{z-b}{z-a} = \frac{k-b+re^{i\theta}}{k-a+re^{i\theta}} = \frac{(a-b)+2re^{i\theta}}{(b-a)+2re^{i\theta}} = \frac{e^{i\theta}+e^{i\theta_0}}{e^{i\theta}-e^{i\theta_0}} = \frac{2e^{i\frac{\theta-\theta_0}{2}}\cos\frac{\theta-\theta_0}{2}}{2e^{i\frac{\theta-\theta_0}{2}}\,i\sin\frac{\theta-\theta_0}{2}} = -\frac{\cos\frac{\theta-\theta_0}{2}}{\sin\frac{\theta-\theta_0}{2}}i$$

Donc $\arg\left(\dfrac{z-b}{z-a}\right) \equiv \arg(-i) \equiv \dfrac{\pi}{2}[\pi]$. Donc $\mathscr{C} \setminus \{A, B\} \subset \mathscr{E}$.

— Réciproquement, si $z \in \mathscr{E}$, il existe $R \in \mathbb{R}$ avec $z \neq a, b$

$$\frac{z-b}{z-a} = Ri \iff z-b = Ri(z-a) \iff (1-Ri)z = b-Ria \iff z = \frac{b-Ria}{1-Ri} = \frac{(b+R^2a)+Ri(b-a)}{1+R^2}$$

Donc, toujours avec $k = \frac{a+b}{2}$, affixe de K, milieu de $[AB]$,

$$z-k = z-\frac{a+b}{2} = \frac{(b-a)[1-R^2+2Ri]}{2(1+R^2)} \Longrightarrow |z-k| = \frac{|b-a|\times|1-R^2+2Ri|}{2(1+R^2)} = \frac{|b-a|}{2}$$

Ce nombre est contant (indépendant de z), c'est le rayon du cercle représenté par $\mathscr{E}$.

Et on a donc $\mathscr{E} \subset \mathscr{C} \setminus \{A, B\}$

Pour finir, nous savons que si $Z \neq 0$,

$$\arg(Z) \equiv \frac{\pi}{2}[\pi] \longleftrightarrow Z \in i\mathbb{R} \longleftrightarrow Z = -\overline{Z}$$

□

5.3. Transformations du plan (point de vue complexe)

Transformations « élémentaires »

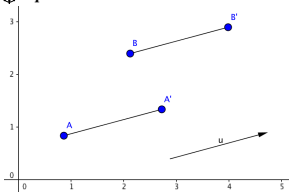
Définition - Transformation du plan

On appelle transformation du plan toute bijection du plan dans lui-même.

Attention - Projection

Une projection sur une droite n'est pas une transformation du plan.

Représentation - Translation de vecteur $\vec{u}$



Définition - Translation

On appelle translation de vecteur $\vec{u}$ l'application

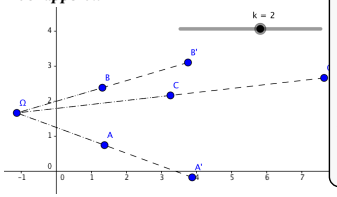
$$\begin{aligned} t_{\vec{u}} : \ \mathscr{P} &\to \mathscr{P} \\ M &\mapsto M' \text{ tel que } \overrightarrow{MM'} = \vec{u} \end{aligned}$$

En complexes, $t_{\vec{u}}$ est représentée par l'application de $\mathbb{C}$ dans $\mathbb{C}$ définie par

$$z \mapsto z + z_0$$

où z_0 est l'affixe du vecteur $\vec{u}$.

Représentation - Homothétie de centre Ω et de rapport $k = 2$



Définition - Homothétie

On appelle homothétie de centre Ω et de rapport le réel $k \neq 0$ l'application

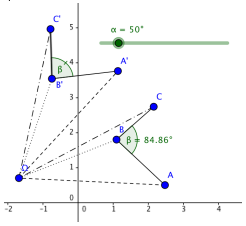
$$\begin{aligned} h_{\Omega,k} : \ \mathscr{P} &\to \mathscr{P} \\ M &\mapsto M' \text{ tel que } \overrightarrow{\Omega M'} = k\overrightarrow{\Omega M} \end{aligned}$$

En complexes, $h_{\Omega,k}$ est représentée par l'application de $\mathbb{C}$ dans $\mathbb{C}$ définie par

$$z \mapsto z_0 + k(z - z_0)$$

où z_0 est l'affixe du point Ω.

Représentation - Rotation d'angle α



Définition - Rotation

On appelle rotation de centre Ω et d'angle θ l'application

$$\begin{aligned} R_{\Omega,\theta} : \ \mathscr{P} &\to \mathscr{P} \\ M &\mapsto M' \text{ tel que } \begin{cases} \Omega M' = \Omega M \\ (\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}) \equiv \theta[2\pi] \end{cases} \text{ si } M \neq \Omega \\ \Omega &\mapsto \Omega \end{aligned}$$

En complexes, $R_{\Omega,\theta}$ est représentée par l'application de $\mathbb{C}$ dans $\mathbb{C}$ définie par

$$z \mapsto z_0 + e^{i\theta}(z - z_0)$$

où z_0 est l'affixe du point Ω.

Similitudes (directes)

Il s'agit de composition de rotation et d'homothétie...

Définition - Similitude directe
On appelle similitude directe du plan toute transformation représentée dans le plan complexe par une application de la forme

$$z \mapsto az + b$$

avec $(a, b) \in \mathbb{C}^* \times \mathbb{C}$.

Remarque - Les transformations élémentaires
Translations, homothéties et rotations sont des similitudes directes, il suffit de regarder leur expression en complexe.

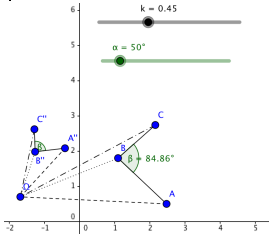
Analyse - Résultats caractéristiques
Si A, B sont deux points distincts d'images respectives A', B' par la transformation associée à $z \mapsto az + b$, alors

$$(\overrightarrow{AB}, \overrightarrow{A'B'}) \equiv \arg a\,[2\pi] \text{ et } \frac{A'B'}{AB} = |a|.$$

Proposition - Similitude directe
Une similitude directe conserve les angles et les rapports des distances.
Si A, B, C sont trois points distincts d'images respectives A', B', C' par Alors

$$(\overrightarrow{AB}, \overrightarrow{AC}) \equiv (\overrightarrow{A'B'}, \overrightarrow{A'C'})[2\pi] \qquad \text{et} \qquad \frac{AB}{AC} = \frac{A'B'}{A'C'}$$

Représentation - Similitude (directe)



Démonstration
Supposons que la transformation est $z \mapsto az + b$. Et notons z_M, l'affixe du point M, générique.

$$\frac{z_{A'} - z_{B'}}{z_{A'} - z_{C'}} = \frac{az_A + b - az_B - b}{az_A + b - az_C - b} = \frac{z_A - z_B}{z_A - z_C}$$

En prenant l'argument et le module, on retrouve respectivement la conservation des angles et des longueurs. □

Théorème - Caractérisation
Soit f la transformation du plan représentée par $z \mapsto az + b$ avec $a \in \mathbb{C}^*, b \in \mathbb{C}$.
- Si $a = 1$, f est la translation de vecteur d'affixe b.
- Si $a \neq 1$, f admet un unique point fixe (point invariant) $\Omega(\frac{b}{1-a})$ appelé centre de la similitude.
  f s'écrit alors : $f = h \circ r = r \circ h$ avec
  · r rotation de centre Ω d'angle de mesure $\arg a$
  · h homothétie de centre Ω et de rapport $|a|$.
  On dit que $|a|$ est le rapport de la similitude, et $\arg a$ est (la mesure de) l'angle de la similitude.

Démonstration
Soit $\Omega(z)$, un point fixe de f i.e. : $z = f(z)$ i.e. $z = az + b$, donc $z = \dfrac{b}{1-a}$ $(a \neq 1)$.
On a donc un unique point fixe. Notons $z_0 = \frac{b}{1-a}$.
Ainsi, pour tout $z \in \mathbb{C}$,

$$f(z) - z_0 = f(z) - f(z_0) = (az + b) - (az_0 + b) = a(z - z_0) \qquad \Longrightarrow \qquad f(z) = z_0 + a(z - z_0)$$

En notant $a = |a|e^{i\arg(a)}$, on retrouve le produit complexe ou la composition de transformation de la rotation $(\times e^{i\theta})$ et de l'homothétie $(\times |a|)$. □

Remarque - Cas particuliers avec $a \neq 1$:
- Si $a \in \mathbb{R}^*$, f est l'homothétie de centre Ω de rapport a.
- Si $|a| = 1$, f est la rotation de centre Ω, d'angle $\theta = \arg a$.

Corollaire - Caractérisation de la similitude
La similitude de centre d'affixe z_0, de rapport k et d'angle θ est représentée par

$$z \mapsto z_0 + ke^{i\theta}(z - z_0).$$

Savoir faire - Reconnaître une similitude
Etant donnée une transformation, pour reconnaître une similitude il faut :
1. chercher le point fixe : la solution de $f(z) = z$.
   On le note z_0, c'est le centre de la similitude.
2. chercher le complexe a tel que $f(z) - z_0 = a(z - z_0)$.
   Ce complexe a donne le rapport et l'angle de la similitude

Proposition - Composée de similitudes
La composée de deux similitudes est une similitude dont le rapport est le produit des rapports et l'angle, la somme des angles.
On a les cas particuliers suivants :
- la composée de deux translations est une translation de vecteur la somme des deux vecteurs,
- la composée de deux homothéties est soit une homothétie soit une translation,
- la composée de deux rotations de même centre est une rotation de même centre et d'angle la somme des deux angles (éventuellement d'angle nul, i.e. l'identité du plan)
- la composée de deux rotations de centres distincts, d'angles respectifs θ et θ' est :
  · une rotation si $\theta + \theta' \not\equiv 0[2\pi]$
  · une translation (éventuellement de vecteur nul, i.e. l'identité) sinon.

Démonstration
Considérons les deux similitudes $z \mapsto az + b$ et $z \mapsto a'z + b'$.
La composée des deux similitudes est

$$z \mapsto a(a'z + b') + b = aa'z + (ab' + b)$$

On reconnait, à cas particuliers près, une similitude. Pour les cas particuliers, on reprend chacun dans le même ordre :
- la composée de deux translations est une translation de vecteur la somme des deux vecteurs.
  Dans ce cas $a = a' = 1$, on a bien une translation.
- la composée de deux homothéties est soit une homothétie soit une translation.
  Dans ce cas $a, a' \in \mathbb{R}$, donc $aa' \in \mathbb{R}$; on a donc une homothétie ou une translation (si $aa' = 1$)
- la composée de deux rotations de même centre est une rotation de même centre et d'angle la somme des deux angles (éventuellement d'angle nul, i.e. l'identité du plan).
  Dans ce cas, en notant Ω ce centre : $r \circ r'(\Omega) = r(\Omega) = \Omega$. Donc Ω est centre de la similitude.
  Comme $a, a' \in \mathbb{U}$, alors $aa' \in \mathbb{U}$ et donc cette similitude est une rotation.
  Son angle est $\arg(aa') = \arg(a) + \arg(a')$.
- la composée de deux rotations de centres distincts, d'angles respectifs θ et θ'.
  On a $a = e^{i\theta}$ et $a' = e^{i\theta'}$, donc il s'agit de l'application $z \mapsto e^{i(\theta+\theta')}z + (ab' + b)$.
  Et donc il s'agit d'une
  · rotation si $\theta + \theta' \not\equiv 0[2\pi]$
  · translation (éventuellement de vecteur nul, i.e. l'identité) sinon.

□

Corollaire - Transformation réciproque (ou inverse)
On a les transformations réciproques suivantes :

$$t_{\vec{u}}^{-1} = t_{-\vec{u}}; \quad h_{\Omega,k}^{-1} = h_{\Omega,\frac{1}{k}}; \quad R_{\Omega,\theta}^{-1} = R_{\Omega,-\theta}.$$

Proposition - Transformation du plan
Etant donné deux segments $[MN]$ et $[M'N']$ de longueurs non nulles, il existe une et une seule similitude directe transformant M en M' et N en N'.

Démonstration
On peut typiquement faire une démonstration en analyse-synthèse.
Supposons que cette transformation existe, notée $z \mapsto az+b$.
On a donc $z_{M'} = az_M + b$ et $z_{N'} = az_N + b$. Et donc $a = \dfrac{z_{M'} - z_{N'}}{z_M - z_N}$.

a est donc unique et de même $b = z_{M'} - \dfrac{z_{M'} - z_{N'}}{z_M - z_N} z_M$.
Mais pour s'assurer de l'existence, il faut qu'on retrouve bien $az_N + b = z_{N'}$:

$$az_N + b = \frac{z_{M'} - z_{N'}}{z_M - z_N} z_N + z_{M'} - \frac{z_{M'} - z_{N'}}{z_M - z_N} z_M = \frac{(z_{M'} - z_{N'})(z_N - z_M)}{z_M - z_N} + z_{M'} = -z_{M'} + z_{N'} + z_{M'} = z_{N'}$$

□

Symétries

Définition - Symétries
On appelle :

— Symétrie centrale de centre Ω l'application

$$s_\Omega : \begin{array}{ccc} \mathscr{P} & \to & \mathscr{P} \\ M & \mapsto & M' \text{ tel que } \overrightarrow{\Omega M'} = -\overrightarrow{\Omega M} \end{array}$$

En complexes, s_Ω est représentée par l'application de $\mathbb{C}$ dans $\mathbb{C}$ définie par $z \mapsto 2z_0 - z$ où z_0 est l'affixe du point Ω.

— Symétrie orthogonale d'axe la droite $\mathscr{D}$ (ou réflexion d'axe $\mathscr{D}$) l'application

$$s_\mathscr{D} : \begin{array}{ccc} \mathscr{P} & \to & \mathscr{P} \\ M & \mapsto & M' \text{ tel que } \begin{cases} M' = M \text{ si } M \in \mathscr{D} \\ \mathscr{D} \text{ est la médiatrice de } [MM'] \text{ sinon} \end{cases} \end{array}$$

La symétrie orthogonale par rapport à Ox est représentée par l'application de $\mathbb{C}$ dans $\mathbb{C}$ définie par $z \mapsto \overline{z}$.

Remarque - Symétrie centrale
Une symétrie centrale peut être considérée comme une homothétie de rapport -1 ou une rotation d'angle π, c'est une similitude directe.

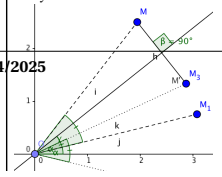
Attention - Réflexion
Une réflexion n'est pas une similitude directe

Proposition - Involution
Une symétrie est une transformation du plan : $s^{-1} = s$.

Pour aller plus loin - Symétrie axiale (orthogonale) et composition
Une réflexion peut s'écrire comme une composée de similitude directe et de conj : $z \mapsto \overline{z}$. La figure suivant donne une décomposition possible :

$$r(z) = \left[R_{0,\theta} \circ conj \circ R_{O,\theta}^{-1}\right](z)$$

où θ est l'angle entre l'axe de abscisse et l'axe de symétrie.



Démonstration
Toute involution : ($s^2 = \mathrm{id}$) est nécessairement bijective car $\forall\ y, \exists\ x = s(y)$ tel que $y = s(x)$.
En effet $s(x) = s(s(y)) = s^2(y) = y$.
Toute symétrie est une involution :

— si $s_\Omega(M) = M'$ et $s_\Omega(M') = M''$, alors $\overrightarrow{\Omega M} = -\overrightarrow{\Omega M'} = \overrightarrow{\Omega M''}$, et donc $M = M'' = s_\Omega^2(M)$.
— si $s_\mathscr{D}(M) = M'$ et $s_\mathscr{D}(M') = M''$, alors $\mathscr{D}$ est la médiatrice de $[MM']$ et de $[M'M'']$,
donc (MM') et $(M'M'')$ sont parallèles (perpendiculaire à une même troisième)
et comme elles ont un point commun : M', ces droites sont confondues,
donc M, M', M'' sont alignés.
$\mathscr{D}$ étant médiatrice de $[MM']$ et de $[M'M'']$, les milieux de $[MM']$ et de $[M'M'']$ sont confondus.
Et finalement : $M = M'' = s_\mathscr{D}^2(M)$

□

Pour aller plu
L'inversion est u
en géométrie pr
L'inversion par i
$\Omega(\omega)$ et de rayon
$M'(z')$ tel que $(z$
Pour que Ω puis
nit sur $\mathbb{C} \cup \{\infty\}$

6. Bilan

Synthèse

⇝ Les relations trigonométriques permettent d'obtenir une relation algébrique simple lorsqu'on considère la fonction d'EULER à valeurs complexes $t \mapsto \cos t + i \sin t$, notée e^{it} : $e^{i(a+b)} = e^{ia} \times e^{ib}$. A partir de celle-ci, on retrouve toutes les formules (en exploitant la relation de DE MOIVRE, le binôme de NEWTON ou les fonctions linéaires Re ou Im). **A savoir-faire manipuler absolument!**

⇝ Très souvent la question se pose de manière réciproque : étant donné une longueur de quel angle en est-elle le cos ? Le problème, la fonction n'est pas injective : on peut avoir $\theta \neq \theta'$ et $\cos\theta = \cos\theta'$. On restreint donc l'intervalle image. On crée ainsi une fonction réciproque arccos à la fonction $\cos_{|[0,\pi]} : [0,\pi] \to [-1,1]$. De même pour les fonctions $\sin_{|[-\frac{\pi}{2},\frac{\pi}{2}]}$ et $\tan_{|[-\frac{\pi}{2},\frac{\pi}{2}]}$.

⇝ On se pose la même question pour $z \mapsto z^2$ et plus largement $z \mapsto z^n$. Etant donné un nombre complexe $Z = \rho e^{i\alpha}$, il y a exactement n nombres complexes différents $z_1, \dots z_n$ tels que pour tout $k \in \mathbb{N}_n$, $(z_k)^n = Z$. Ce sont les racines n-ième de Z. Pour les obtenir, on se ramène **aux classiques racines $n$ième de l'unité** $e^{2ik\pi/n}$ en en divisant par $\sqrt[n]{\rho} e^{i\alpha/n}$.
Au passage, on trouve une méthode complémentaire (algébrique) dans le simple cas de la racine carrée d'un nombre complexe.

⇝ La géométrie plane (de $\mathbb{R}^2$) se code parfaitement par du calcul, sur $\mathbb{C}$. Les concepts naturels de géométrie (longueur, orthogonalité, parallélisme) se réduise exactement par du calcul, selon le rêve de Descartes ou de Leibniz.

⇝ En retour, le calcul complexe simple : addition, multiplication, division devient une opération géométrique : translation, similitude sans ou avec conjugaison respectivement voire inversion…

Savoir-faire et Truc & Astuce du chapitre

— Truc & Astuce pour le calcul - Factorisation de l'angle moitié
— Savoir-faire - Linéarisation
— Savoir-faire - Expression de $\cos(nt)$ et $\sin(nt)$ en fonction de $\cos t$ et $\sin t$
— Truc & Astuce pour le calcul - Racine carrée. Exploitation de la forme trigonométrique
— Truc & Astuce pour le calcul - Racine carrée. Exploitation de la forme algébrique
— Savoir-faire - Obtenir l'équation d'une droite (avec un point et un vecteur directeur ou avec deux points)

— Savoir-faire - Interprétation en terme de projection
— Savoir-faire - Obtenir l'équation d'une droite (avec un point et un vecteur normal)
— Savoir-faire - Reconnaître une similitude

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
Re, Im	Fonctions partie réelles et parties imaginaires, appliquées à un nombre complexe	Elles sont $\mathbb{R}$-linéaires ($\forall\, a_1, a_2 \in \mathbb{R}, z_1, z_2 \in \mathbb{C}$, $\mathrm{Re}(a_1 z_1 + a_2 z_2) = a\mathrm{Re}(z_1) + a_2\mathrm{Re}(z_2)\ldots$)	
$e^{i\theta}$	$e^{i\theta} := \cos\theta + i\sin\theta$ (Euler)	$e^{i(\theta+\theta')} = e^{i\theta} \times e^{i\theta'}$	Relations de de Moivre : $\cos\theta = \mathrm{Re}(e^{i\theta}) = \frac{1}{2}(e^{i\theta} + e^{-i\theta})$, $\sin\theta = \mathrm{Im}(e^{i\theta}) = \frac{1}{2i}(e^{i\theta} - e^{-i\theta})$.
j	$j := e^{2i\pi/3} = \dfrac{-1+i\sqrt{3}}{2}$	$j^3 = 1$, $1 + j + j^2 = 0$	Racine primitive troisième de l'unité (avec $\overline{j} = j^2$)
$\mathbb{U}_n$	Ensemble des racines n-ième de l'unité $\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$	$z \in \mathbb{U}_n$ si et seulement si $\exists!\, k \in \mathbb{N}_n$ (ou $\exists!\, k \in [\![0, n-1]\!]$) tq $z = e^{2ik\pi/n}$	Reviendra souvent dans l'année.

Retour sur les problèmes

15. Multiplication des nombres.
$z \times z'$ donne (géométriquement) le nombre complexe obtenu par similitude de centre O, de longueur $|z|$, et d'angle $\arg(z)$ à partir du point $Z'(z')$.
On peut l'obtenir en appliquant le théorème de Thalès. On note I, l'intersection du cercle unité et de la droite OZ'. Puis on trace la parallèle à IZ passant par Z'. L'intersection de cette droite avec OZ donne le point $Z''(z \times z')$.
16. Le centre du triangle équilatéral sur le côté $[AB]$ a pour affixe $z_1 = \dfrac{b - e^{i\pi/6}a}{1 - e^{i\pi/6}} = \dfrac{ibe^{-i\pi/12} - iae^{i\pi/12}}{2\sin\frac{\pi}{12}}$ car $(b - z_1) = e^{i\pi/6}(a - z_1)\ldots$.
17. Transformation du plan
Tout le chapitre répond à cet exercice
18. $\cos\theta_2 = i\dfrac{\sqrt{n_1^2\sin^2\theta_1 - n_2^2}}{n_2}$. Pour le reste, voir avec M. Lagoute.

Chapitre 5

Utilisation de la dérivation

Résumé -

Ce chapitre se présente comme un large résumé du cours de première S avec ajouts de fonctions usuelles (vues en terminale ou en MPSI). On reprend tous les résultats en admettant la notion fine de limite, ils nous serviront d'outils pour des études plus poussés par la suite ou bien pour leur application dans d'autres domaines scientifiques. Le but est donc de raffiner notre technique (calculs)....
Il ne faut pas oublier que la notion de fonctions est une notion fine des mathématiques modernes, elle a mis plusieurs siècle à émerger : Leibniz, puis Euler, puis Cantor et Weierstrass... pour arriver jusqu'à nous. Et encore, le joyau n'est pas encore définitivement ciselé (distributions de Schwartz...). Sur internet :

- *OptimalSup-Spé - Cours Fonctions usuelles. https ://www.youtube.com/watch ?v=xTbtre9dgmQ*
- *Micmaths - Merveilleux logarithmes - https ://www.youtube.com/watch ?v=rWfl7Pw8YVE*
- *El Jj - Différences équations/fonctions (pas de questions stupides#01)*

Sommaire

1. Problèmes 88
2. Dérivation 89
2.1. Approche historique 89
2.2. Dérivabilité 89
2.3. Approximation linéaire 90
2.4. Règles de dérivation 90
2.5. Dérivation de fonctions usuelles 91
2.6. Dérivées seconde, troisième... 94
3. Quelques utilisations de la dérivation 94
3.1. Variations 94
3.2. Bijections et réciproques 95
3.3. Inégalités 97
3.4. Calculs de limites (lever les indéterminations) 97
3.5. Approximation polynomiale (développement limité) 99
4. Dérivation de fonctions réelles à valeurs complexes . . . 100
4.1. Fonctions à valeurs complexes 100
4.2. Dérivation d'une fonctions d'une variable réelle, à valeurs complexes 103
4.3. Propriétés 103
4.4. Composition avec l'exponentielle complexe 104
5. Bilan 104

1. Problèmes

? Problème 19 - Optimisation par FERMAT. Raisonnement pré-dérivatoire

Reprenons l'exemple de Fermat qui cherche à trouver la position E sur un segment $[AC]$ de manière à ce que $AE \times EC$ soit maximum.
Notons $a = AE$ et $b = EC$. On a donc $a + b = d (= AC)$ fixé. On cherche la valeur maximal de $AE \times EC = a(d-a) = ad - a^2$.
La méthode de Fermat consiste donc à ajouter une valeur e à AE, on a alors une nouvelle valeur qui vaut : $(a+e)d - (a+e)^2 = ad - a^2 + e(d - 2a) - e^2$.
Ajouter une valeur e à AE consiste donc à faire évaluer $AE \times EC$ d'une valeur $ad - a^2 + e(d-2a) - e^2 - ad + a^2 = e(d-2a) + e^2$.
Fermat dit qu'il faut « adégaler » les deux valeurs cela donne $e(d-2a) + e^2 = 0$. On peut simplifier par $e \neq 0$.
On trouve donc $d - 2a + e = 0$, et il prend $e = 0$ et donc $a = \frac{d}{2}$. E est au milieu de $[AC]$. Qu'en pensez-vous ?

? Problème 20 - Optimisation

On passe notre vie à optimiser nos actions, nos décisions (la plus efficace, la moins longue...).
Comment assurément trouver une stratégie qui permet à tous les coups d'optimiser (au moins localement) nos décisions.
Si elle se mesure sous la forme Résultat(Action), on doit trouver : Résultat(Action+δ)<Résultat(Action) et Résultat(Action-δ)<Résultat(Action) également...

? Problème 21 - Dérivation : concept local ou global ?

A priori l'optimisation précédente de la fonction Résultat donne des valeurs différentes selon la valeur Action où l'on se place. Ainsi, la notion de dérivation est un concept local.
Et donc, dans un second temps, une fois que pour tout x, $f'(x)$ est bien défini, on peut seulement réunir toutes ces valeurs en une seule fonction f.
D'où vient le miracle que dans la pratique, on peut directement agir de f à f' (de fonction à fonction) ?

? Problème 22 - Dérivations de fonctions usuelles et des opérations

Et ainsi, en particulier, quelles sont les transformations de dérivation pour les fonctions usuelles ? Et également, que deviennent les opérations classiques $(+, \times, \circ)$ pour la dérivation ?

? Problème 23 - Se concentrer sur un problème

D'une certaine façon, regarder la dérivation de f en x_0, c'est faire l'approximation affine (donc relativement simple) mais juste des valeurs $f(x)$ pour x proche de x_0.
Ces valeurs approchées peuvent se concentrer autour de 0. Et si l'on se

trouve autour d'un cas de limite problématique du type : $\frac{\to 0}{\to 0}$, ne peut-on pas exploiter les approximations affines (et donc les dérivées) pour obtenir une bonne évaluation de cette forme indéterminée?

? Problème 24 - Etude de fonctions complexes

Comment étudier des fonctions à valeurs dans $\mathbb{C}$: $f : \mathbb{R} \to \mathbb{C}$ (comme $\theta \mapsto e^{i\theta}$)?
Nous les avons définies lors du chapitre précédent; comment les dériver maintenant?
Mieux : comment étudier des fonctions de la variables complexes? Peut-on les dériver, comment cela s'adapte?

2. Dérivation

2.1. Approche historique

Heuristique - Infinitésimaux

Le calcul différentiel et le calcul intégral ont été finalisés indépendamment et associés par Leibniz (1684) et Newton (1671, publié en 1736).
Leurs raisonnement repose sur une notion floue d'infinitésimaux (ou de fluente), notion non convaincante à l'époque.
Johan Bernoulli (1692) popularise auprès de toute sa dynastie, du marquis de L'Hospital et surtout d'Euler, la découvert de Leibniz (« une énigme plutôt qu'un explication ») et pense que des explications trop abondantes au sujet de l'infiniment petit pourrait troubler l'entendement de ceux qui ne sont pas « accoutumés à de longues explications ».
En fait, il manque la notion claire de limite, dont d'Alembert (1754) s'approche le plus. La bonne notion de limite est définie par Bolzano (1817), Cauchy (1823) ou Weierstrass (1861) et donnent ainsi une définition bien formalisée et solide mathématiquement (permettant de démontrer des résultats), abandonnant la notion d'Infinitésimaux.
Ce chapitre s'appuie sur des mathématiques du XVII. Nous ferons les démonstrations après avoir défini la notion de limite.

Pour aller plus loin - Analyse non standard

En 1961, Abraham Robinson crée une nouvelle logique mathématique en s'appuyant sur les nombres hyperréels.
Edward Nelson, en 1977, renouvelle l'analyse non standatd (IST) en donnant un nouveau sens aux infinitésimaux et définit un nouveau calcul…

Remarque - Cours de physique

En physique, en MPSI, le cours est proche des idées de Leibniz et Newton, et c'est très bien ainsi.
La notation $\frac{\partial f}{\partial x}$ est celle de Leibniz. La notation $\dot{x}$ est due à Newton!
C'est Lagrange, après un détour par Euler, qui impose la notation f'.

Remarque - Limite

On va faire comme si on connaissait la notion de limite, application linéaire ($\lim \lambda f + g = \lambda \lim f + \lim g$)…

2.2. Dérivabilité

Définition - Nombre dérivée

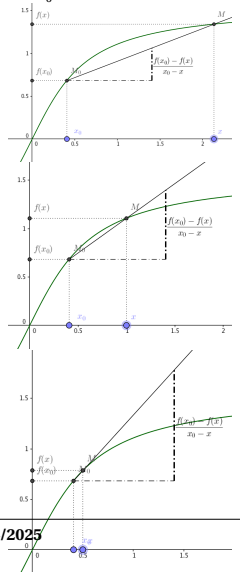
Soient I un intervalle de $\mathbb{R}$, f une fonction définie sur I et x_0 un point de I.
f est dérivable en x_0 si la fonction $x \mapsto \frac{f(x)-f(x_0)}{x-x_0}$, définie sur $I-\{x_0\}$, admet une limite finie en x_0.
On a alors

$$f'(x_0) = \lim_{x\to x_0} \frac{f(x)-f(x_0)}{x-x_0} = \lim_{h\to 0} \frac{f(x_0+h)-f(x_0)}{h}$$

f est dérivable sur I si elle est dérivable en tout point de I.
$f'(x)$ s'appelle le nombre dérivé en x et la fonction qui à $x \in I$ associe $f'(x)$ s'appelle la (fonction) dérivée de f.

Représentation - Nombre dérivée

Il s'agit d'une notion « dynamique » (limite). Il faut le voir comme un film, en plusieurs temps $x \mapsto x_0$:



On retrouve ce type de schémas dans le cours de Leibniz ou de Joh. Bernoulli

2.3. Approximation linéaire

On donne parfois une définition équivalente de la dérivation de f en x_0.
Son avantage : elle cache la question de la limite dans l'hypothèse de continuité de ϵ en x_0. .

Pour aller plus loin - Continuité = limite

Nous verrons que la notion de continuité de f en un point x_0 est équivalente à la notion d'existence de limite de f en x_0.

Proposition - Définition de Weierstrass

Soit f définie sur un intervalle I. Soit $x_0 \in I$
f est dérivable en x_0 si et seulement si
il existe $A \in \mathbb{R}$, ϵ continue en x_0 avec $\epsilon(x_0) = 0$ tels que

$$f(x) = f(x_0) + (x-x_0)(A+\epsilon(x))$$

On a alors $A = f'(x_0)$

Démonstration

Si f est dérivable en x_0, on considère $A = f'(x_0)$ et $\epsilon : x \mapsto \frac{f(x)-f(x_0)}{x-x_0} - f'(x_0)$.
Ces fonctions répondent aux conditions.
Réciproquement, si $f(x) = f(x_0) + (x-x_0)(A+\epsilon(x))$, alors $\frac{f(x)-f(x_0)}{x-x_0}$ admet une limite égale à A en x_0. □

Application - Pour quelques fonctions usuelles (connaissant les dérivées en 0

On trouve avec $\epsilon_i(x) \to 0$ pour $x \to 0$:

$$\exp(x) = 1 + x + x\epsilon_1(x)$$
$$\ln(1+x) = x + x\epsilon_2(x)$$
$$(1+x)^\alpha = 1 + \alpha x + x\epsilon_3(x)$$

C'est le début du calcul des équivalents.

Pour aller plus loin - Linéarisation

Autre idée essentielle pour l'exploitation de la dérivation : transformer un problème paramétré par une fonction plus ou moins compliquée en un autre problème linéaire. Pour cela on remplace f par une droite, la plus proche c'est-à-dire la dérivée de f (en un x_0 bien choisi).
C'est en particulier la méthode de Newton que nous reverrons en informatique. Il s'agit de resoudre $f(x) = 0$.

Définition - Équation de la tangente

Soit f définie sur I, dérivable en $x_0 \in I$.
La droite d'équation

$$y = f(x_0) + f'(x_0)(x-x_0)$$

s'appelle la tangente à la courbe représentative de f en $M(x_0, f(x_0))$

Truc & Astuce pour le calcul - A propos de la tangente

On notera :
- qu'il s'agit bien de l'équation d'une droite ($y = ax+b$)
- qu'elle passe bien par le point M : $f(x_0) + f'(x_0)(x_0-x_0) = f(x_0)$.
- que sa pente vaut $f'(x_0)$.

2.4. Règles de dérivation

Les résultats suivants seront démontrées plus tard dans l'année (linéarité de la limite). Ils ont été énoncés pour la première fois par Leibniz en 1684. Le but pour le moment est de se former pour le calcul!

Proposition - Résultats

Soient u et v dérivable en x_0
- $u+v, uv, u^n, \exp u$ sont dérivables en x_0 ;
- si, en outre, u ne s'annule pas sur un intervalle contenant x_0 et est dérivable en x_0 alors $\frac{1}{u}, \ln|u|$ sont dérivables en x_0 ;
- si, en outre, v ne s'annule pas sur un intervalle contenant x_0 et est

dérivable en x_0 alors $\frac{u}{v}$ est dérivable en x_0 ;
— si, en outre, $\alpha \in \mathbb{R}^*$ et si u est strictement positive sur un intervalle contenant x_0, alors u^α est dérivable en x_0

Si $u\circ\phi$ est définie, si φ est dérivable en x_0 et u dérivable en $\varphi(x_0)$ alors $u\circ\varphi$ est dérivable en x_0 et $(u\circ\varphi)'(x_0) = \varphi'(x_0)\times u'(\varphi(x_0))$.

Résumé :

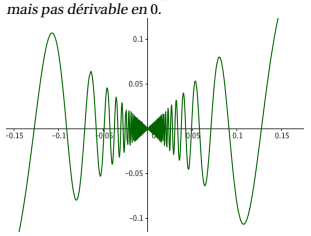
Proposition - Résumé des formules usuelles de dérivation

fonction f de la forme	fonction dérivée f'
$u+v$	$u'+v'$
uv	$u'v+uv'$
$u_1u_2\dots u_n$	$u_1'u_2\dots u_n+u_1u_2'u_3\dots u_n+\dots+u_1u_2\dots u_{n-1}u_n'$
u^n où $n\in\mathbb{N}^*$	$nu'u^{n-1}$
$\frac{1}{u}$	$\frac{-u'}{u^2}$
$\frac{u}{v}$	$\frac{u'v-uv'}{v^2}$
$u\circ\phi$	$\phi'\times u'\circ\phi = u'\circ\phi\times\phi'$
$u_1\circ\dots\circ u_n$	$(u_1'\circ u_2\circ\dots\circ u_n)\times(u_2'\circ u_3\circ\dots\circ u_n)\times\dots\times u_n'$
$\exp u$	$u'\times\exp u$
$\ln\lvert u\rvert$	$\frac{u'}{u}$
u^α où $\alpha\in\mathbb{R}^*$	$\alpha u'u^{\alpha-1}$

Ces formules sont vraies, sous réserve, évidente, de dérivabilité des fonctions qui interviennent.

Pour aller plus loin - Toutes les fonctions sont dérivables?

La fonction $x\mapsto x\cos\frac{1}{x}$ est continue sur $\mathbb{R}$, mais pas dérivable en 0.



Mais pire, il existe des fonctions partout continues et nulle part dérivable. La construction est subtile. Par exemple :

$$x\mapsto\sum_{n=1}^{+\infty}\frac{\sin(10^n\pi x)}{2^n}$$

2.5. Dérivation de fonctions usuelles

Fonctions exponentielles et logarithmes

Savoir faire - Encadrement pour le calcul de limite

Pour obtenir des résultats sur les limites (indéterminées), la meilleure stratégie est l'encadrement :
si $a(x)\leqslant b(x)\leqslant c(x)$ et que a et c admettent la même limite en x_0 égale à ℓ,
alors b admet également une limite en x_0, égale à ℓ.

Analyse - Exponentielle (naturelle) en 0

On sait que pour tout $x\in]-1,1[$, $1+x\leqslant e^x\leqslant\frac{1}{1-x}$, donc $x\leqslant e^x-1\leqslant\frac{x}{1-x}$.
Puis en divisant par $x\neq 0$:

$$1\geqslant\frac{e^x-1}{x}\geqslant\frac{1}{1-x}\ (\text{cas } x<0\qquad 1\leqslant\frac{e^x-1}{x}\leqslant\frac{1}{1-x}\ (\text{cas } x>0$$

Par encadrement : exp est dérivable en 0, de valeur égale à 1.

Proposition - Dérivation des fonctions exponentielles

exp est dérivable sur $\mathbb{R}$ et pour tout $x\in\mathbb{R}$, $\exp'(x)=\exp(x)$.
Pour $a>0$ et $a\neq 1$. Si $f:x\mapsto a^x$, alors f est dérivable sur $\mathbb{R}$ et pour tout $x\in\mathbb{R}$, $f'(x)=\ln a\times a^x$.

Savoir faire - Transférer un problème exponentiel « en a », vers « en 0 »

Si on étudie exp au voisinage de a, donc des points de la forme $a+h$ avec h proche de 0,
on exploite $\exp(a+h)=\exp a\times\exp(h)$.
Donc on factorise (à l'extérieur) par $\exp a$ et on se concentre sur une étude en ϵ, ϵ proche de 0

On appliquera souvent cette méthode dans le calcul de développement limité.

Démonstration
Soit $x_0\in\mathbb{R}$, pour tout $h=x-x_0\in\mathbb{R}$,

$$\frac{\exp(x)-\exp x_0}{x-x_0}=\frac{\exp(x_0+h)-\exp x_0}{h}=e^{x_0}\frac{e^h-1}{h}\to e^{x_0}$$

On rappelle que $a^x=\exp(x\times\ln a)$. En posant $u=\ln a(x-x_0)$:

$$\frac{a^x-a^{x_0}}{x-x_0}=\frac{\exp(x_0\ln a+h\ln a)-\exp(x_0\ln a)}{h\ln a}\times\ln a=e^{x_0\ln a}\times\ln a\frac{e^u-1}{u}\to\ln a a^{x_0}$$

car pour $x\to x_0$, on a $u\to 0$ □

Par addition et composition (démontrée plus loin)

Proposition - Fonction trigonométrique hyperbolique

Les fonctions ch, sh et th sont dérivables sur $\mathbb{R}$ et

$$\forall\ x\in\mathbb{R},\ \text{ch}'(x)=\text{sh}\,x,\ \text{sh}'(x)=\text{ch}\,x\ \text{et}\ \text{th}'(x)=1-\text{th}^2(x)=\frac{1}{\text{ch}\,x}.$$

Démonstration
$\text{ch}'(x)=e^x+(-1)e^{-x}=\text{sh}(x)$, $\text{sh}'(x)=e^x-(-1)e^{-x}=\text{ch}(x)$.
$\text{th}'(x)=\frac{\text{ch}^2(x)-\text{sh}^2(x)}{\text{ch}^2(x)}=1-\text{th}^2(x)=\frac{1}{\text{ch}^2(x)}$. □

Remarque - $\frac{\partial}{\partial x}e^{-x}$?

On peut noter que $e^{-x}=\left(e^{-1}\right)^x$, c'est une fonction exponentielle de base e^{-1}.
Donc de dérivée : $\ln(e^{-1})\times(e^{-1})^x=-e^{-x}$.

Analyse - Logarithme (naturel) en 1

On vient de voir que $\lim\limits_{x\to0}\frac{e^x-1}{x}=1$.
En composant par $X=e^x$ et donc $x=\ln X$, avec l'équivalence $x\to0\Leftrightarrow X\to1$, on a

$$\lim_{X\to1}\frac{X-1}{\ln X-\underbrace{\ln 1}_{=0}}=1$$

En prenant l'inverse, on a donc ln est dérivable en 1, de valeur égale à $\frac{1}{1}=1$.

Proposition - Dérivation des fonctions logarithmes

ln est dérivable sur $\mathbb{R}_+$ et pour tout $x\in\mathbb{R}_+$, $\ln'(x)=\frac{1}{x}$.
Si $g:x\mapsto\ln_a(x)$, alors g est dérivable sur $\mathbb{R}_+$ et pour tout $x\in\mathbb{R}_+$, $g'(x)=\frac{1}{(\ln a)\times x}$.

Savoir faire - Transférer un problème logarithme « en a », vers « en 1 »

Si on étudie ln au voisinage de a, donc des points de la forme $a+h$ avec h proche de 0,
on factorise (à l'intérieur) par a : $a+h=a(1+\frac{h}{a})$ et exploite $\ln(a+h)=\ln a+\ln(1+\frac{h}{a})$.
Et on se concentre sur une étude en $1+\epsilon$, ϵ proche de 0

On appliquera souvent cette méthode dans le calcul de développement limité.

Démonstration
Soit $x_0 \in \mathbb{R}_+$, pour tout $h = x - x_0 \in \mathbb{R}$ (et $u = \frac{x-x_0}{x_0}$),

$$\frac{\ln(x)-\ln x_0}{x-x_0} = \frac{\ln(x_0(1+\frac{h}{x_0}))-\ln x_0}{h} = \frac{1}{x_0}\times\frac{\ln(1+u)}{u} \to \frac{1}{x_0}$$

On rappelle que $\ln_a(x) = \dfrac{\ln x}{\ln a}$. Par produit (démontré plus loin), $\ln'_a(x_0) = \dfrac{1}{\ln a}\ln'(x_0) = \dfrac{1}{(\ln a)\times x_0}$ □

Fonctions puissances

Proposition - Fonctions puissances
La fonction puissance $x \mapsto x^\alpha$ est dérivable sur son ensemble de définition (privé de 0, si besoin : $\alpha - 1 < 0$ alors que $\alpha > 0$), de dérivée : $x \mapsto \alpha x^{\alpha-1}$.

Démonstration
Il faudrait étudier tous les cas $\alpha \in \mathbb{N}$, $\alpha \in \mathbb{Z}$, $\alpha \in \mathbb{Q}$.
Notons que $x \mapsto x^\alpha = \exp(\alpha \ln x)$, de dérivée (par composition) : $x \mapsto \alpha\dfrac{1}{x}\exp(\alpha\ln x) = \alpha\dfrac{x^\alpha}{x} = \alpha x^{\alpha-1}$. □

Par sommation, on retrouve ce qu'on a déjà démontré :

Proposition - Fonctions polynomiales
Les fonctions polynomiales sont dérivables sur $\mathbb{R}$ et précisément, si $f : x \mapsto \sum_{k=0}^{n} a_k x^k$, on a pour tout $x \in \mathbb{R}$, $f'(x) = \sum_{k=0}^{n} k a_k x^{k-1} = \sum_{k=1}^{n} k a_k x^{k-1} = \sum_{k=0}^{n-1}(k+1)a_{k+1}x^k$.
On notera qu'il s'agit encore d'un polynôme, de degré $\deg f - 1$.

L'ensemble de définition des fonctions puissances entières étant $\mathbb{R}$ en entier, les résultats précédents ne sont pas suffisants. Il faut refaire une démonstration.
Il serait tout de même étonnant de trouver des résultats différents…

Fonctions circulaires

Proposition - Fonction trigonométrique
sin, cos et tan sont dérivables sur leur ensemble de définition. Précisément :
$\forall\, x \in \mathbb{R}$, $\sin'(x) = \cos x$, $\forall\, x \in \mathbb{R}$, $\cos'(x) = -\sin x$. et pour tout $x \in \mathbb{R}\setminus\{\frac{\pi}{2} + k\pi, k \in \mathbb{Z}\}$, $\tan'(x) = 1 + \tan^2 x = \dfrac{1}{\cos^2 x}$.

On applique une méthode déjà connue.

Démonstration
Par encadrement (chapitre précédent) : $\dfrac{\sin x}{x} \underset{x\to 0}{\longrightarrow} 1$.
Ainsi sin est dérivable en 0 de dérivée égale à 1.
De même étudions la dérivabilité de cos en 0 :
$\cos x - 1 = \mathrm{Re}(e^{ix} - 1) = \mathrm{Re}(e^{ix/2}(2i\sin\frac{x}{2})) = -2\sin^2\frac{x}{2}$.
Donc $\dfrac{\cos x - 1}{x} = -\sin\frac{x}{2}\dfrac{\sin\frac{x}{2}}{\frac{x}{2}} \to 0$ (par produit 0×1).
Ainsi cos est dérivable en 0 de dérivée égale à 0.

Puis $\dfrac{\sin(x_0)-\sin x}{x_0 - x} = \dfrac{\sin(x_0+h)-\sin x_0}{h} = \dfrac{\sin x_0(\cos h - 1) + \sin h\cos x_0}{h} = \dfrac{\cos h - 1}{h}\sin x_0 + \dfrac{\sin h}{h}\cos x_0 \to \cos x_0$ pour $h \to 0$.
Puis $\dfrac{\cos(x_0)-\cos x}{x_0 - x} = \dfrac{\cos(x_0+h)-\cos x_0}{h} = \dfrac{\cos x_0(\cos h - 1) - \sin h\sin x_0}{h} = \dfrac{\cos h - 1}{h}\cos x_0 - \dfrac{\sin h}{h}\sin x_0 \to -\sin x_0$ pour $h \to 0$.
Pour la fonction tangente, on se souvient que $\tan(x_0+h) - \tan x_0 = \dfrac{\tan x_0 + \tan h}{1 - \tan x_0\tan h} - \tan x_0 = \dfrac{\tan h(1+\tan^2 x_0)}{1+\tan x_0\tan h}$.
Donc $\dfrac{\tan(x_0+h)-\tan x_0}{h} = \dfrac{\sin h}{h}(1+\tan^2 x_0)\dfrac{1}{\cos h(1+\tan x_0\tan h)} \underset{h\to 0}{\longrightarrow} 1 + \tan^2(x_0) = \dfrac{1}{\cos^2 x_0}$
□

Les résultats sur les dérivées des fonctions réciproques arcsin… seront vus loin lorsqu'on étudiera la dérivation de fonctions réciproques.

2.6. Dérivées seconde, troisième...

Définition - Dérivables
Soient I un intervalle et f une fonction définie sur I.
On dit que f est deux fois dérivable sur I si f est dérivable sur I et si f' est elle-même dérivable sur I, on note f'' la dérivée seconde de f (c'est-à-dire la dérivée de f').
Si f'' est encore dérivable sur I, on dit que f est trois fois dérivable sur I et on note $f''' = f^{(3)} = (f'')'$ sa dérivée troisième, et ainsi de suite.

Définition - Fonction de classe $\mathscr{C}^k$
On dit que f est de classe $\mathscr{C}^1$ ou continûment dérivable si elle est dérivable et que f' est continue, de classe $\mathscr{C}^2$ ou 2 fois continûment dérivable si elle est deux fois dérivable et que f'' est continue...

Comme les dérivées des fonctions usuelles vues plus haut sont de la forme de fonctions usuelles, par récurrence :

Proposition - Fonctions usuelles
Les fonctions usuelles vues précédemment sont de classe $\mathscr{C}^\infty$ sur leur ensemble de définition (sauf les fonctions puissances $x \mapsto x^\alpha$ qui peuvent perdre le 0 dans l'ensemble à la dérivée n-ième si $n > \alpha$…).

3. Quelques utilisations de la dérivation

3.1. Variations

En utilisant les théorèmes suivants (qui seront démontrés ultérieurement), on peut étudier les variations d'une fonction que l'on résume **systématiquement** dans un tableau de variations, complété par les limites aux bornes (et non par des phrases !)

Théorème - Monotonie et fonction dérivée
Soient I un **intervalle** de $\mathbb{R}$ et f une fonction dérivable sur I. Alors :
f est constante sur I si et seulement si $\forall x \in I$, $f'(x) = 0$;
f est croissante sur I si et seulement si $\forall x \in I$, $f'(x) \geqslant 0$;
f est décroissante sur I si et seulement si $\forall x \in I$, $f'(x) \leqslant 0$.
Si $f' > 0$ (resp. $f' < 0$) sauf en un nombre fini de points de I, alors f est

strictement croissante (resp. décroissante) sur I.

Attention - Intervalle!
Il est indispensable que I soit un intervalle. On peut en effet trouver f définie sur D, dérivable sur D et vérifiant $\forall x \in D$, $f'(x) < 0$ mais qui n'est pas décroissante sur D.

Exercice
Donner un tel contre-exemple

Correction

3.2. Bijections et réciproques

Théorème - Dérivation de la bijection réciproque
Soient I, J deux intervalles de $\mathbb{R}$ et $f : I \to J$ bijective de I sur J. On suppose que f est dérivable en $x_0 \in I$.
Alors f^{-1} est dérivable en $f(x_0)$ **si et seulement si** $f'(x_0) \neq 0$
et on a alors

$$(f^{-1})'(f(x_0)) = \frac{1}{f'(x_0)}$$

ou encore, avec $y_0 = f(x_0)$,

$$(f^{-1})'(y_0) = \frac{1}{f' \circ f^{-1}(y_0)}$$

Remarque - Se souvenir
On peut retrouver la formule en dérivant l'égalité $f^{-1} \circ f = \mathrm{Id}$, en effet :

$$(f^{-1} \circ f)' = f' \times (f^{-1})' \circ f = (\mathrm{Id})' = (x \mapsto 1)$$

mais attention à ne pas oublier la condition de dérivabilité de f^{-1} !
Si $f'(x) \neq 0$: $(f^{-1})'(f(x)) = \dfrac{1}{f'(x)}$ si $y = f(x)$ et $f'(x) = f'(f^{-1}(y)) \neq 0$:

$$(f^{-1})'(y) = \frac{1}{f'(f^{-1}(y))}$$

Proposition - Fonctions trigonométriques réciproques
Les fonctions arcsin et arccos sont de classe $\mathscr{C}^\infty$ sur $]-1,1[$,
avec $\forall\, x \in]-1,1[$, $\arcsin'(x) = \dfrac{1}{\sqrt{1-x^2}}$ et $\arccos'(x) = \dfrac{-1}{\sqrt{1-x^2}}$.
La fonction arctan est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$,
avec $\forall\, x \in \mathbb{R}$, $\arctan'(x) = \dfrac{1}{1+x^2}$

Démonstration
$x \in \mathscr{D}_{(\sin^{-1})'} \iff \sin'(\arcsin(x)) \neq 0 \iff \cos(\arcsin(x) \neq 0 \iff \arcsin x \notin \{-\frac{\pi}{2}, \frac{\pi}{2}\} \iff x \notin \{-1,1\}$.
Donc $\mathscr{D}_{\arcsin'} =]-1,1[$ et
$\forall\, x \in]-1,1[$, $\arcsin'(x) = \dfrac{1}{\cos(\arcsin(x))} = \dfrac{1}{\sqrt{1-x^2}}$.
$x \in \mathscr{D}_{(\cos^{-1})'} \iff \cos'(\arccos(x)) \neq 0 \iff \sin(\arccos(x) \neq 0 \iff \arccos x \notin \{0,\pi\} \iff x \notin \{-1,1\}$.
Donc $\mathscr{D}_{\arccos'} =]-1,1[$ et
$\forall\, x \in]-1,1[$, $\arccos'(x) = \dfrac{1}{-\sin(\arccos(x))} = \dfrac{-1}{\sqrt{1-x^2}}$.
$x \in \mathscr{D}_{(\tan^{-1})'} \iff \tan'(\arctan(x)) \neq 0 \iff x \notin \{\frac{\pi}{2} + 2k\pi, k \in \mathbb{Z}\}$.
Or cette dernière affirmation est toujours vraie. Donc $\mathscr{D}_{\arctan'} = \mathbb{R}$ et
$\forall\, x \in \mathbb{R}$, $\arctan'(x) = \dfrac{1}{\tan'(\arctan(x))} = \dfrac{1}{1+\tan^2(\arctan x)} = \dfrac{1}{1+x^2}$. □

Pour aller plus loin - Création de fonctions
Dans un autre sens, on peut considérer :
1. *f strictement monotone et continue de I sur J.*
2. *Donc f admet une fonction réciproque f^{-1} de J sur I.*

Corollaire -
Si $f : I \to \mathbb{R}$ est :
— continue strictement monotone sur l'intervalle I,
— dérivable sur I et
— $\forall x \in I$, $f'(x) \neq 0$
alors f est bijective de I sur $J = f(I)$, donc $f^{-1} : J \to I$ existe (et est bijective).
Mieux : f^{-1} est dérivable sur J et $(f^{-1})' = \dfrac{1}{f' \circ f^{-1}}$.
Graphiquement : $\mathscr{C}_{f^{-1}}$ est la symétrique de $\mathscr{C}_f$ par rapport à l'axe $y = x$.

Savoir faire - Etudier si f est un $\mathscr{C}^1$-difféomorphisme
On considère f, de classe $\mathscr{C}^1$ sur un intervalle I.

1. On coupe I, en réunion d'intervalles $I_1, I_2, \dots I_n$ sur lesquels f est strictement monotone
   (A noter que cela n'est pas toujours possible.... Donnez des contre-exemple).
   Cela conduit à étudier le signe strictement non nul de f'. Les frontières sont en dans $\{x \mid f'(x) = 0\}$.
2. Sur chaque intervalle I_k, on note $J_k = \{y = f(x), x \in I_k\}$ et donc $f_k = f^{|J_k}_{|I_k} : I_k \to J_k$ est bijective.
3. Puis, on considère $J'_k = \{y = f(x), x \in I_k \mid f'(x) \neq 0\} \subset J_k$.
   (Souvent les problèmes sont sur les bords des J_k, lié à la jonction de I_k et I_{k+1} ou I_{k-1}, mais cela n'est pas nécessaire).
   Alors $f_k^{-1} : J_k \to I_k$ est de classe $\mathscr{C}^1$ sur J'_k et pour tout $y \in J'_k$:

$$(f^{-1})'(y) = (f_k^{-1})'(y) = \frac{1}{f'(f_k^{-1}(y)} = \frac{1}{f'(f^{-1}(y)}$$

Gardons en mémoire que graphiquement : $\mathscr{C}_{f^{-1}}$ est la symétrique de $\mathscr{C}_f$ par rapport à l'axe $y = x$.
Les cas problématique correspond à une pente nulle pour $\mathscr{C}_f$ et donc infinie pour $\mathscr{C}_{f^{-1}}$...

Exercice
La fonction sh réalise une bijection de $\mathbb{R}$ sur $\mathbb{R}$. La bijection réciproque est notée argsh (argument sinus hyperbolique).
La fonction ch réalise une bijection de $[0,+\infty[$ sur $[1,+\infty[$. La bijection réciproque est notée argch (argument cosinus hyperbolique).
La fonction th réalise une bijection de $\mathbb{R}$ sur $]-1,1[$. La bijection réciproque est notée argth (argument tangente hyperbolique).

1. Dérivées.
   (a) Montrer que les fonctions argsh, argch, argth sont dérivables respectivement sur $\mathbb{R}$, $]1,+\infty[$ et $]-1,1[$.
   (b) Montrer que $(\mathrm{argsh})'(x) = \frac{1}{\sqrt{x^2+1}}$ sur $\mathbb{R}$
   (c) Montrer que $(\mathrm{argch})'(x) = \frac{1}{\sqrt{x^2-1}}$ sur $]1,+\infty[$
   (d) Montrer que $(\mathrm{argth})'(x) = \frac{1}{1-x^2}$ sur $]-1,1[$
2. Expressions logarithmiques.
   (a) Montrer que $\forall x \in \mathbb{R}$, $\mathrm{argsh}\, x = \ln(x + \sqrt{x^2+1})$
   (b) Montrer que $\forall x \in]1,+\infty[$, $\mathrm{argch}\, x = \ln(x + \sqrt{x^2-1})$
   (c) Montrer que $\forall x \in]-1,1[$, $\mathrm{argth}\, x = \frac{1}{2}\ln\frac{1+x}{1-x}$

Correction

3.3. Inégalités

Savoir faire - Obtenir une inégalité

Pour démontrer une inégalité, une méthode est d'étudier la fonction formée par la différence des deux membres, d'établir son tableau de variations pour obtenir son signe.

Exercice

Montrer les inégalités :

$$\forall x \in \mathbb{R},\ 1-\frac{x^2}{2} \leqslant \cos x \leqslant 1;$$

$$\forall x \in \mathbb{R}^+,\ x-\frac{x^3}{6} \leqslant \sin x \leqslant x;$$

$$\forall x \in \mathbb{R}^-,\ x-\frac{x^3}{6} \geqslant \sin x \geqslant x.$$

Correction

Commençons par noter que $\forall\ x \in \mathbb{R}$, $\cos x \leqslant 1$.

Les fonctions sin, cos et polynomiales sont dérivables sur $\mathbb{R}$, de même de leurs additions :

$$f_1 : x \mapsto \cos x - 1 + \frac{x^2}{2} \qquad f_2 : x \mapsto \sin x - x \qquad f_3 : x \mapsto \sin x - x + \frac{x^3}{6}$$

Les dérivées sont respectivement :

$$f_1' : x \mapsto -\sin x + x \qquad f_2' : x \mapsto \cos x - 1 \qquad f_3' : x \mapsto \cos x - 1 + \frac{x^2}{2}$$

On en déduit les tableaux de variations dans l'ordre déductif suivant :

x	$-\infty$		0		$+\infty$
f_2'		$-$		$-$	
f_2		↘	0	↘	
$f_1'(=-f_2)$		$-$	0	$+$	
f_1		↘	0	↗	
$f_3'(=f_1)$		$+$	0	$+$	
f_3		↗	0	↗	

Donc $\cos x \leqslant 1$ et pour $x \in \mathbb{R}_+$, $f_1(x) \geqslant 0$, donc $\cos x \geqslant 1 - x$.

Et pour tout $x \in \mathbb{R}_+$, $f_3(x) \geqslant 0$, donc $\sin x \geqslant x - \frac{x^3}{6}$ et $f_2(x) \leqslant 0$ donc $\sin x \leqslant x$.

Et pour tout $x \in \mathbb{R}_-$, $f_3(x) \leqslant 0$, donc $\sin x \leqslant x - \frac{x^3}{6}$ et $f_2(x) \geqslant 0$ donc $\sin x \geqslant x$.

Savoir faire - Obtenir un maximum (avec une dérivée)

Pour obtenir un extremum de f (dérivable deux fois) sur I, on résout $f'(x) = 0$.

On note x_0 la solution de cette équation (donc $f'(x_0) = 0$).

- si $f''(x_0) > 0$, alors f présente un minimum (local) en x_0.
- si $f''(x_0) < 0$, alors f présente un maximum (local) en x_0.
- si $f''(x_0) = 0$, alors on ne peut rien dire.

Remarque - Convexité

On rappelle que si pour tout $x \in I$, $f''(x) \geqslant 0$, on dit que f est convexe sur I.

3.4. Calculs de limites (lever les indéterminations)

On peut calculer certaines limites en reconnaissant le taux de variations d'une fonction dérivable connue.

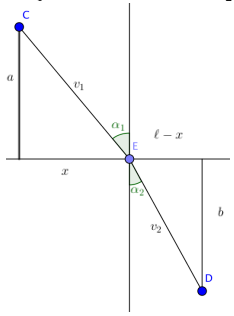
Exercice

Rappeler les valeurs des limites suivantes :

$$\lim_{x\to 0}\frac{\sin x}{x};\quad \lim_{x\to 0}\frac{\tan x}{x};\quad \lim_{x\to 0}\frac{\cos x-1}{x}.$$

Pour aller plus loin - Querelle entre Fermat et Descartes

Fermat et Descartes se sont querellés sur les lois de refraction (loi de Snell-Descartes). Pour Fermat, la démonstration de Descartes était incomplète. Le Toulousain proposait de trouver le chemin le plus rapide pour aller de C à D, sachant que la vitesse dans le premier milieu est v_1 et celle dans le second est v_2.



Paramétrons ce chemin par x (abscisse de E). On a à minimiser :

$$T(x) = \frac{\sqrt{a^2+x^2}}{v_1} + \frac{\sqrt{b^2+(\ell-x)^2}}{v_2}$$

Et comme $\sin\alpha_1 = \frac{x}{\sqrt{a^2+x^2}}$ *et* $\sin\alpha_2 = \frac{\ell-x}{\sqrt{b^2+(\ell-x)^2}}$, *on retrouve* $\frac{\sin\alpha_1}{v_1} = \frac{\sin\alpha_2}{v_2}$.

En déduire

$$\lim_{x\to 0}\frac{\cos x-1}{x^2}$$

Correction

Il s'agit de limite de taux de variations donc d'un calcul de dérivée :

$\lim_{x\to 0}\frac{\sin x}{x} = \sin'(0) = \cos(0) = 1$, $\frac{\tan x}{x} = \tan'(0) = 1+\tan^2(0) = 1$ et $\lim_{x\to 0}\frac{\cos x-1}{x} = \cos'(0) = \sin(0) = 0$.

Enfin, en posant $u = \frac{x}{2}$:

$$\frac{\cos x-1}{x^2} = -2\frac{\sin^2(\frac{x}{2})}{x^2} = -\frac{\sin^2(u)}{2u^2} = -\frac{\sin^2(u)}{2u^2} = \frac{-1}{2}\left(\frac{\sin u}{u}\right)^2$$

En faisant tendre $x \to 0$, donc $u \to 0$, on a par produit de limite : $\lim_{x\to 0}\frac{\cos x-1}{x^2} = -\frac{1}{2}\times 1^2 = -\frac{1}{2}$

Proposition - Règle de L'Hospital (1696)

Soient f et g deux fonctions définies sur I, dérivables en $x_0 \in I$.

On suppose que $f(x_0) = g(x_0) = 0$ et que $\frac{f'}{g'}$ admet une limite en x_0.

Alors $\lim_{x\to x_0}\frac{f(x)}{g(x)} = \lim_{x\to x_0}\frac{f'(x)}{g'(x)}$

On fait la démonstration dans le cas où $g'(x_0) \neq 0$. Sinon, on exploitera l'inégalité des accroissements finis (dans un chapitre prochain).

Démonstration

Avec les notations de Weierstrass :

$$f(x) = (x-x0)(f'(x_0)+\epsilon_1(x)) \qquad g(x) = (x-x0)(g'(x_0)+\epsilon_2(x))$$

$$\frac{f(x)}{g(x)} = \frac{f'(x_0)+\epsilon_1(x)}{g'(x_0)+\epsilon_2(x)} \underset{x\to x_0}{\longrightarrow} \frac{f'(x_0)}{g'(x_0)}$$

□

Pour aller plus loin - Généralisation en $+\infty$

Il existe une généralisation de la règle de L'Hôpital avec une indétermination du type $\frac{+\infty}{+\infty}$.

Si $\lim_a |f| = \lim_a |g| = +\infty$ *et si* $\lim_a \frac{f'}{g'} = \ell$, *alors* $\lim_a \frac{f}{g} = \ell$

Attention - Pas d'abus

La règle ne s'applique qu'en cas d'indetermination.

$$-4 = \lim_{x\to 1}\frac{3x^2+1}{2x-3} \neq \lim_{x\to 1}\frac{6x}{2} = 3$$

Savoir faire - Lever une indétermination par la règle de L'Hospital

1. D'abord on vérifie bien qu'on peut appliquer la règle de L'Hospital :

$$f = \frac{n}{d} \text{ avec } n(x) \underset{x\to a}{\longrightarrow} 0 \text{ et } d(x) \underset{x\to a}{\longrightarrow} 0$$

2. On calcule $n'(x)$, $n''(x)\ldots n^{(k)}(x)\ldots$ jusque à ce que $n^{(k)}(x) \underset{x\to a}{\not\longrightarrow} 0$

   Et de même $d'(x)$, $d''(x)\ldots d^{(\ell)}(x)\ldots$ jusqu'à ce que $d^{(\ell)}(x) \underset{x\to a}{\not\longrightarrow} 0$.

3. On note $m = \min\{k \in \mathbb{N} \mid n^{(k)}(x) \not\to 0 \text{ ou } d^{(k)}(x) \not\to 0\}$.

Et on connait donc $\lim_a \frac{n^{(k)}}{d^{(k)}}$, et par la règle de L'Hospital : $\lim_a \frac{n^{(k-1)}}{d^{(k-1)}}$ a la même valeur.

4. Et on remonte ainsi à $\lim_a \frac{n}{d}$, dont on sait seulement maintenant qu'elle existe et qu'elle a cette même valeur.

Exercice

Calculer $\lim_{x\to 0} \dfrac{\cos 2x - 1}{x^3 + 5x^2}$.

Evidemment, on exploitera les résultats non encore démontrés sur les fonctions usuelles

Correction

On note $f : x \mapsto \cos 2x - 1$, dérivable, $f'(x) = -2\sin(2x)$, donc $f'(0) = 0$.
On note $g : x \mapsto x^3 + 5x^2$, dérivable, $g'(x) = 3x^2 + 10x$, donc $g'(0) = 0$.
On a toujours une forme indéterminée.
On reprend avec $f''(x) = -4\cos(2x)$, donc $f''(0) = -4$.
Et $g''(x) = 6x + 10$ donc $g''(0) = 10$.
Ainsi

$$\lim_{x\to 0} \frac{f(x)}{g(x)} = \lim_{x\to 0} \frac{f'(x)}{g'(x)} = \frac{-4}{10} = \frac{-2}{5}$$

3.5. Approximation polynomiale (développement limité)

Heuristique - Approximation polynomiale LOCALE

Nos fonctions usuelles ne sont pas des polynômes, on ne cherche par à remplacer une fonction usuelle par une fonction polynomiale sur un intervalle de $\mathbb{R}$ contenant une infinité de points.
Mais on peut faire des comparaison au voisinage d'un point.
La définition de Weierstrass de la dérivabilité de φ en x_0 avec pour valeur $A(=\varphi'(x_0))$ exprime :

$\exists\, A \in \mathbb{R}, \exists\, \epsilon : I \to \mathbb{R}$ continue en x_0 avec $\epsilon(x_0) = 0 \mid \forall\, x \in I, \varphi(x) = \varphi(x_0) + A(x - x_0) + (x - x_0)\epsilon(x)$

On va donc chercher une fonction polynomiale f de degré n tel que

$$\varphi(x) = f(x) + (x - x_0)^n \epsilon(x) \qquad \text{avec } \epsilon(x) \underset{x\to x_0}{\longrightarrow} 0$$

On commence par étudier les cas $x_0 = 0$.

Proposition - Développement polynomiale en 0

Soit $n \in \mathbb{N}^*$.
On considère φ de classe C^{n+1} sur I, contenant 0.
On note $T : x \mapsto \sum_{k=0}^{n} \dfrac{f^{(k)}(0)}{k!}$. Alors

$$\lim_{x\to 0} \frac{\varphi(x) - T(x)}{x^n}$$

Autrement écrit : il existe $\epsilon : I \to \mathbb{R}$ tel que $\epsilon(x) \underset{x\to 0}{\longrightarrow} 0$ et $f(x) = T(x) + x^n\epsilon(x)$.

On commence par un lemme (qui sera enrichit dans la suite du cours)

Lemme - Dérivation monôme

Notons $m_s : x \mapsto x^s$.
Alors pour tout $k \in \mathbb{N}$, $m_s^{(k)}(0) = 0$ si $k \neq s$ et $m_s^{(s)}(0) = s!$.

Commençons par démontrer le lemme

Démonstration

Pour le lemme, on remarque que m_s est une fonction polynomiale donc de classe $\mathscr{C}^\infty$.
Par récurrence (finie), on note pour $k \leqslant s$, $\mathscr{P}_k : m_s^{(k)} : x \mapsto \dfrac{s!}{(s-k)!} x^{s-k}$.

- $\mathscr{P}_0$ est vraie
- Soit $k \leqslant s-1$. Supposons que $\mathscr{P}_k$ est vraie.

$$m_s^{(k+1)}(x) = (m_s^{(k)})'(x) = \left(x \mapsto \frac{s!}{(s-k)!} x^{s-k}\right)'(x) = \frac{(s-k)\times s!}{(s-k)!} x^{s-k-1} = \frac{s!}{(s-k-1)!} x^{s-k-1}$$

Donc $\mathscr{P}_{k+1}$ est vraie.

On a donc, ensuite, $m_s^{(s)}(x) = s!$ (constante) et pour tout $k > s$, $m_s^{(k)}(x) = 0$, en particulier $m_s^{(k)}(0) = 0$.
□

Démonstration

On applique la règle de L'hopsital.
1. Notons $den : x \mapsto x^n$. Donc $den = s_n$.
En application directe du lemme : $den^{(k)}(0) = 0$ si $k \leqslant n-1$ et $den^{(n)}(0) = n!(\neq 0)$.
2. Notons $num : x \mapsto f(x) - T(x)$.
Par linéarité (addition ici) n est de classe $\mathscr{C}^n$ et pour tout $k \leqslant n$, $(f-T)^{(k)}(0) = f^{(k)}(0) - T^{(k)}(0)$.
Puis par linéarité de la dérivation d'un polynôme (pour $k \leqslant n$) :

$$T^{(k)} = \left(\sum_{i=0}^{n} [T]_i s_i\right)^{(k)} = \sum_{i=0}^{n} [T]_i s_i^{(k)} = 0 + \cdots + 0 + [T]_k k! + 0 + \cdots + 0 = f^{(k)}(0)$$

On a donc $num^{(k)}(0) = 0$, pour tout $k \leqslant n$. On peut enfin appliquer la règle de L'Hospital en remontant : Pour tout k de 1 à n, $\dfrac{num^{n-k}}{den^{n-k}} \underset{x\to 0}{\longrightarrow} 0$ □

Exemple - DL de $x \mapsto (1+x)^\alpha$ ($\alpha \notin \mathbb{N}$)

Notons $f_\alpha : x \mapsto (1+x)^\alpha$.
Alors $f'_\alpha(x) = \alpha(1+x)^{\alpha-1}$, et par récurrence :

$$f_\alpha^{(k)}(x) = \prod_{i=0}^{k-1} (\alpha - i) \times (1+x)^{\alpha-k}$$

Et donc $f(x) = \sum_{k=0}^{n} \dfrac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} x^k + x^n\epsilon(x)$.

Exercice

Quelle formule obtient-on pour $\alpha = -1$?

Correction

La formule de Lagoute $\dfrac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots + (-1)^n x^n + x^n\epsilon(x)$ ou suite géomtérique

Exercice

1. Donner une équation différentielle simple vérifiée par exp
2. En déduire le $DL_n(0)$ de exp.
3. En déduire le $DL_n(0)$ de ch et sh
4. Exprimer, pour tout $n \in \mathbb{N}$, la dérivée n-ième de $x \mapsto e^{ix}$.
5. En déduire le $DL_n(0)$ de cos et sin

Correction

1. On note $y = \exp$, on a $y' = y$.
2. Par récurrence immédiate : $y^{(n)} = y = \exp$ et donc $\exp^{(n)}(0) = e^0 = 1$.
Donc pour x proche de 0, $\exp(x) = \sum_{k=0}^{n} \frac{1}{k!} x^k + x^n\epsilon(x)$.
3. Par linéarité de la dérivation (ou du calcul polynomial) ou par périodicité des dérivées :
Pour x proche de 0, $\mathrm{ch}(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{(2k)!} x^{2k} + x^n\epsilon(x)$
Pour x proche de 0, $\mathrm{sh}(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{1}{(2k+1)!} x^{2k+1} + x^n\epsilon(x)$
4. Notons $E : x \mapsto e^{ix}$, on a $E^{(n)} = i^n e^{ix} = e^{ix + n\frac{\pi}{2}} = \cos(x + n\frac{\pi}{2}) + i\sin(x + n\frac{\pi}{2})$.
En prenant les parties réelles et imaginaires :
Pour x proche de 0, $\cos(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{1}{(2k)!} x^{2k} + x^n\epsilon(x)$
Pour x proche de 0, $\sin(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{1}{(2k+1)!} x^{2k+1} + x^n\epsilon(x)$

4. Dérivation de fonctions réelles à valeurs complexes

4.1. Fonctions à valeurs complexes

Aparté. L'exponentielle complexe

Définition - Exponentielle complexe
Soit $z \in \mathbb{C}$. On définit l'exponentielle complexe de z par

$$\exp z = e^z = e^{\mathrm{Re}(z)} e^{i\mathrm{Im}(z)}.$$

Son module est $e^{\mathrm{Re}(z)}$ et un argument est $\mathrm{Im}(z)$.

Proposition - Elargissement
On retrouve les propriétés classiques de l'exponentielle :
- L'exponentielle complexe coïncide bien avec l'exponentielle sur $\mathbb{R}$ pour les réels ou avec l'exponentielle des imaginaires purs.
- Pour $(z,z') \in \mathbb{C}^2$, on a : $e^{z+z'} = e^z e^{z'}$ et $\dfrac{1}{e^z} = e^{-z}$.

Démonstration
Si $z = a + 0i \in \mathbb{R}$, alors $\exp(z) = e^a$.
Si $z = a + ib$ et $z' = a' + ib'$ (notation standard), alors

$$e^{z+z'} = e^{(a+a')+i(b+b')} = e^{a+a'} e^{i(b+b')} = e^a e^{a'} e^{ib} e^{ib'} = e^{a+ib} e^{a'+ib'} = e^z e^{z'}$$

En particulier :

$$e^{-z} e^z = e^{-z+z} = e^0 = 1 \qquad \Longrightarrow \qquad e^{-z} = \frac{1}{e^z}$$

□

Exercice
1. Résoudre $e^z = 1$.
2. Résoudre $e^z = 1 - i\sqrt{3}$.
3. Résoudre plus généralement $e^z = z_0$
4. Déterminer l'image d'une droite d'équation $x = a$ par l'application $\exp : \mathbb{C} \to \mathbb{C}^*$.
5. Déterminer l'image d'une droite d'équation $y = b$ par l'application $\exp : \mathbb{C} \to \mathbb{C}^*$.

Correction

1. Soit $z \in \mathbb{C}$.
$$e^z = 1 \Longleftrightarrow \mathrm{Re}(z) = 0, \mathrm{Im}(z) \equiv 0[2\pi] \Longleftrightarrow z \in \{2ik\pi, k \in \mathbb{Z}\}$$
2. Soit $z \in \mathbb{C}$
$$e^z = 1 - i\sqrt{3} \Longleftrightarrow e^{\mathrm{Re}(z)} = \sqrt{1+3} = 2, \mathrm{Im}(z) \equiv \frac{\pi}{3}[2\pi] \Longleftrightarrow z \in \{\ln 2 + i(\frac{\pi}{3} + 2k\pi), k \in \mathbb{Z}\}$$
3. Résoudre plus généralement $e^z = z_0$.
$$e^z = z_0 \Longleftrightarrow e^{\mathrm{Re}(z)} = |z_0|, \mathrm{Im}(z) \equiv \arg(z_0)[2\pi] \Longleftrightarrow z \in \{\ln|z_0| + i(\arg(z_0) + 2k\pi), k \in \mathbb{Z}\}$$
4. Déterminer l'image d'une droite $\mathscr{D}_a$ d'équation $x = a$ par l'application $\exp : \mathbb{C} \to \mathbb{C}^*$.
$z \in \mathscr{D}_a \Longleftrightarrow \exists\, y \in \mathbb{R} \mid z = a + iy$. Et $\exp(z) = e^a e^{iy}$. Donc :
$$\exp(\mathscr{D}_a) = \mathscr{C}_{e^a},$$
cercle de centre O et de rayon e^a.
Il faudrait vérifier (trivialement) l'inclusion réciproque...
5. Déterminer l'image d'une droite $\mathscr{D}_b$ d'équation $y = b$ par l'application $\exp : \mathbb{C} \to \mathbb{C}^*$.
$z \in \mathscr{D}_b \Longleftrightarrow \exists\, x \in \mathbb{R} \mid z = x + ib$. Et $\exp(z) = e^x e^{ib}$. Donc :
$$\exp(\mathscr{D}_a) = \mathscr{D}_{\theta_b},$$
demi-droite d'origine O et faisant un angle b avec l'axe des abscisses.
Il faudrait vérifier (trivialement) l'inclusion réciproque...

Proposition - Résolution d'équation
- Pour $(z,z') \in \mathbb{C}^2$, $\exp z = \exp z'$ si et seulement si $z - z' \in 2i\pi\mathbb{Z}$.
- Tout complexe $z_0 \neq 0$ peut s'écrire sous la forme $\exp z$.

Démonstration
Notons $z = a + ib$ et $z' = a' + ib'$.

$$e^z = e^{z'} \Longleftrightarrow e^a e^{ib} = e^{a'} e^{ib'} \Longleftrightarrow \begin{cases} e^a = e^{a'} \\ b \equiv b'[2\pi] \end{cases} \Longleftrightarrow z - z' \in 2i\pi\mathbb{Z}$$

Par construction, si $z_0 \neq 0$, en prenant $z = \ln(|z_0|) + i\arg(z_0)$ (possible car $|z_0| \neq 0$) :

$$e^z = e^{\ln(|z_0|)} e^{i\arg(z_0)} = |z_0| e^{i\arg(z_0)} = z_0$$

□

Fonctions d'une variable réelle, à valeurs complexes

I désigne un intervalle de $\mathbb{R}$.

Définition - Découpage d'une fonction à valeurs dans $\mathbb{C}$
Soient $f_1 : I \to \mathbb{R}$ et $f_2 : I \to \mathbb{R}$. On pose : $\forall x \in I,\ f(x) = f_1(x) + i f_2(x)$.
$f : I \to \mathbb{C}$ est une fonction définie sur I à valeurs dans $\mathbb{C}$ *(si I n'est pas précisé au départ, son domaine de définition est l'intersection de ceux de f_1 et f_2).*
On définit les fonctions $\mathrm{Re}(f)$ (partie réelle de f) et $\mathrm{Im}(f)$ (partie imaginaire de f) à valeurs dans $\mathbb{R}$ par

$$\mathrm{Re}(f) = f_1 : \begin{array}{ccc} I & \to & \mathbb{R} \\ x & \mapsto & \mathrm{Re}(f(x)) \end{array} \qquad \mathrm{Im}(f) = f_2 : \begin{array}{ccc} I & \to & \mathbb{R} \\ x & \mapsto & \mathrm{Im}(f(x)) \end{array}$$

On dit que f est continue sur I si f_1 et f_2 sont continues sur I.

Exemple - $t \mapsto e^{it}$
L'exemple classique (simple) est la fonction circulaire exponentielle : $\exp_i : t \mapsto \cos t + i\sin t$.
Sa partie réelle est la fonction cosinus et sa partie imaginaire est la fonction sinus.
On a vu qu'il s'agissait bien d'une fonction exponentielle car vérifiant :

$$\exp_i(a+b) = \exp_i(a) \times \exp_i(b)$$

mais à valeurs complexes et non réels (donc on perd $\exp_i(a) > 0$, les limites à l'infini,...).
Analyse - Justifions que sa base est bien e^i
On a défini $\exp(x) = e^x$ comme la limite de $x_n = \left(1 + \frac{x}{n}\right)^n$.
Que se passe-t-il si l'on considère $x = it$?
x_n est alors une suite à valeurs complexes dont le module est. :

$$\left|1 + \frac{ix}{n}\right|^n = \sqrt{\left(1 - \frac{x^2}{n^2}\right)^n}$$

Comme $\frac{x^2}{n}$ tend vers 0, à partir d'un certain rang :

$$1 - n\frac{x^2}{n^2} \leqslant \left(1 - \frac{x^2}{n^2}\right)^n \leqslant \frac{1}{1 + n\frac{x^2}{n^2}}$$

Le deux termes à gauche et à droite tendent vers 1, par encadrement (et continuité de $\sqrt{\cdot}$), $|x_n| \to \sqrt{1} = 1$.
Et si θ_n est l'argument de x_n, on a

$$\theta_n = \arg\left(1 + \frac{ix}{n}\right)^n = n\arg(1 + i\frac{x}{n}) = n\arctan\frac{x}{n}$$

On démontre que pour $u \to 0$, $\frac{\arctan u}{u} \to 1$, donc $\dfrac{\arctan\frac{x}{n}}{\frac{x}{n}} \to 1$ et donc $\theta_n \to x$.
Ainsi $x_n \to \cos x + i\sin x$, ce qui justifie officiellement le signe égal de $e^{ix} = \cos x + i\sin x$.

4.2. Dérivation d'une fonctions d'une variable réelle, à valeurs complexes

I désigne un intervalle de $\mathbb{R}$.

Définition - Dérivation d'une fonction à valeurs dans $\mathbb{C}$
Soit $f : \mathbb{R} \to \mathbb{C}$, une fonction à valeurs complexes.
Soient $f_1 : I \to \mathbb{R}$ et $f_2 : I \to \mathbb{R}$ telles que $\forall x \in I$, $f(x) = f_1(x) + i f_2(x)$.
On dit que f est dérivable, respectivement de classe $\mathscr{C}^1$ sur I si f_1 et f_2 sont dérivables, respectivement de classe $\mathscr{C}^1$ sur I.
Si f est dérivable sur I, on définit sa dérivée par :

$$\forall x \in I, \quad f'(x) = f_1'(x) + i f_2'(x).$$

On note $\mathscr{C}(I, \mathbb{C})$ (resp. $\mathscr{C}^1(I, \mathbb{C})$) l'ensemble des fonctions continues (resp. de classe $\mathscr{C}^1$ de I dans $\mathbb{C}$).

Remarque - Commutativité de la dérivation complexe et de la partie réelle ou imaginaire
Si f à valeurs complexes est dérivable on a donc $(\mathrm{Re}(f))' = \mathrm{Re}(f')$ et $(\mathrm{Im}(f))' = \mathrm{Im}(f')$.

Proposition - Constance et dérivation
Soit $f : I \to \mathbb{C}$ dérivable sur I. Alors f est constante sur I si et seulement si f' est nulle sur I.

Pour la démonstration, on admet ces résultats pour des fonctions de $\mathbb{R}$ dans $\mathbb{R}$.

Démonstration
Sur I :

$$f' = 0 \iff \begin{cases} f_1' = 0 \\ f_2' = 0 \end{cases} \iff \begin{cases} f_1 \text{ constante} \\ f_2 \text{ constante} \end{cases} \iff f \text{ constante}$$

□

4.3. Propriétés

Attention - Croissance sur $\mathbb{C}$?
Parler de croissance (ou de décroissance) d'une fonction à valeurs dans $\mathbb{C}$ n'a pas de sens.

Proposition - Opérations
Soient f et g deux fonctions dérivables sur I à valeurs dans $\mathbb{C}$ et $\alpha \in \mathbb{C}$. Alors $f+g$, fg et αf sont dérivables sur I et

$$\begin{aligned} \forall x \in I, \quad (f+g)'(x) &= f'(x) + g'(x) \\ (fg)'(x) &= f'(x)\,g(x) + f(x)\,g'(x) \\ (\alpha f)' &= \alpha f' \end{aligned}$$

Si g ne s'annule pas, alors $\frac{1}{g}$ et $\frac{f}{g}$ sont dérivables sur I et

$$\begin{aligned} \forall x \in I, \quad \left(\frac{1}{g}\right)'(x) &= \frac{-g'(x)}{g(x)^2} \\ \left(\frac{f}{g}\right)'(x) &= \frac{f'(x)g(x) - f(x)g'(x)}{g(x)^2} \end{aligned}$$

Exercice
Faire les démonstration.
Il suffit d'exploiter la commutativité entre dérivation et partie réelle ou imaginaire.

Correction

4.4. Composition avec l'exponentielle complexe

Théorème - Dérivée de l'exponentielle complexe
Soit $\phi : I \to \mathbb{C}$ dérivable sur I. Alors

$$\begin{aligned} \psi : \quad I &\to \mathbb{C} \\ x &\mapsto e^{\phi(x)} \end{aligned}$$

est dérivable sur I et : $\forall x \in I, \quad \psi'(x) = \phi'(x) e^{\phi(x)}$

Démonstration
On note $\phi = \phi_1 + i\phi_2$.
On a alors

$$\forall\, x \in I, \quad \psi(x) = e^{\phi_1(x)} \times e^{i\phi_2(x)} = e^{\phi_1(x)} \times (\cos(\phi_2(x)) + i\sin(\phi_2(x)))$$

dérivable par produit :

$$\begin{aligned} \forall\, x \in I, \quad \psi'(x) &= \phi_1'(x) e^{\phi_1(x)} e^{i\phi_2(x)} + e^{\phi_1(x)} \phi_2'(x)(-\sin(\phi_2(x)) + i\cos(\phi_2(x))) \\ &= \phi_1'(x) e^{\phi_1(x)} e^{i\phi_2(x)} + e^{\phi_1(x)} \phi_2'(x) i(i\sin(\phi_2(x)) + \cos(\phi_2(x))) \\ &= (\phi_1'(x) + i\phi_2'(x)) e^{\phi(x)} = \phi'(x) e^{\phi(x)} \end{aligned}$$

□

Attention - i joue un rôle comparable à celle d'un nombre réel
On fera bien attention à ne pas oublier le i dans la dérivation!

Exercice
Calculer la dérivée $f : x \mapsto (\arcsin(x)) e^{2x + ix^2}$.

Correction
f est dérivable sur $\mathbb{C}$, comme produit et composition de fonctions dérivables sur $]-1, 1[$.

$$\forall\, x \in]-1, 1[, \quad f'(x) = \left(\frac{1}{\sqrt{1-x^2}} + (2 + 2ix)\arcsin(x)\right) e^{2x+ix^2}$$

Application - Fonction polaire
On considère $g : \mathbb{R} \to \mathbb{C}, \theta \mapsto \rho(\theta) e^{i\theta}$. On dit que l'on définie une fonction polaire.
On suppose que $\rho : \mathbb{R} \to \mathbb{R}_+$ est dérivable sur I.
• Montrons que g est dérivable et calculons g'.
Par produit de fonctions dérivables sur I, g est dérivable sur I.
Et pour tout $x \in I$, $g'(\theta) = \rho'(\theta) e^{i\theta} + i\rho(\theta) e^{i\theta}$.
• Il arrive que pour ce genre de fonction, on ait besoin de calculer $|g'(\theta)|$.
On utilise la quantité conjuguée :

$$\begin{aligned} \forall\, \theta \in I, \quad |g'(\theta)|^2 &= g'(\theta)\overline{g'(\theta)} = (\rho'(\theta)e^{i\theta} + i\rho(\theta)e^{i\theta})\overline{(\rho'(\theta)e^{i\theta} + i\rho(\theta)e^{i\theta})} \\ &= (\rho'(\theta)e^{i\theta} + i\rho(\theta)e^{i\theta})(\rho'(\theta)e^{-i\theta} - i\rho(\theta)e^{-i\theta}) \\ &= [\rho'(\theta)]^2 + [\rho(\theta)]^2 \end{aligned}$$

Donc pour tout $\theta \in I$, $|g'(\theta)| = \sqrt{[\rho'(\theta)]^2 + [\rho(\theta)]^2}$

5. Bilan

Synthèse

⇝ Au voisinage d'un point, on peut regarder comment la fonction évolue : c'est la valeur de la dérivée en ce point qui nous l'indique. On

associe alors (si possible) f une nouvelle fonction : celle qui donne la valeur de dérivée en tout point. MIRACLE. Le passage $f \to f'$ se décrit très bien en terme d'algorithme (sans avoir à passer par le nombre dérivée). Il faut donc apprendre des tas de règles de calculs (à démontrer, par ailleurs...).

⇝ Ainsi plusieurs fonctions de référence sont à connaître : exponentielle(s) et logarithme(s) en toute base ; les fonctions puissances ; les fonctions circulaires (sin, arc cos...) et hyperboliques directes. On doit savoir comment comparer ces fonctions lorsqu'elles sont en compétition au voisinage de point problématique.

⇝ Le théorème de la bijection est un résultat important. Il faut le connaître, même si pour l'heure la démonstration nous échappe sans une définition précise de la continuité (et donc de $\mathbb{R}$).

⇝ En retour, la fonction dérivée permet de mieux comprendre localement la fonction. On peut alors étudier des variations, faire de l'optimisation (locale) ou lever des indéterminations (pour du calcul de limite).

⇝ Les fonctions complexes de la variables réelles s'étudient de la même façon (même si la représentation est plus complexe). En fait, ce qui compte, c'est la nature de la variable « de départ ».

Savoir-faire et Truc & Astuce du chapitre

— Truc & Astuce pour le calcul - A propos de la tangente
— Savoir-faire - Encadrement pour le calcul de limite
— Savoir-faire - Transférer un problème exponentiel de « en a » vers « en 0 ».
— Savoir-faire - Transférer un problème logarithme « en a » vers « en 1 ».
— Savoir-faire - Transférer un problème trigonométrique « en a » vers « en 0 ».
— Savoir-faire - Etudier si f est un $\mathscr{C}^1$-difféomorphisme
— Savoir-faire - Obtenir une inégalité
— Savoir-faire - Obtenir un maximum (dérivation)
— Savoir-faire - Lever une indétermination par la règle de L'Hospital
— Savoir-faire - Etude des branches infinies (et définition)

Retour sur les problèmes

19. On a une fonction $A(a_0+e)$ qui donne l'aire en fonction de a_0+e. Elle est optimale en a_0 lorsque $A(a_0-\epsilon) < A(a_0)$ et $A(a_0+\epsilon) < A(a_0)$ avec $\epsilon > 0$.
Le calcul $A(a_0+e)$ donne exactement $A(a_0)+eA'(a_0)+\dots$. On trouve, avec la méthode de Fermat : $A'(a_0)=0$, ce qui donne bien l'optimal de A.
20. Il faut nécessairement que Résultat$'$(Action) = 0, ce qui conduit à une équation donc la valeur recherchée Action_0 est solution. Malheureusement, la condition bien que nécessaire n'est pas suffisante.
21. C'est un vrai miracle que cela soit aussi simple (et que le tableau ne soit pas plus compliqué...).
A moins que cela soit l'inverse : c'est parce que $y'=y$ se rencontre partout que l'exponentielle est si importante...
22. Cours
23. C'est le but de la formule de L'Hospital.
24. On vient de terminer ce chapitre en répondant à cette question.

Chapitre 6

Fonctions primitives et équations différentielles

Résumé -

Dans ce chapitre, le point de vue adopté est celui de Newton et Leibniz puis Euler, qui font de l'intégration l'opération inverse de la dérivation, c'est-à-dire que si f est une fonction définie sur I intervalle de $\mathbb{R}$ contenant a et b, admettant une primitive F, on définit l'intégrale de a à b de f par $\int_a^b f(t)\,dt = F(b)-F(a) = \left[F(t)\right]_a^b$.
Par propriétés de la dérivation (linéarité et primitivation d'inégalités), on obtient la linéarité et la croissance de l'intégrale ainsi définie. On s'exercera aussi techniquement pour maitriser ce calcul intégral, le fameux calculus.
Hypothèse forte : on admet toujours qu'une fonction continue sur un intervalle I admet des primitives sur I. La démonstration aura lieu plus tard.
Dans la très grande famille des équations différentielles, nous nous concentrons uniquement sur les équations différentielles linéaires d'ordre 1 et les équations différentielles d'ordre 2 à coefficients constants. Cela réduit largement les équations différentielles rencontrées, mais la raison est bonne : ce sont celles que l'on rencontre le plus souvent (à cause de la linéarisation des problèmes physiques) et ce sont celles que l'on sait résoudre (la fonction exponentielle a été crée pour cela).
Quelques liens youtube :

- *Hedacademy - Les primitives. https ://www.youtube.com/watch ?v=05ikcAFcPZ0*
- *Exo7 - Equation différentielle - https ://www.youtube.com/watch ?v=dkjXofPNMDo*
- *5min Lebesgue - forme idéale - https ://www.youtube.com/watch ?v=9x91d0UnBTw*

Sommaire

1. Problèmes 108
2. Primitives 109
2.1. Définitions 109
2.2. Primitives usuelles 110
2.3. Quelques cas particuliers 111
3. Intégrales 113
3.1. Théorème fondamental et conséquences 113
3.2. Quelques propriétés de l'intégrale 115
3.3. Technique 1 : Intégration par parties 116
3.4. Technique 2 : Changement de variables 118
4. Equation différentielle (dérivation/primitivation tordue) 123
4.1. Vocabulaire 123
4.2. Equation différentielle linéaire d'ordre 1 124
4.3. Equation différentielle linéaire d'ordre 2 à coefficients constants 129
5. Bilan 135

1. Problèmes

Problème 25 - Lien primitve/intégrale

Calculer l'aire d'une surface est un « vieux » problème. Par exemple : quelle est l'aire d'une ellipse, d'une lunule ?
Optimiser, trouver un maximum ou un minimum est un autre « vieux » problème des mathématicien.
Existe-t-il un lien (profond, donc) entre les deux ?

Problème 26 - Problèmes historiques

Galilée affirme en 1638 que la forme d'une chaîne suspendue entre deux clous est presqu'une parabole. Huygens, démontre 20 ans plus tard que ceci est faux. La solution, appelée caténaire (ou chainette) est donnée une vingtaine d'année plus tard par Leibniz et Johann Bernoulli.
Lors du séjour de Leibniz à Paris (1672-1673) durant lequel il suit des cours d'Huygens, Claude Perrault lui pose le problème suivant : *quelle est la courbe qui a la propriété qu'en chacun de ses points P, le segment de la tangente entre P et l'axe x et de longueur constante a ?* Pour concrétiser cette question, Perrault tire de son gousset une "hotlogio portabili suae thecae argenteae" et la fait glisser sur la table. Il précise qu'aucun mathématicien parisien ni toulousain (Fermat) n'a été capable d'en trouver l'équation.

Problème 27 - Primitivisation des opérations algébriques

Pour le calcul de dérivation, le cours est grossièrement constitué d'un tableau de dérivation usuelle et de trois savoir-faire : comment dériver une addition, comment dériver une multiplication, comment dériver une composition ?
Avec ça, on arrive à tout (ou presque)…
Qu'en est-il de la primitivisation (opération inverse de la dérivation) ? Un tableau semble tout à fait possible, la règle de l'addition semble également bien s'inverser. Mais pour la multiplication ? Et la composition ?
Quelle est la primitive de $f \times g$? Quelle est la primitive de $f \circ g$?

Problème 28 - Fraction rationnelle

Il est facile d'intégrer (ici, trouver la primitive) de toutes fonctions polynomiales.
Est-il possible d'intégrer toute division de polynôme, c'est-à-dire toute fraction rationnelle ?
Dans le cas d'une forme factorisée, cela donne :
Quelle est une primitive de $x \mapsto \dfrac{P(x)}{(x-a)(x-b)^n(x^2+cx+d)^m}$ avec $c^2-4d<0$?

Problème 29 - Implication

Si une fonction est dérivable, alors elle est continue. La réciproque est bien entendu fausse.
Existe-t-il un lien entre « admettre une primitive » et « être continue » ?
Comment gère-t-on une fonction non continue ?
Par exemple, existe-t-il une primitive à tan ? Existe-t-il une primitive

continue à tan ?

? Problème 30 - Problème de M. Lagoute

Que dire de $y'' + y = 0$? Tout dire !
C'est le fameux oscillateur harmonique, vu et revu en cours de sciences physiques.

? Problème 31 - Existence. Unicité

Est-ce qu'une équation différentielle admet toujours une, une seule, solution ?
Ce n'est pas le cas de $y'' + y = 0$ qui admet au moins comme solution $x \mapsto \cos x$ et $x \mapsto \sin x$. En admette-t-elle d'autres ? Peut-on lister toutes les solutions ?
Et alors, quel type de contraintes ajoutées pour obtenir une équation différentielle avec une et une seule solution ?
Et par ailleurs, existe-t-il des équations différentielles sans solution ?

? Problème 32 - Linéarisation

Dans ce cas, nous étudions que des équations différentielles linéaires.
Comment faire lorsque l'équation différentille n'est pas linéaire ? Peut-on revenir au cas précédent ? Par ailleurs, existe-t-il des moyens complémentaires (informatiques, par exemple) pour étudier des équations différentielles variées ?

2. Primitives

I désigne un intervalle de $\mathbb{R}$.
On commence par se concentrer sur les primitives, bien qu'il ne s'agit que d'un cas particulier d'une équation différentielle. Mais c'est la méthode essentielle pour résoudre les équations différentielles linéaires d'ordre 1.

2.1. Définitions

Définition - Primitives
Soit f une fonction définie sur un intervalle I de $\mathbb{R}$ à valeurs dans $\mathbb{R}$ (resp. à valeurs dans $\mathbb{C}$). On appelle primitive de f sur I toute fonction F **dérivable** sur I à valeurs dans $\mathbb{R}$ (resp. à valeurs dans $\mathbb{C}$) telle que, sur I, $F' = f$.

Proposition - CNS de primitive sur $\mathbb{C}$
$F : I \to \mathbb{C}$ est une primitive de $f : I \to \mathbb{C}$
si et seulement si $\mathrm{Re}F$ et $\mathrm{Im}F$ sont des primitives de $\mathrm{Re}f$ et $\mathrm{Im}f$ (resp.).

Proposition - Définition à constante additive près
Deux primitives de f sur l'intervalle I diffèrent d'une constante.
C'est-à-dire que si F est une primitive de f sur I alors l'ensemble des primitives de f sur I est

$$\left\{x \mapsto F(x) + C ; C \in \mathbb{K}\right\}$$

Pour aller plus loin - Classe d'équivalence
On a déjà vu, comme il n'y a pas unicité de la primitive, primitiver devrait plutôt signifier : donner un ensemble, une classe d'équivalence pour la relation d'équivalence : $f \equiv g$ ssi $f - g \in \mathbb{R}$ (est une constante).

où $\mathbb{K} = \mathbb{R}$ (resp. $\mathbb{K} = \mathbb{C}$) si f est à valeurs dans $\mathbb{R}$ (resp. dans $\mathbb{C}$).

Démonstration
Soit F, une primitive de f. On a les équivalences :

$$\begin{aligned} \varphi \text{ est primitive de } f &\iff \varphi' = f = F' \iff (\varphi - F)' = 0 \\ &\iff \exists\, C \in \mathbb{K} \text{ tel que } \varphi - F = C \end{aligned}$$

(ce dernier résultat bien connu, sera démontré un peu plus tard. □

2.2. Primitives usuelles

En reprenant simplement le tableau de dérivations des fonctions usuelles, on trouve :

Pour aller plus loin - Tableau fini ?
Pour être utile, une table de primitives doit comporter plusieurs centaines de pages. Mentionnons ici celles de Gröbner et Hofreiter (1949) et de Gradshteyn et Ryzhik (1980). Aujourd'hui de nombreux logiciels de calcul symbolique contiennent de telles tables

Proposition - Tableau des primitives usuelles des fonctions à valeurs réelles (1)

fonction	primitives (C est une constante réelle)
x^α où $\alpha \in \mathbb{R} \setminus \{-1\}$	$\frac{x^{\alpha+1}}{\alpha+1} + C$
$\frac{1}{x}$	$\ln\lvert x\rvert + C$
e^x	$e^x + C$
$e^{\beta x}$ où $\beta \in \mathbb{C} \setminus \{0\}$	$\frac{e^{\beta x}}{\beta} + C$
$\mathrm{sh}\,\beta x$ où $\beta \neq 0$	$\frac{\mathrm{ch}\,\beta x}{\beta} + C$
$\mathrm{ch}\,\beta x$ où $\beta \neq 0$	$\frac{\mathrm{sh}\,\beta x}{\beta} + C$
$\sin x$	$-\cos x + C$
$\cos x$	$\sin x + C$
$\sin \beta x$ où $\beta \neq 0$	$-\frac{\cos \beta x}{\beta} + C$
$\cos \beta x$ où $\beta \neq 0$	$\frac{\sin \beta x}{\beta} + C$
$1 + \tan^2 x$	$\tan x + C$
$\ln x$	$x \ln x - x + C$
$\frac{1}{1+x^2}$	$\arctan x + C$
$\frac{1}{\sqrt{1-x^2}}$	$\arcsin x + C$ ou $-\arccos x + C'$

Proposition - Tableau des primitives usuelles des fonctions à valeurs réelles (2)

fonction f de la forme :	primitive F
$u'(x)u(x)^\alpha$ où $\alpha \in \mathbb{R} \setminus \{-1\}$	$\frac{u(x)^{\alpha+1}}{\alpha+1} + C$
$\frac{u'(x)}{u(x)}$	$\ln\lvert u(x)\rvert + C$
$u'(x)e^{u(x)}$	$e^{u(x)} + C$

Ces formules sont valables sur tout **intervalle** I où f (ou u) est continue.

Attention - Primitive sur deux intervalles
Si f admet des primitives sur la réunion de deux intervalles disjoints, on peut avoir des constantes différentes sur chacun des deux intervalles.
On rencontrera particulièrement cette situation dans le chapitre sur les

, équations différentielles.

2.3. Quelques cas particuliers

Exponentielles et trigonométrie

Savoir faire - $e^{\alpha x}\cos\beta x$ **ou** $e^{\alpha x}\sin\beta x$

Pour $f(x)=e^{\alpha x}\cos\beta x$ ou $f(x)=e^{\alpha x}\sin\beta x$ $(\alpha,\beta\in\mathbb{R})$, il suffit de primitiver $e^{(\alpha+i\beta)x}$ et récupérer partie réelle ou imaginaire.

Savoir faire - $\sin^n x\cos^m x$

Pour $f(x)=\sin^n x\cos^m x$, on peut linéariser.
Rappelons que pour cela on utilise les formules de de Moivre : $\sin^n x = \left(\frac{e^{ix}-e^{-ix}}{2i}\right)^n\dots$

Exercice
Déterminer des primitives des fonctions suivantes :

$$f_1(x)=e^{3x}\sin(2x);\quad f_2(x)=\sin^3(x)\cos^4(x)$$

Correction
$f_1=\text{Im}(e^{3x+2ix})=\text{Im}(e^{(3+2i)x})$.

$$F_1(x)=\text{Im}\left(\frac{1}{3+2i}e^{(3+2i)x}\right)=\text{Im}\left(\frac{3-2i}{13}e^{(3+2i)x}\right)=\frac{e^{3x}}{13}\big(3\sin(2x)-2\cos(2x)\big)$$

$$f_2(x)=\left(\frac{e^{ix}-e^{-ix}}{2i}\right)^3\times\left(\frac{e^{ix}+e^{-ix}}{2}\right)^4=\frac{i}{128}\left(e^{3ix}-3e^{ix}+3e^{-ix}-e^{-3ix}\right)\left(e^{4ix}+4e^{2ix}+6+4e^{-2ix}+e^{-4ix}\right)$$

$$=\frac{i}{128}\left((e^{7ix}-e^{-7ix})+(e^{5ix}-e^{-5ix})-3(e^{3ix}-e^{-3ix})-3(e^{ix}-e^{-ix})\right)$$

$$=\frac{-1}{64}\left(\sin(7x)+\sin(5x)-3\sin(3x)-3\sin(x)\right)$$

Donc

$$F_2(x)=\frac{1}{448}\cos(7x)+\frac{1}{320}\cos(5x)-\frac{1}{64}\cos(3x)-\frac{3}{64}\cos(x)$$

Idée pour « vérifier » le calcul : faire un DL en 0 :

$f_2(x)\sim x^3$ *et* $\frac{-1}{64}\left(\sin(7x)+\sin(5x)-3\sin(3x)-3\sin(x)\right)=\frac{-1}{64}\left[(7+5-9-3)x-\frac{1}{6}(343+125-81-3)x^3+o(x^3)\right]=x^3+o(x^3)$

Remarque - Si on a un doute…
On peut toujours vérifier en calculant la dérivée de la primitive obtenue.
Ici la dérivée de $x\mapsto\frac{e^{3x}}{13}\big(3\sin(2x)-2\cos(2x)\big)$ est

$$x\mapsto\frac{e^{3x}}{13}\big((9\sin(2x)-6\cos(2x))+(6\cos(2x)+4\sin(2x))\big)=e^{3x}\sin(2x)$$

Fractions rationnelles

Des résultats et un savoir-faire à connaître :

Proposition - Tableau de primitives de certaines fonctions rationnelles (fonctions à valeurs dans $\mathbb{R}$)

fonction	primitives (C est une constante réelle)
$\frac{1}{x-a}$	$\ln\lvert x-a\rvert+C$
$\frac{1}{(x-a)^n}$ où $n\in\mathbb{N}^*\setminus\{1\}$	$\frac{-1}{n-1}\frac{1}{(x-a)^{n-1}}+C$
$\frac{1}{x^2+a^2}$	$\frac{1}{a}\arctan\frac{x}{a}+C$
$\frac{2x+p}{x^2+px+q}$	$\ln\lvert x^2+px+q\rvert+C$
$\frac{2x+p}{(x^2+px+q)^n}$ où $n\in\mathbb{N}^*\setminus\{1\}$	$\frac{-1}{n-1}\frac{1}{(x^2+px+q)^{n-1}}+C$

Exercice
A démontrer

Correction
Il suffit de dériver les cas de droites

Remarque - Division euclidienne
Lorsque le polynôme au numérateur a un degré plus important que celui du dénominateur, on commence par effectuer une division euclidienne pour se trouver en présence des cas précédent.
Nous reverrons les divisions euclidiennes en fin de premier semestre

Pour aller plus loin - Avec l'arithmétique complexe (à manipuler avec précaution…)
On rappelle que $\arg(1+ix)=\arctan(x)$, *donc si* $z=e^{i\theta}=1+ix$, *on a donc*

$$\ln(1+ix)=\ln(z)=i\theta=i\arg(1+ix)=i\arctan(x)$$

Donc

$$\int\frac{1}{x^2+1}=\frac{i}{2}\int\frac{1}{x+i}-\frac{1}{x-i}$$

$$=\frac{i}{2}\left(\ln(x+i)-\ln(x-i)\right)$$

$$=\frac{i}{2}\left(\ln(1+\frac{i}{x})-\ln(1-\frac{i}{x})\right)$$

$$=\frac{1}{2}(-\arctan\frac{1}{x}+\arctan\frac{-1}{x})=-\frac{\pi}{2}+\arctan x$$

En fait le logarithme complexe est définie à une constante $2i\pi$ *près…*

Savoir faire - Fractions rationnelles $\frac{1}{ax^2+bx+c}$

Pour les fractions rationnelles de la forme $f(x)=\frac{1}{ax^2+bx+c}$ $((a,b,c)\in\mathbb{R}^3, a\neq0)$:

— si $\Delta>0$, le trinôme a deux racines réelles distinctes α et β. On cherche alors $\lambda,\mu\in\mathbb{R}$ tels que

$$f(x)=\frac{\lambda}{x-\alpha}+\frac{\mu}{x-\beta}$$

et on primitive avec $\ln|.|$

$$F(x)=\lambda\ln|x-\alpha|+\mu\ln|x-\beta|=\ln|(x-\alpha)^\lambda(x-\beta)^\mu|$$

— si $\Delta=0$, on a alors

$$f(x)=\frac{1}{a(x-\alpha)^2}$$

on primitive directement avec la fraction rationnelle

$$F(x)=\frac{-1}{a(x-\alpha)}$$

— si $\Delta<0$, on met le dénominateur sous forme canonique

$$f(x)=\frac{1}{(x+\alpha)^2+\beta^2}$$

on reconnaît une fonction composée qui se primitive avec arctan

$$F(x)=\frac{1}{\beta}\arctan\left(\frac{x+\alpha}{\beta}\right)$$

Exercice
Déterminer des primitives des fonctions suivantes :

$$f_1(x)=\frac{1}{(x^2-x-2)};\quad f_2(x)=\frac{1}{x^2+x+1};\quad f_3(x)=\frac{2x-1}{x^2+x+1};\quad f_4(x)=\frac{2x+1}{x^2+4x+4}.$$

Correction

$x^2-x-2=(x+1)(x-2)$, donc il existe $\lambda,\mu\in\mathbb{R}$ tel que $\forall\, x\in\mathbb{R}$: $\dfrac{1}{x^2-x-2}=\dfrac{\lambda}{x+1}+\dfrac{\mu}{x-2}=\dfrac{(\lambda+\mu)x+(-2\lambda+\mu)}{x^2-x-2}$.

On peut (et on doit...) prendre $\lambda=-\mu=\frac{-1}{3}$, on a donc $\dfrac{1}{x^2-x-2}=\dfrac{1}{3}\left(\dfrac{1}{x+2}-\dfrac{1}{x-1}\right)$ Donc une primitive de f_1 est $F_1:x\mapsto\dfrac{1}{3}\ln\left|\dfrac{x+2}{x-1}\right|+C$.

Le discriminant de x^2+x+1 est $\Delta=1-4=-3<0$, on a $x^2+x+1=(x+\frac{1}{2})^2+\frac{3}{4}$.

Une primitive de f_2 est donc $F_2:x\mapsto\dfrac{2}{\sqrt{3}}\arctan\dfrac{2x+1}{\sqrt{3}}+C$

$f_3(x)=\dfrac{2x+1}{x^2+x+1}-2\dfrac{1}{x^2+x+1}$, on reconnait $\frac{u'}{u}-2f_2$.

Donc une primitive de f_3 est $F_3:x\mapsto\ln(x^2+x+1)-2\dfrac{2}{\sqrt{3}}\arctan\dfrac{2x+1}{\sqrt{3}}+C$

Pourquoi n'est-il pas besoin de valeur absolue ici ? Enfin, $f_4(x)=\dfrac{2x+1}{(x+2)^2}=2\dfrac{x+2-\frac{3}{2}}{(x+2)^2}=\dfrac{2}{x+2}-3\dfrac{1}{(x+2)^2}$.

Donc une primitive de f_4 est $F_4:x\mapsto\ln|x+2|+3\dfrac{1}{x+2}+C$.

3. Intégrales

3.1. Théorème fondamental et conséquences

Extension de l'intégrale sur $\mathbb{C}$

Définition - Notation
Soit $f:I\to\mathbb{R}$, pour tout $a<b\in I$, on note

$$\int_a^b f(t)\mathrm{d}t$$

l'aire (algébrique) comprise entre les segments de droites $x=a$, $y=0$ et $x=b$, et la courbe $y=f(x)$.
Nous admettons son existence si f est continue sur $[a,b]$.

Définition - Intégrale de f sur $[a,b]$
Si $f:[a,b]\to\mathbb{C}$ est continue sur $[a,b]$, on appelle intégrale de f sur $[a,b]$ le nombre complexe

$$\int_a^b f(t)\,dt=\int_a^b \mathrm{Re}f(t)\,dt+i\int_a^b \mathrm{Im}f(t)\,\mathrm{d}t.$$

Attention - Définition?
Est-ce vraiment une définition? Non, car on ne sait pas bien ce qu'est ce calcul. Préciser qu'il s'agit du nombre obtenu à partir d'une primitive de f, c'est tourner en rond par rapport au théorème et au corollaire qui suivent.
A ce stade, on est obligé de prendre ce nombre comme construit à partir de f, a et b. Au second semestre, nous prendrons le temps de bien montrer l'existence et donner un algorithme de calcul de ce nombre. Nous verrons qu'il n'est pas nécessaire que f soit continue (f pourrait être moins régulière)

Exercice

Soit P une application polynomiale. On suppose que pour tout $m\in\mathbb{N}$, $\int_0^{2\pi}e^{-imt}P(e^{it})\mathrm{d}t=0$.
Montrer que P est nul

Correction

Pour fixer les notations, on suppose que $P(x)=\sum_{k=0}^{d}a_kx^k$.

Alors $\int_0^{2\pi}e^{-imt}P(e^{it})\mathrm{d}t=\sum_{k=0}^{d}\int_0^{2\pi}a_ke^{i(k-m)t}\mathrm{d}t=2\pi a_m+\sum_{k\neq m}\left[\dfrac{a_k}{i(k-m)\pi}e^{i(k-m)t}\right]_0^{2\pi}=2\pi a_m$.
Donc pour tout $m\in\mathbb{N}$, $a_m=0$.

Fonction : intégrale de sa borne supérieure

Théorème - Théorème fondamental du calcul différentiel
Soit f continue sur I, intervalle de $\mathbb{R}$, à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$. Soit $a\in I$.
Alors la fonction

$$\begin{array}{rccc}F:&I&\to&K\\&x&\mapsto&\displaystyle\int_a^x f(t)\mathrm{d}t\end{array}$$

est de classe C^1 (c'est-à-dire dérivable de dérivée continue) sur I et $F'=f$.
C'est de plus l'unique primitive de f nulle en $a\in I$.

Corollaire - Existence de primitive
Toute fonction continue sur I admet une primitive sur I.

Attention - Pas toutes les primitives avec cette notation
On n'obtient pas toutes les primitives ainsi.
Ainsi, pour $f(x)=\cos x$, la primitive $F(x)=\sin x+2$ ne peut s'obtenir ainsi. En effet, on aurait alors $F(x)=\sin x-\sin a$, or il n'existe pas de $a\in\mathbb{R}$ tel que $\sin a=-2$.

Remarque - Démonstration?
Ce théorème est admis, pour le démontrer il faudrait une meilleure définition de $\int_a^b f(t)\mathrm{d}t$

Fusion : primitive et intégrale (de sa borne supérieure)

Théorème - Calcul fondamental
Soit f continue sur I intervalle de $\mathbb{R}$ contenant a et b. Soit F une primitive de f. Alors

$$\int_a^b f(t)\,\mathrm{d}t=F(b)-F(a)=\Big[F(t)\Big]_a^b.$$

Définition - Notation par extension
On notera, par extension des notations précédentes :
- $\int_\cdot^x f(t)\mathrm{d}t$, une primitive quelconque de f.
  On pourra même considérer avec cette notation l'ensemble de toutes les primitives de f
- $\left[F(t)\right]_\cdot^x=F(x)$

Corollaire - Avec f'
Soit f de classe C^1 sur I. Alors

$$\forall (a,x)\in I^2,\ f(x)-f(a)=\int_a^x f'(t)\,\mathrm{d}t.$$

3.2. Quelques propriétés de l'intégrale

Proposition - Linéarité, croissance, Chasles...
Pour des fonctions f et g continues sur un intervalle I à valeurs dans $\mathbb{R}$, on a, pour $a,b\in I$, les propriétés suivantes :

— **linéarité** : si λ et μ sont deux réels,

$$\int_a^b (\lambda f+\mu g)(t)\,\mathrm{d}t=\lambda\int_a^b f(t)\,dt+\mu\int_a^b g(t)\,\mathrm{d}t$$

— **relation de Chasles** : pour $c\in]a,b[$,

$$\int_a^b f(t)\,\mathrm{d}t=\int_a^c f(t)\,dt+\int_c^b f(t)\,\mathrm{d}t$$

— **positivité** : si $a\leqslant b$ **et** $\forall x\in[a,b]$, $f(x)\geqslant 0$ alors

$$\int_a^b f(t)\,\mathrm{d}t\geqslant 0$$

— **croissance** : si $a\leqslant b$ **et** $\forall x\in[a,b]$, $f(x)\geqslant g(x)$ alors

$$\int_a^b f(t)\,dt\geqslant\int_a^b g(t)\,\mathrm{d}t$$

Truc & Astuce pour le calcul - Encadrer une intégrale
Pour encadrer une intégrale, on encadre la fonction à intégrer

Savoir faire - Inégalité des accroissements finis (avec f de classe $\mathscr{C}^1$)
Si f est de classe $\mathscr{C}^1$ sur $[a,b]\subset I$.
Notons $M=\sup_{[a,b]}f'$ et $m=\inf_{[a,b]}f'$, on a donc, pour tout $t\in[a,b]$:

$$f'(t)-m\geqslant 0\qquad\text{et}\qquad M-f'(t)\geqslant 0$$

On intègre sur $[a,b]$:

$$f(b)-f(a)-m(b-a)=\int_a^b f'(t)\mathrm{d}t-m\int_a^b m\mathrm{d}t\geqslant 0\Longrightarrow f(b)-f(a)\geqslant m(b-a)$$

$$f(b)-f(a)-M(b-a)=\int_a^b f'(t)\mathrm{d}t-M\int_a^b m\mathrm{d}t\leqslant 0\Longrightarrow f(b)-f(a)\leqslant M(b-a)$$

Pour aller plus loin - Inégalité des accroissements finis
Ce savoir-faire de l'inégalité des accroissements finis sera améliore plus loin : il suffira que f soir dérivable (et non nécessairement de classe $\mathscr{C}^1$.

Remarque - Combinaison linéaire
Si f et g sont deux fonctions, λ et μ deux réels $\lambda f+\mu g$ s'appelle une combinaison linéaire à coefficients réels de f et g.

Proposition - Fonctions à valeurs complexes
Soient f,g deux fonctions continues sur $[a,b]$ à valeurs dans $\mathbb{C}$ et λ,μ deux complexes. Alors on a les propriétés suivantes :

— **linéarité** :

$$\int_a^b(\lambda f+\mu g)(t)\,dt=\lambda\int_a^b f(t)\,\mathrm{d}t+\mu\int_a^b g(t)\,\mathrm{d}t$$

— **relation de Chasles** : pour $c\in]a,b[$,

$$\int_a^b f(t)\,\mathrm{d}t=\int_a^c f(t)\,\mathrm{d}t+\int_c^b f(t)\,\mathrm{d}t$$

Attention - Sur $\mathbb{C}$, pas de relation d'ordre...
Donc la croissance de l'intégrale sur $\mathbb{C}$ n'a pas de sens. Mais on peut exploiter les modules, si l'on souhaite faire des encadrements de la partie réelle et la partie imaginaire...

Exemple - Cela reste vraie, même si $c\notin]a,b[$
Si, par exemple, on a $c<b<a$ et F une primitive de f sur $[c,a]$:

$$\int_c^a f(t)\mathrm{d}t=\int_c^b f(t)\mathrm{d}t+\int_b^a f(t)\mathrm{d}t$$

Donc $\int_a^b f(t)\mathrm{d}t=F(b)-F(a)=-\int_b^a f(t)\mathrm{d}t=\int_c^b f(t)\mathrm{d}t-\int_c^a f(t)\mathrm{d}t=\int_a^c f(t)\mathrm{d}t+\int_c^b f(t)\mathrm{d}t$.

3.3. Technique 1 : Intégration par parties

Enoncé

Théorème - Intégration par parties
Si u et v sont deux fonctions de classe C^1 sur un intervalle I de $\mathbb{R}$, à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$, alors

$$\forall (a,b)\in I^2,\qquad\int_a^b u'(t)v(t)\,\mathrm{d}t=\Big[u(t)v(t)\Big]_a^b-\int_a^b u(t)v'(t)\,\mathrm{d}t$$

Démonstration
$u(a)v(a)-u(b)v(b)=[uv]_a^b=\int_a^b(uv)'=\int_a^b uv'+\int_a^b u'v$.
Donc $\int_a^b u'v=[uv]_a^b-\int_a^b uv'$ □

Obtenir une primitive

Savoir faire - Obtenir une primitive avec une IPP cachée
Pour calculer une primitive par IPP de $f=u'v$, notée

$$\int_{\cdot}^x f(t)\,\mathrm{d}t$$

(attention, il s'agit d'**une fonction** et non d'un scalaire), on peut écrire

$$\int_{\cdot}^x u'(t)v(t)\,\mathrm{d}t=u(x)v(x)-\int_{\cdot}^x u(t)v'(t)\,\mathrm{d}t+C$$

Exercice

Avec une intégration par parties trouver une primitive de $x \mapsto \frac{x^2}{(x^2+1)^2}$ puis de $x \mapsto \frac{1}{(x^2+1)^2}$.

On verra une autre méthode plus loin.

Correction

Les applications $u : x \mapsto \frac{1}{x^2+1}$ et $v : x \mapsto \frac{1}{2}x$ sont de classe $\mathscr{C}^1$ sur $\mathbb{R}$.

$$\int \frac{x^2}{(x^2+1)^2}\,\mathrm{d}x = \int \frac{1}{2}x \times \frac{2x}{(x^2-1)^2}\,\mathrm{d}x = \int v(t)u'(t)\mathrm{d}t = u(x)v(x) - \int u(x)v'(x)\mathrm{d}x + C$$

$$= \frac{x}{2(x^2+1)} + \int \frac{1}{2(x^2+1)}\,\mathrm{d}x + C = \frac{1}{2}\left(\frac{x}{x^2+1} + \arctan(x)\right) + C$$

Puis

$$\frac{1}{(x^2+1)^2} = \frac{1+x^2}{(x^2+1)^2} - \frac{x^2}{(x^2+1)^2} = \frac{1}{(x^2+1)} - \frac{x^2}{(x^2+1)^2}$$

Par linéarité :

$$\int \frac{1}{(x^2+1)^2}\,\mathrm{d}x = \arctan x - \frac{1}{2}\left(\frac{x}{x^2+1} + \arctan(x)\right) + C' = \frac{1}{2}\left(\arctan(x) - \frac{x}{x^2+1}\right) + C'$$

Primitives de $P(x)e^{\alpha x}$

Savoir faire - $f(x) = P(x)e^{\alpha x}$

Pour $f : t \mapsto P(t)e^{\alpha t}$ où P est une fonction polynomiale, on peut faire $\deg(P)$ intégrations par parties (IPP) en dérivant $v : t \mapsto P(t)$ et en intégrant $u' : t \mapsto e^{\alpha t}$.
On peut appliquer la même méthode pour $f : t \mapsto P(t)\sin(\alpha t)$ ou $f : t \mapsto P(t)\cos(\alpha t)$.

Remarque - Autre méthode

On peut aussi directement chercher une primitive de la forme $Q(t)e^{\alpha t}$ avec $\deg Q = \deg P$.
On dérive cette fonction et identifie les coefficients de Q.

Exercice

Calculer

$$I = \int_0^{\pi/2} t\sin t\,\mathrm{d}t, \quad J = \int_0^1 e^{2x}(6x^2+2x-4)\,\mathrm{d}x$$

Correction

Les fonctions $u : t \mapsto -\cos t$ et $v : t \mapsto t$ sont de classe $\mathscr{C}^1$ sur $\mathbb{R}$,

$$I = [-t\cos t]_0^{\pi/2} + \int_0^{\pi/2} \cos t = 0 + [\sin(t)]_0^{\pi/2} = 1$$

Les fonctions $u : x \mapsto \frac{1}{2}e^{2x}$, $v : x \mapsto 6x^2+2x-4$ et $w : x \mapsto 12x+2$ sont de classe $\mathscr{C}^1$ sur $\mathbb{R}$,

$$J = \left[\frac{1}{2}e^{2x}(6x^2+2x-4)\right]_0^1 - \frac{1}{2}\int_0^1 e^{2x}(12x+2)\mathrm{d}x = 2e^2 + 2 - \frac{1}{4}\left[e^{2x}(12x+2)\right]_0^1 + \frac{1}{4}\int_0^1 12e^{2x}\mathrm{d}x$$

$$= 2e^2 + 2 - \frac{14}{4}e^2 + \frac{1}{2} + \frac{3}{2}e^2 - \frac{3}{2} = 1$$

Exercice

Pour aller plus loin : trouver une formule générale de $\int e^{\alpha x}P(x)$ qui exploite les puissances de α et les dérivées de P

Correction

$$\int_a^b e^{\alpha x}P(x) = \sum_{k=0}^{n} \frac{(-1)^k}{\alpha^{k+1}}\left(e^{\alpha a}P^{(k)}(a) - e^{\alpha b}P^{(k)}(b)\right)$$

Primitives de $P(x)\ln\big(Q(x)\big)$

Savoir faire - $f(x) = P(x)\ln\big(Q(x)\big)$

Pour $f : t \mapsto P(t)\ln\big(Q(t)\big)$ où P est une fonction polynomiale, on peut faire une intégrations par parties (IPP) en dérivant $v : t \mapsto \ln\big(Q(t)\big)$ et en intégrant $u' : t \mapsto P(t)$.
On se retrouve alors en présence d'une fraction rationnelle, que l'on sait

Pour aller plus loin - Fonction beta

On note $B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}\mathrm{d}t$.
On montre par IPP que
$B(x,y+1) = \frac{y}{x+y}B(x,y)$.
Puis si n *et* m *sont des entiers :*

$$B(n+1,m+1) = \frac{n!m!}{(n+m+1)!} = \frac{1}{(n+m+1)\binom{n+m}{n}}$$

Cela peut donner un sens à $\binom{x+y}{x}$, *avec* $x, y \in \mathbb{R}\ldots$

, intégrer, en principe…

Exercice

Calculer

$$I_b = \int_0^b x\ln(x^2+1)\,\mathrm{d}x.$$

On pourra remarquer que $x^3 = x(x^2+1) - x\ldots$

Correction

Les fonctions $u : x \mapsto \frac{1}{2}x^2$ et $v : x \mapsto \ln(x^2+1)$ sont de classe $\mathscr{C}^1$ sur $\mathbb{R}$,

$$I_b = \left[\frac{1}{2}x^2\ln(x^2+1)\right]_0^b - \int_0^b \frac{x^3}{x^2+1}\,\mathrm{d}x = \frac{1}{2}b^2\ln(b^2+1) + \int_0^b \frac{x}{x^2+1} - x\mathrm{d}x$$

$$= \frac{1}{2}b^2\ln(b^2+1) + \frac{1}{2}\ln(b^2+1) - \frac{1}{2}b^2$$

3.4. Technique 2 : Changement de variables

Enoncé

Théorème - Changement de variable
Soient I, J des intervalles de $\mathbb{R}$, $\alpha, \beta \in I$,
Soient $\phi : I \to \mathbb{R}$ de classe C^1 telle que $\phi(I) \subset J$ et $f : J \to \mathbb{R}$ (ou $\mathbb{C}$) continue.
Alors

$$\int_{\phi(\alpha)}^{\phi(\beta)} f(t)\,\mathrm{d}t = \int_\alpha^\beta f(\varphi(x))\varphi'(x)\,\mathrm{d}x.$$

Démonstration
Notons F, une primitive de f, on a alors :

$$\int_{\phi(\alpha)}^{\phi(\beta)} f(t)\,\mathrm{d}t = F(\phi(\alpha)) - F(\phi(\beta)) = [F\circ\phi]_\alpha^\beta = \int_\alpha^\beta f(\varphi(x))\varphi'(x)\,\mathrm{d}x.$$

car $(F\circ\phi)' = \phi' \times F'\circ\phi = \phi' \times f\circ\phi$. □

Analyse - Deux cas possibles

Deux cas se produise : une application directe de ce théorème, ou bien une application avec la fonction réciproque de ϕ.

1. Cas direct (non bijectif) :
   On doit calculer $\int_a^b f(u)\mathrm{d}u$.
   On pose $u = \varphi(t)$, où φ est de classe $\mathscr{C}^1$ sur $[\alpha,\beta]$, avec $\varphi(\alpha) = a$ et $\varphi(\beta) = b$ et donc $\mathrm{d}u = \varphi'(t)\mathrm{d}t$.
   Ainsi : $\int_a^b f(u)\,\mathrm{d}u = \int_\alpha^\beta f(\varphi(t))\varphi'(t)\,\mathrm{d}t$
2. Cas indirect (bijectif) :
   On doit calculer $\int_a^b f(u)\mathrm{d}u$.
   On pose $t = \psi(u)$, où ψ est de classe $\mathscr{C}^1$ sur $[a,b]$, et bijective de $[a,b]$ sur $[\alpha,\beta]$.
   avec $\varphi = \psi^{-1}$, on a donc $u = \varphi(t)$
   et donc $\mathrm{d}u = \varphi'(t)\mathrm{d}t = \frac{1}{\psi'(\varphi(t))}\mathrm{d}t \iff \psi'(u)\mathrm{d}u = \mathrm{d}t$.
   Ainsi : $\int_a^b f(u)\,\mathrm{d}u = \int_a^b f(\psi^{-1}(t))\frac{\mathrm{d}t}{\psi'(\psi^{-1}(t))}$

Mais, c'est la pratique qui compte, pas d'apprendre ces formulations !

Pour aller plus loin - Aire d'un cercle

Donner l'aire d'un cercle de rayon r.

Savoir faire - Changement de variable - dans la pratique

on veut calculer $\int_{\phi(\alpha)}^{\phi(\beta)} f(t)\,\mathrm{d}t$. On pose $t = \phi(x)$ (changement de variable), on remplace alors

— t par $\phi(x)$
— $\mathrm{d}t$ par $\phi'(x)\,\mathrm{d}x$ $\qquad (\phi'(x) = \frac{d\phi(x)}{dx} = \frac{dt}{dx})$

— t varie de $\phi(\alpha)$ à $\phi(\beta)$ par x varie de α à β (et inversement)
On peut faire un tableau

Exercice
Calculer par changement de variables les intégrales suivantes

$$I=\int_0^{\pi/2} x\sin(x^2)\,\mathrm{d}x,\quad J=\int_0^1\sqrt{1-t^2}\,\mathrm{d}t$$

Correction
On considère $\phi: t\mapsto\sqrt{t}$, de classe $\mathscr{C}^1$ sur $\left[0,\frac{\pi^2}{4}\right]$,
On pose alors $x=\phi(t)$, et donc, comme $\phi'(t)=\frac{1}{2\sqrt{t}}$

$$I=\int_0^{\pi^2/4}\sqrt{t}\sin t\times\frac{1}{2\sqrt{t}}\mathrm{d}t=\left[\frac{-1}{2}\cos t\right]_0^{\pi^2/4}=\frac{1}{2}(1-\cos\frac{\pi^2}{4})$$

On considère $\psi: t\mapsto\sin(t)$, de classe $\mathscr{C}^1$ sur $\left[0,\frac{\pi}{2}\right]$,
On pose alors $x=\psi(t)$, et donc, comme $\psi'(t)=\cos(t)$

$$I=\int_0^{\pi/2}\sqrt{1-\sin^2 t}\times\cos(t)\mathrm{d}t=\frac{1}{2}\int_0^{\pi/2}(1+\cos(2t))\,\mathrm{d}t=\frac{1}{2}\left[t+\frac{1}{2}\sin(2t)\right]_0^{\pi/2}=\frac{\pi}{4}$$

(C'est l'aire d'un quart de disque...)

Application : calcul de primitive

Soulignons l'importance que ϕ soit bijective pour exploiter ϕ^{-1}...

Savoir faire - Calculer une primitive par changement de variable
On cherche une primitive F de f sur I,
— on pose $t=\phi(x)$ et donc $\mathrm{d}t=\phi'(x)\mathrm{d}x$ où ϕ est une **bijection de classe** C^1 de J sur I,

— on cherche une primitive $G(x)=\int f(\phi(x))\phi'(x)\,\mathrm{d}x$ et on prend $F(t)=G(\phi^{-1}(t))$.

Exemple - Primitive de $t\mapsto\frac{1}{t^2+a^2}$
Par exemple en posant $x=\frac{t}{a}$, on a

$$\int\frac{dt}{t^2+a^2}=\int\frac{1}{a}\frac{dx}{x^2+1}=\frac{1}{a}\arctan x+C=\frac{1}{a}\arctan\frac{t}{a}+C$$

Attention - Ne pas oublier de revenir à la variable de départ
Pour éviter les erreurs (oubli de revenir à la variable de départ...) on aurait intérêt à écrire

$$F(x)=\int_{\cdot}^{x}\frac{dt}{t^2+a^2}$$

Exercice
Soit $a\in\mathbb{R}$. Donner une primitive de $x\mapsto\frac{1}{(x^2+a^2)^2}$ en faisant le changement de variable $\tan t=\frac{x}{a}$.
On rappelle que $1+\tan^2 u=\frac{1}{\cos^2 u}$

Correction
On pose $\tan\theta=\frac{t}{a}$, $\frac{1}{a}\mathrm{d}t=(1+\tan^2\theta)\mathrm{d}\theta$

$$\int^x\frac{\mathrm{d}t}{(t^2+a^2)^2}=\frac{1}{a^4}\int^x\frac{\mathrm{d}t}{(1+(\frac{t}{a})^2)^2}=\frac{1}{a^3}\int^{\arctan(x/a)}\cos^2\theta\mathrm{d}\theta=\frac{1}{2a^3}\int^{\arctan(x/a)}(\cos 2\theta+1)\mathrm{d}\theta$$

$$=\frac{1}{2a^3}\left[\frac{1}{2}\sin\left(2\arctan\frac{x}{a}\right)+\arctan\frac{x}{a}\right]+C=\frac{1}{2a^3}\left[\tan(\arctan\frac{x}{a})\cos^2(\arctan\frac{x}{a})+\arctan\frac{x}{a}\right]+C$$

$$=\frac{1}{2a^3}\frac{x}{a}\times\frac{1}{1+\frac{x^2}{a^2}}+\frac{1}{2a^3}\arctan\frac{x}{a}+C=\frac{ax+\arctan\frac{x}{a}}{2a^3(a^2+x^2)}+C$$

Exercice
Aller plus loin : Donner l'expression des primitives de $x\mapsto\frac{1}{(x^2+a^2)^n}$

Correction

Savoir faire - Bijection par morceaux
Lorsque le changement de variable doit être bijectif, mais ne l'est que par morceaux, alors
1. on cherche une primitive sur chaque morceaux d'intervalle
2. on « recolle » chaque morceaux en ajustant les constante de manière à ce que la primitive soit bien continue.

L'exercice suivant illustre ce savoir-faire.
Exercice
Donner l'ensemble de définition et calculer la primitive de $h: x\mapsto\frac{1}{2+\cos x}$
On posera $t=\tan\frac{x}{2}$

Correction
h est définie et continue sur $\{x\in\mathbb{R}\mid\cos x\neq-2\}=\mathbb{R}$, elle admet donc des primitives sur cet ensemble.
D'abord, pour tout $x\in\mathbb{R}$, $h(x)=\frac{1}{2+\frac{1-\tan^2\frac{x}{2}}{1+\tan^2\frac{x}{2}}}=\frac{1+\tan\frac{x}{2}}{3+\tan\frac{x}{2}}$,

$$H(x)=\int^x\frac{1+\tan^2\frac{t}{2}}{3+\tan^2\frac{t}{2}}\mathrm{d}t$$

On réalise le changement de variable $u=\tan\frac{t}{2}$, donc $\mathrm{d}u=\frac{1}{2}(1+\tan^2\frac{t}{2})\mathrm{d}t$.

$$H(x)=\int^{\tan\frac{x}{2}}\frac{2}{3+u^2}\mathrm{d}u=\frac{2}{3}\int^{\tan\frac{x}{2}}\frac{\mathrm{d}u}{1+[\frac{u}{\sqrt{3}}]^2}=\frac{2}{\sqrt{3}}\left[\arctan\frac{u}{\sqrt{3}}\right]^{\tan\frac{x}{2}}$$

$$\exists K\in\mathbb{R},\qquad H(x)=\frac{2}{\sqrt{3}}\arctan\left(\frac{\tan\frac{x}{2}}{\sqrt{3}}\right)+K$$

MAIS le changement de variable posée : $u=\tan\frac{t}{2}$ n'est pas bijective sur $\mathbb{R}$.
Il s'agit de bijection d'intervalle de la forme $]-\pi+2j\pi;\pi+2j\pi[$ sur $\mathbb{R}$.
Donc les solutions obtenues sont plutôt :

$$\exists\,(K_j)_{j\in\mathbb{Z}}\in\mathbb{R}^{\mathbb{Z}},\qquad\forall\,x\in](2j-1)\pi;(2j+1)\pi[,H(x)=\frac{2}{\sqrt{3}}\arctan\left(\frac{\tan\frac{x}{2}}{\sqrt{3}}\right)+K_j$$

Puis comme H est dérivable, elle est nécessairement continue donc continue en $\frac{\pi}{2}+j\pi$.

$$\lim_{x\to((2j+1)\pi)^+}H(x)=\lim_{x\to((2(j+1)\pi)^-}J(x)$$

Et comme, par composition des limites :

$$\lim_{x\to((2j+1)\pi)^+}H(x)=\lim_{x\to((2j+1)\pi)^+}\frac{2}{\sqrt{3}}\arctan\left(\frac{\tan\frac{x}{2}}{\sqrt{3}}\right)+K_{j+1}=\lim_{y\to-\infty}\frac{2}{\sqrt{3}}\arctan(y)+K_{j+1}=-\frac{\pi}{\sqrt{3}}+K_{j+1}$$

$$\lim_{x\to((2j+1)\pi)^-}\frac{2}{\sqrt{3}}\arctan\left(\frac{\tan\frac{x}{2}}{\sqrt{3}}\right)+K_j=\lim_{y\to+\infty}\frac{2}{\sqrt{3}}\arctan(y)+K_j=\frac{\pi}{\sqrt{3}}+K_j$$

On a donc, pour tout $j\in\mathbb{Z}$,

$$-\frac{\pi}{\sqrt{3}}K_{j+1}=\frac{\pi}{\sqrt{3}}+K_j$$

Donc $K_{j+1}=K_j+\frac{2\pi}{\sqrt{3}}$. On reconnait une suite arithmétique : $K_j=K_0+\frac{2\pi}{\sqrt{3}}j$.
Et finalement, comme

$$x\in](2j-1)\pi;(2j+1)\pi[\iff\frac{x}{\pi}+1\in]2j,2j+2[\iff\frac{x+\pi}{2\pi}\in]j,2j+1[\iff j=\left\lfloor\frac{x+\pi}{2\pi}\right\rfloor$$

on peut affirmer :

$$\exists\,K(=K_0)\in\mathbb{R}\text{ tel que :}\qquad\forall\,x\in\mathbb{R},\qquad H(x)=\frac{2}{\sqrt{3}}\arctan\left(\frac{\tan\frac{x}{2}}{\sqrt{3}}\right)+\frac{2\pi}{\sqrt{3}}\times\left\lfloor\frac{x+\pi}{2\pi}\right\rfloor+K$$

Fonctions définies à partir de fonctions trigonométrique

Savoir faire - Calcul pour $f(t)=\sin^n t\cos^m t$ avec n ou m impair

Pour $f(t)=\sin^n t\cos^m t$, on peut linéariser, ou,

- si n est impair, effectuer le changement de variables $u=\cos t$ (ou isoler un $\sin t$ et dans $\sin^{n-1} t$ remplacer $\sin^2 t$ par $1-\cos^2 t$ puis reconnaître des primitives),
- si m est impair, effectuer le changement de variables $u=\sin t$ (ou remplacer $\cos^2 t$ par $1-\sin^2 t$).

Exercice

Calculer par changement de variables l'intégrale suivante

$$\int_0^{\pi/2}\sin^2 u\cos^3 u\,\mathrm{d}u$$

Correction

On pose $t=\sin u$, de classe $\mathscr{C}^1$ sur $[0,\frac{\pi}{2}]$. On a donc $\mathrm{d}t=\cos u\mathrm{d}u$

$$\int_0^{\pi/2}\sin^2 u\cos^3 u\,\mathrm{d}u=\int_0^1 t^2(1-t^2)\mathrm{d}t=\left[\tfrac{1}{3}t^3-\tfrac{1}{5}t^5\right]_0^1=\frac{2}{15}$$

Savoir faire - Cas général ($\tan\frac{x}{2}$)

D'une manière générale, les changements de variables utiles pour les fonctions construites avec de fonctions trigonométriques sont $t=\cos x$, $t=\sin x$, $t=\tan x$, $t=\tan\frac{x}{2}$.

On rappelle que si $t=\tan\frac{x}{2}$, alors $\cos x=\dfrac{1-t^2}{1+t^2}$, $\sin x=\dfrac{2t}{1+t^2}$ et $\tan x=\dfrac{2t}{1-t^2}$.

Exercice

Calculer par changement de variables l'intégrale suivante

$$\int_{\pi/3}^{\pi/2}\frac{\mathrm{d}t}{\sin t}$$

Correction

On pose $t=\tan\frac{x}{2}$ de classe $\mathscr{C}^1$ sur $[\frac{\pi}{3},\frac{\pi}{2}]$.

On a $\mathrm{d}t=\frac{1}{2}(1+\tan^2\frac{x}{2})\mathrm{d}x$, donc $\mathrm{d}x=\dfrac{2\mathrm{d}t}{1+t^2}$.

$$\int_{\pi/3}^{\pi/2}\frac{\mathrm{d}t}{\sin t}=\int_{1/\sqrt{3}}^1\frac{t^2+1}{2t}\times\frac{2}{1+t^2}\mathrm{d}t=\int_{1/\sqrt{3}}^1\frac{\mathrm{d}t}{t}=\frac{1}{2}\ln 3$$

Simplification des calculs

Théorème - Simplification des calculs

Soit $f:[-a,a]\to\mathbb{R}(\mathbb{C})$ une fonction continue :

- si f est paire, $\displaystyle\int_{-a}^a f(t)\mathrm{d}t=2\int_0^a f(t)\mathrm{d}t$;
- si f est impaire, $\displaystyle\int_{-a}^a f(t)\mathrm{d}t=0$;
- si $f:\mathbb{R}\to\mathbb{R}$ (ou $\mathbb{C}$) est une fonction continue T-périodique, $\displaystyle\int_{a+T}^{b+T}f(t)\,dt=\int_a^b f(t)\mathrm{d}t$ et $\displaystyle\int_a^{a+T}f(t)\mathrm{d}t=\int_0^T f(t)\mathrm{d}t$.

Démonstration

Si f est paire,

$$\int_{-a}^a f(t)\mathrm{d}t=\int_{-a}^0 f(t)\mathrm{d}t+\int_0^a f(t)\mathrm{d}t=\underbrace{\int_a^0 f(-u)(-\mathrm{d}u)}_{u=-t}+\underbrace{\int_0^a f(u)(\mathrm{d}u)}_{u=t}=2\int_0^a f(u)\mathrm{d}u$$

Si f est impaire,

$$\int_{-a}^a f(t)\mathrm{d}t=\int_{-a}^0 f(t)\mathrm{d}t+\int_0^a f(t)\mathrm{d}t=\underbrace{\int_a^0 f(-u)(-\mathrm{d}u)}_{u=-t}+\underbrace{\int_0^a f(u)(\mathrm{d}u)}_{u=t}=\int_0^a f(u)(\mathrm{d}u)-\int_0^a f(u)(\mathrm{d}u)=0$$

Si f est T-périodique

$$\int_{a+T}^{b+T}f(t)\,dt=\underbrace{\int_a^b f(u+T)\mathrm{d}u}_{u=t-T}=\int_a^b f(u)\mathrm{d}u$$

Notons $n=\left\lfloor\dfrac{a}{T}\right\rfloor$, donc $nT\leqslant a<(n+1)T$:

$$\int_a^{a+T}f(t)\mathrm{d}t=\int_a^{(n+1)T}f(t)\mathrm{d}t+\int_{(n+1)T}^{a+T}f(t)\mathrm{d}t=\int_{a-nT}^{(n+1)T-nT}f(t)\mathrm{d}t+\int_{(n+1)T-(n+1)T}^{a+T-(n+1)T}f(t)\mathrm{d}t$$
$$=\int_{a-nT}^T f(t)\mathrm{d}t+\int_0^{a-nT}f(t)\mathrm{d}t=\int_0^{a-nT}f(t)\mathrm{d}t+\int_{a-nT}^T f(t)\mathrm{d}t=\int_0^T f(t)\mathrm{d}t$$

d'après la formule de Chasles □

Variable dans les bornes de l'intégrale (composition)

Savoir faire - Variable dans le bornes de l'intégrale

Il arrive qu'on doit étudier des fonctions de la forme

$$g:x\mapsto\int_{f_1(x)}^{f_2(x)}h(t)\mathrm{d}t$$

, sans pouvoir exprimer explicitement H, une primitive de h.
Néanmoins, la simple existence de H, permet d'écrire :

$$g(x)=H(f_2(x))-H(f_1(x))$$

Dont on déduit de nombreuses informations. Par exemple : g est dérivable si f_1 et f_2 le sont. Et dans ce cas :

$$\forall\,x\in\mathscr{D},\qquad g'(x)=f_2'(x)\times h(f_2(x))-f_1'(x)\times h(f_1(x))$$

Exercice

Soit $H:x\mapsto\displaystyle\int_x^{2x}\frac{\mathrm{d}t}{\sqrt{1+t^4}}$. Etudier la parité de H. Montrer que H est dérivable sur $\mathbb{R}$, calculer H' et dresser le tableau de variations de H. Déterminer les limites de H en $+\infty$ et $-\infty$.

Correction

$H(-x)=\displaystyle\int_{-x}^{-2x}\frac{\mathrm{d}t}{\sqrt{1+t^4}}=\int_x^{2x}\frac{-\mathrm{d}u}{\sqrt{1+u^4}}=-H(x)$ en faisant le changement de variable $u=-t$.
Donc H est impaire. On étudie sur $\mathbb{R}_+$, on appliquera la symétrie ensuite.
L'application $g:t\mapsto\dfrac{1}{\sqrt{1+t^4}}$ est continue sur $\mathbb{R}$, donc elle admet une primitive G sur $\mathbb{R}$.
On a alors $H(x)=G(2x)-G(x)$. Et par composition, H est dérivable sur $\mathbb{R}$ et

$$\forall\,x\in\mathbb{R},\qquad H'(x)=2G'(2x)-G'(x)=2g(2x)-g(x)=\frac{2}{\sqrt{1+16x^4}}-\frac{1}{\sqrt{1+x^4}}$$

Pour tout $x>0$,

$$H'(x)\leqslant 0\iff\frac{4}{1+16x^4}\leqslant\frac{1}{1+x^4}\iff 3-12x^4\leqslant 0\iff 1-4x^4\leqslant 0$$

$$H'(x)\leqslant 0\iff(1-2x^2)(1+2x^2)\leqslant 0\iff(1-\sqrt{2}x)(1+\sqrt{2}x)\leqslant 0\iff x\in\left[0,\frac{1}{\sqrt{2}}\right]$$

donc H est croissante sur $\left[0, \frac{1}{\sqrt{2}}\right]$, puis décroissante sur $\left[\frac{1}{\sqrt{2}}, +\infty\right[$.

Par ailleurs $H(0) = 0$ et par décroissance de $t \mapsto \frac{1}{\sqrt{1+t^4}}$ sur $[x, 2x]$,

$$0 \leqslant H(x) \leqslant \int_x^{2x} \frac{1}{\sqrt{1+x^4}}\,\mathrm{d}t = \frac{2x-x}{\sqrt{1+x^4}} \leqslant \frac{x}{\sqrt{x^4}} = \frac{1}{x}$$

Et par encadrement : $\lim\limits_{x\to+\infty} H(x) = 0$.

4. Equation différentielle (dérivation/primitivation tordue)

4.1. Vocabulaire

D'une manière générale on appelle équation différentielle une équation faisant intervenir les dérivées successives d'une même fonction, elle est du premier ordre si elle porte sur la fonction et sa dérivée première, du second ordre si elle porte sur la fonction et ses dérivées première et seconde...
La résolution d'un problème de Cauchy est la résolution d'une équation différentielle avec des conditions initiales.
Plus précisément :

Définition - Equation différentielle linéaire du premier ordre
Une équation différentielle (E) est dite *linéaire et du premier ordre* si elle s'écrit $\alpha(t)y' + \beta(t)y = \gamma(t)$ où α, β, γ sont trois fonctions définies sur un intervalle I de $\mathbb{R}$ (à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$).
Elle est dite *normalisée* si elle s'écrit $y' + a(t)y = b(t)$ où a, b sont deux fonctions définies sur un intervalle I de $\mathbb{R}$ (à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$).
$b(t)$ (ou $\gamma(t)$) est le *second membre*, l'équation est dite *sans second membre ou homogène* si la fonction b est nulle.

Remarque - Mise sous forme normale
Si α ne s'annule pas sur I l'équation différentielle $\alpha(t)y' + \beta(t)y = \gamma(t)$ se ramène à une équation normalisée.

Définition - Problème de Cauchy du premier ordre
On appelle problème de Cauchy du premier ordre la donnée d'une équation différentielle du premier ordre et d'une condition initiale $y(t_0) = y_0$ où $t_0 \in \mathbb{R}$ et $y_0 \in \mathbb{C}$ (ou $\mathbb{R}$).

Définition - Solutions
Soit f une fonction de I dans $\mathbb{C}$.
f est solution de (E) $\quad \alpha(t)y' + \beta(t)y = \gamma(t)$ si

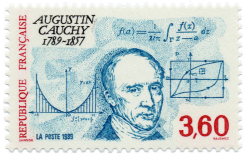
(1) $\quad f$ est dérivable sur I,
(2) $\quad \forall t \in I, \quad \alpha(t)f'(t) + \beta(t)f(t) = \gamma(t)$.

0n pourra noter S_E l'ensemble des solutions de (E).
Résoudre l'équation différentielle (E) c'est donc déterminer l'ensemble S_E, c'est-à-dire trouver toutes les solutions sur I.
On appelle *courbe intégrale* de (E) la courbe représentative d'une solution de (E).

Remarque - Convention réelle
En l'absence d'indications contraires, si les fonctions α, β, γ sont à valeurs dans $\mathbb{R}$, on notera S_E l'ensemble des fonctions de I dans $\mathbb{R}$ qui sont solutions de (E).

Histoire - Révolution newtonienne
La double découverte, par Newton, des lois de physique qui s'expriment sous forme d'équations différentielles et des méthodes mathématiques pour les résoudre a permis la révolution scientifique en Europe. Pendant deux siècles, les techniques se sont affinées et la maîtrise de tous les phénomènes de sciences physiques s'est élargies. Au milieu du XIX-ième siècle, les scientifiques croyaient au déterminisme totalement compris (l'avenir totalement écrit sous nos yeux)...

Histoire - Louis-Augustin Cauchy



Louis-Augustin Cauchy (1789-1857) est un mathématicien français aux intérêts très large en mathématiques. Son attitude face aux événements politiques contemporains l'a beaucoup isolé, sans totalement le marginaliser; probablement grâce à son génie. On le retrouvera à de nombreuses reprises tout au long de l'année.

Définition - Solution d'un problème de Cauchy
Résoudre le problème de Cauchy défini par (E) et $y(t_0) = y_0$, c'est déterminer toutes les solutions f de (E) vérifiant $f(t_0) = y_0$.

Remarque - Une/la solution?
On parle souvent de solution particulière de (E), il s'agit en fait d'UNE fonction qui est solution, par opposition à solution générale qui est la forme générale des solutions. Par exemple, $t \mapsto e^{3t}$, $t \mapsto 4e^{3t}$ sont des solutions particulières de $y' = 3y$ alors que $t \mapsto \lambda e^{3t}$ est la solution générale.

Savoir faire - Découper I pour avoir des équations normalisées
Si α s'annule sur I, on cherchera à découper I en plusieurs intervalles ouverts sur lesquels elle ne s'annule pas pour se ramener à des équations normalisées.
Ensuite on cherchera les solutions sur I par « recollement », c'est-à-dire que l'on regardera, parmi les fonctions définies par morceaux sur chacun des intervalles, celles qui sont dérivables sur I (problème aux points de recollement, c'est-à-dire ceux où α s'annulait) et vérifient (E) sur I.

Le principe suivant est d'usage fréquent en physique : il permet de s'intéresser à des seconds membres simples.

Proposition - Principe de superposition des solutions
Si le second membre de l'équation (E) est de la forme $b(t) = b_1(t) + \cdots + b_n(t)$
et si l'on connaît des solutions particulières $\widetilde{y}_1, \ldots, \widetilde{y}_n$ des équations avec les seconds membres $b_1(t), \ldots, b_n(t)$,
alors une solution particulière de (E) est $\widetilde{y} = \widetilde{y}_1 + \cdots + \widetilde{y}_n$.

Démonstration
On exploite la linéarité de l'équation différentielle linéaire.
On a

$$\widetilde{y}' + a\widetilde{y} = (\widetilde{y}_1 + \cdots + \widetilde{y}_n)' + a(\widetilde{y}_1 + \cdots + \widetilde{y}_n)$$
$$= (\widetilde{y}_1' + a\widetilde{y}_1) + \cdots + (\widetilde{y}_n' + a\widetilde{y}_n) = b_1 + \cdots + b_n = b$$

□

4.2. Equation différentielle linéaire d'ordre 1

Principe

On considère désormais l'équation différentielle linéaire normalisée

$$(E) \qquad y' + a(t)y = b(t)$$

où a et b sont continues sur I, intervalle de $\mathbb{R}$.
Dans la suite $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

Heuristique - Démonstration et savoir-faire. Que retenir?
Pour les démonstrations, nous allons décomposer l'application $F_a : \mathscr{D}(\mathbb{R}) \to \mathscr{D}(\mathbb{R})$, $y \mapsto y' + ay$ en applications, plus ou moins inversible. Nous verrons alors que l'équation différentielle est une dérivation « tordue ».
A la fin du cours, nous donnerons une méthode qu'on appliquera directement lors des exercices.
Sauf pour les exercices théoriques (du type inégalités différentielles).

Analyse

Analyse - Décomposition de F_a
Notons $D : y \mapsto y'$ et pour une application h quelconque $\varphi_h : y \mapsto \exp(h) \times y$.
Alors :

1. $\varphi_{-h} \circ \varphi_h : y \mapsto \exp(-h) \times (\exp(h) \times y) = \exp(-h+h) \times y = y = \mathrm{id}(y)$.
   Ainsi $\varphi_{-h} \circ \varphi_h = \mathrm{id} = \varphi_h \circ \varphi_{-h}$. Donc φ_h est inversible et $\varphi_h^{-1} = \varphi_{-h}$.
2. $\varphi_{-h} \circ D \circ \varphi_h : y \mapsto \exp(-h)[\exp(h)y]' = \exp(-h)[h'y + y']\exp(h) = y' + h'y = F_{h'}(y)$.
   Ainsi : $\varphi_{-h} \circ D \circ \varphi_h = F_{h'}$.

Ainsi, si $a \leftarrow h'$ donc $A \leftarrow h$ UNE primitive de a :

$$F_a(y) = b \iff \varphi_{-A} \circ D \circ \varphi_A(y) = b \iff D \circ \varphi_A(y) = \varphi_A(b)$$

Le problème : D n'est pas bijective… Il faudra gérer des constantes…
On continuera cette résolution plus loin.

Remarque - Non commutativité de D et φ_A
Malheureusement, on n'a pas $F_a = \varphi_{-A} \circ D \circ \varphi_A = D \circ \varphi_{-A} \circ \varphi_A = D$.
C'est là où on voit que l'équation différentielle est une dérivation tordue…

Exercice

Résoudre (E) $\quad (1+t^2)y' + 4ty = 0$ sur $I = \mathbb{R}$.

Correction

Sous forme normalisée (et homogène) : $y' + \frac{4t}{1+t^2}y = 0$, l'équation est définie sur $\mathbb{R}$ $(1+t^2 \neq 0)$.

On note alors $a(t) = \frac{4t}{1+t^2}$, de primitive $A(t) = 2\ln(1+t^2)$.

On a donc $D \circ \varphi_A(y) = \exp(A(t)) \times 0 = 0$, donc il existe $C \in \mathbb{R}$ tel que $y = \varphi_{-A}(C) = C\exp(-A)$.

Les solutions de (E) sont donc $t \mapsto Ce^{-2\ln(1+t^2)} = \frac{C}{(1+t^2)^2}$.

Remarque - Comment retenir l'ensemble des solutions ?
On dispose d'une méthode intuitive (mais qui n'est pas une démonstration car elle suppose que l'on sait que les solutions y ne s'annulent en aucun point) pour retrouver le résultat dans le cas des fonctions à valeurs réelles (c'est-à-dire lorsque $\mathbb{K} = \mathbb{R}$) en écrivant $\frac{y'(t)}{y(t)} = -a(t)$ et en primitivant.

$$\begin{aligned} \frac{y'(t)}{y(t)} = -a(t) \quad &\implies \ln(y(t)) = -A(t) + K \\ &\implies y(t) = \exp(-A(t)+K) = Ce^{-A(t)} \text{ avec } C = e^K \end{aligned}$$

On écrirait plutôt, heuristiquement :

$$(ye^{\int a})' = [y' + ay]e^{\int a} = 0 \implies ye^{\int a} = K \implies y = Ke^{-\int a}$$

Attention - Variable x, variable t ?
Nous avons noté y la fonction de la variable t, mais l'on peut bien évidemment avoir d'autres notations, par exemple y fonction de la variable x (équations différentielles donnant l'ordonnée en fonction de l'abscisse) ou x en fonction de t (équations différentielles donnant l'abscisse en fonction du temps) ou encore z en fonction de t (équations différentielles donnant l'affixe en fonction du temps).

Pour aller plus loin - Simplification de problème
On rencontre toujours en mathématique le diagramme suivant où un problème M (une matrice par exemple) est transformé en un problème D (matrice diagonale par exemple) plus simple à résoudre.

$$\begin{array}{ccc} x & \xrightarrow{M} & y \\ P\downarrow & & \downarrow P \\ \cdot & \xrightarrow{D} & \cdot \end{array}$$

Il y a deux chemins : celui par M, et celui par P, D, puis P (à l'envers). La composition s'écrit de droite à gauche. Cela donne

$$M = P^{-1} \times D \times P$$

Structures des solutions et méthodes

Théorème - Structure de l'ensemble S_E
La solution générale de l'équation (E) est la somme d'une solution particulière et de la solution générale de l'équation homogène associée (H), ce qui peut aussi s'écrire :

Si $\widetilde{y}$ (à lire « y tilde ») est une solution particulière de l'équation (E) alors

$$S_E = \left\{ t \mapsto Ce^{-A(t)} + \widetilde{y}(t);\ C \in \mathbb{K} \right\}.$$

Remarque - Existence
Insistons : L'existence d'(au moins) une solution est donnée par la forme de l'équation (E) :

- normalisée,
- avec a continue (admettant une primitive - plus exactement)
- avec b continue ($t \mapsto b(t)e^{A(t)}$ admettant une primitive - plus exactement)

Pour aller plus loin - Equation à variables séparables
La méthode présentée dans le remarque (comment retenir l'ensemble des solutions ?)est celle proposée dans le cas des équations à variables séparables : $y' \times f(y) = g(t)$. Avec un changement de variables, il s'agit d'un simple calcul d'intégrale (présenté ainsi, cela fonctionne mieux)…
En 1840, le mathématicien belge Pierre Verhulst propose un modèle de dynamique de population qui conduit à l'équation

$$y' = ay\left(1 - \frac{y}{K}\right)$$

où a et K sont des constantes associées à la population considérée.
La résolution donne :

$$y(t) = K\frac{1}{1 + \left(\frac{K}{y_0} - 1\right)e^{-at}}$$

On trouve en particulier : $y(0) = y_0$ et $y \xrightarrow[t\to+\infty]{} K$. Ce qui est contraire au modèle de Maltus

Démonstration
Soit $\tilde{y}$ une solution particulière. On a donc $\varphi_{-A} \circ D \circ \varphi_A(\tilde{y}) = b$.
Donc l'équation devient :

$$D \circ \varphi_A(y) = D \circ \varphi_A(\tilde{y}) \iff \exists\, C \in \mathbb{R} \text{ tel que } \varphi_A(y) = C + \varphi_A(\tilde{y})$$

En exploitant l'inverse de φ_A, on trouve S_E (et il y a équivalence donc égalité d'ensembles). □

Trouver une solution particulière $\tilde{y}$

Analyse - Résoudre l'équation
Continuons notre résolution. Nous en étions à $\varphi_{-A} \circ D \circ \varphi_A = b$.
Donc en remplaçant par leur valeur : $D \circ \varphi_A(y) = be^A$, qu'il faut intégrer à une constante près.
Notons $e^{A(t)}y(t) = \int_{\cdot}^{t} b(u)e^{A(u)}\mathrm{d}u + K$, donc

$$y(t) = \underbrace{Ke^{-A(t)}}_{\text{solution homogène}} + \underbrace{e^{-A(t)}\int_{\cdot}^{t} b(u)e^{A(u)}\mathrm{d}u}_{\text{solution particulière}}$$

.
Si $b = 0$, on a bien une solution homogène avec le premier terme de cette somme-solution.
L'enjeu est donc maintenant de trouver une solution particulière, peut-être plus simplement…
On doit à Lagrange la méthode de la variation de la constante qui répond explicitement à cette question (parmi d'autres méthodes).

Savoir faire - Comment trouver une équation particulière ? Méthode de « variation de la constante »
D'après le théorème précédent, ce qui reste est de trouver une solution particulière.
Sans indication donnée par l'énoncé, la méthode classique à suivre est la suivante :

1. On normalise l'équation différentielle. Cela peut nécessiter une étude sur plusieurs intervalles.
2. On résout l'équation différentielle homogène : $y = Ce^{-A(t)}$
3. On cherche une solution particulière :
   - en cherchant une solution évidente,
   - en utilisant le principe de superposition des solutions,
   - en essayant des fonctions simples (polynomiales lorsque a et b le sont, trigonométriques lorsque a et b le sont…),
   - en faisant varier la constante C, c'est-à-dire sous la forme

     $$\widetilde{y} : t \mapsto C(t)e^{-A(t)}$$

     (La constante C devient variable : « méthode de la variation de la constante »).
     Le calcul (à refaire à chaque fois - il permet de vérifier la bonne

résolution de l'équation homogène) conduit à :

$$C'(t) = b(t)e^{A(t)}$$

C'est un « simple » calcul de primitive

4. Les solutions générales sont alors de la forme

$$y : t \mapsto (K + C(t))e^{-A(t)}$$

avec C définie au point précédent

Problème de Cauchy

Théorème - Problème de Cauchy
Soit $t_0 \in I$ et $y_0 \in \mathbb{K}$.
Il existe une unique solution sur I de l'équation linéaire normalisée (E) $y' + a(t)y = b(t)$ vérifiant la condition initiale $y(t_0) = y_0$.

Démonstration
Les solutions de (E) sont de la forme $y = \bar{y} + Ce^{-A(t)}$ avec C constante « à déterminer ».
On a alors $y(t_0) = y_0 = \bar{y}(t_0) + Ce^{-A(t_0)}$, donc $C = (y_0 - \bar{y}(t_0))e^{A(t_0)}$.
Ce calcul donne une et une seule solution car $e^{-A(t_0)} > 0$ □

Remarque - Résoudre un problème de Cauchy
Pour résoudre un problème de Cauchy, on résout (E) puis on cherche la solution vérifiant $y(t_0) = y_0$.

Applications. Cas classiques

Exercice
Résoudre (E) $y' + ty = t$.

Correction

1. L'équation est sous forme normalisée.
2. L'équation homogène est $y' + ty = 0$ de solution $t \mapsto Ce^{-\frac{1}{2}t^2}$.
3. Une solution particulière de E est $y = 1$

L'ensemble des solutions est donc $\left\{t \mapsto 1 + Ce^{-\frac{1}{2}t^2}, C \in \mathbb{R}\right\}$.

Exercice
Résoudre (E) $z' = (1+i)z - 2it^2 + 2$.

Correction

1. L'équation est sous forme normalisée. A noter qu'ici $z : \mathbb{R} \mapsto \mathbb{C}$
2. L'équation homogène est $z' - (1+i)z = 0$ de solution $t \mapsto Ce^{(1+i)t} = Ce^t e^{it}$.
3. Le second membre est une fonction polynômiale de degré 2 : $t \mapsto -2it^2 + 2$.
   On cherche une solution particulière de la même forme : $\bar{z}(t) = At^2 + Bt + C$

   $$\bar{z}'(t) - (1+i)\bar{z}(t) = -A(1+i)t^2 + (2A - B(1+i))t + (B - C(1+i)) = -2it^2 + 2$$

   En identifiant : $A = \frac{2i}{1+i} = 1 + i$, puis $B = 2$ et $C = 0$, une solution particulière : $\bar{z} : t \mapsto (1+i)t^2 + 2t$
   (On peut/doit vérifier)

L'ensemble des solutions est donc $\left\{t \mapsto 2t + (1+i)t^2 + Ce^{(1+i)t}, C \in \mathbb{C}\right\}$.

Pour aller plus loin - Courbe intégrale
Cela signifie également qu'il existe une unique courbe intégrale passant par le point (t_0, y_0).

Attention - Ensemble des solutions particulières selon le second membre
Attention, si le second membre est colinéaire à la solution homogène, il faut alors chercher une solution particulière de « degré » plus élevé...

Exercice
Résoudre (E) $y' + y = 2e^x + 4\sin x + 3\cos x$.

Correction

1. L'équation est sous forme normalisée.
2. L'équation homogène est $y' + y = 0$ de solution $t \mapsto Ce^{-x}$.
3. On applique la méthode de la variation de la constante pour trouver une solution particulière $\bar{y}(x) = C(x)e^{-x}$.

   $$\bar{y}'(x) + \bar{y}(x) = C'(x)e^{-x} = 2e^x + 4\sin x + 3\cos x$$

   Donc $C'(x) = 2e^{2x} + 4\sin x e^x + 3\cos x e^x$, fonction à primitiver. On commence par primitiver $(\cos x + i\sin x)e^x = e^{(1+i)x}$ en $\frac{1}{1+i}e^{(1+i)x} = \frac{e^x}{2}(1-i)(\cos x + i\sin x)$.
   En prenant les parties réelles et imaginaires :

   $$\int \cos x e^x \mathrm{d}x = \frac{e^x}{2}(\cos x + \sin x) \qquad \int \sin x e^x \mathrm{d}x = \frac{e^x}{2}(-\cos x + \sin x)$$

   On a donc $C(x) = e^{2x} + 2e^x(-\cos x + \sin x) + \frac{3}{2}e^x(\cos x + \sin x) = e^{2x} + e^x(\frac{7}{2}\sin x - \frac{1}{2}\cos x)$.

L'ensemble des solutions est donc $\left\{x \mapsto e^x + \frac{1}{2}(7\sin x - \cos x) + Ce^{-x}, C \in \mathbb{R}\right\}$.

Savoir faire - Etudier une inéquation différentielle
Supposons qu'on ait l'inéquation $y' + ay \leqslant b$.
On reprend les notations précédentes, avec $\varphi_h : y \mapsto (t \mapsto e^{h(t)} \times y(t))$.
On a $\varphi_{-A} \circ D \circ \varphi_A \circ y \leqslant b$ ou encore $\forall\, u \in I : (D \circ \varphi_A)(y)(u) \leqslant e^{A(u)}b(u)$ car $e^z > 0$.
Puis par croissance de l'intégration : $\varphi_A(y)(t) - \varphi_A(y)(t_0) \leqslant \int_{t_0}^{t} b(u)e^{A(u)}\mathrm{d}u$.
Et donc $y(t) \leqslant e^{A(t_0)-A(t)}y(t_0) + e^{A(t)}\int_{t_0}^{t} b(u)e^{A(u)}\mathrm{d}u$.
(La constante t_0 est arbitraire, il faut nécessairement en fixer une!).
On reconnait une solution de l'équation différentielle.

Pour aller plus loin - Inéquations
Souvent les inéquations se transforment en de nouvelles inégalités, où les cas frontières sont exactement obtenus avec les solutions de l'équation identique (⩽ transformé en =).

Cas d'une équation non résolue. Problème du recollement

Savoir faire - Cas non résolue
A résoudre une équation $a(t)y' + b(t)y = c(t)$ sur I avec a qui s'annule sur I.

1. On étudie l'équation sur des sous-intervalles de I où a ne s'annule pas.
   Par exemple si $a(t) = t$ et $I = \mathbb{R}$; on étudie sur $\mathbb{R}_+^*$ et sur $\mathbb{R}_-^*$.
2. On obtient une famille de solutions, paramétrée sur chacun des sous-intervalles par une variable α (par exemple).
3. On essaye de **« recoller »** les solutions. Pour cela, on regarde les limites de y et de y' au voisinage du point t_0 qui annule a de manière à étudier la continuité et la dérivabilité de y en t_0.
   Souvent ces limites dépendent de la valeur paramètre α.

Dans la suite du cours : le théorème de prolongement de classe $\mathscr{C}^1$ et les méthodes de calcul asymptotiques seront très utiles pour résoudre ce problème

Exercice

Résoudre l'équation $t^2y' + y = 1$ sur un intervalle I de $\mathbb{R}$ (on discutera suivant la position de 0 par rapport à I).

Correction

1. L'équation n'est pas sous forme normalisée. Il faut diviser par t^2, cela n'est possible que sur $\mathbb{R}_+^*$ et sur $\mathbb{R}_-^*$.
   L'équation normalisée est alors $y' + \frac{1}{t^2}y = \frac{1}{t^2}$.
   On considère donc, pour la suite, I un intervalle de $\mathbb{R}_+^*$ ou de $\mathbb{R}_-^*$.
2. L'équation homogène normalisée est $y' + \frac{1}{t^2}y = 0$ de solution $t \mapsto Ce^{\frac{1}{t}}$.
3. Une solution particulière de E est $y = 1$
4. L'ensemble des solutions est donc sur $\mathbb{R}_+^*$: $\left\{t \mapsto 1 + Ce^{\frac{1}{t}}, C \in \mathbb{R}\right\}$ et $\mathbb{R}_-^*$: $\left\{t \mapsto 1 + C'e^{\frac{1}{t}}, C' \in \mathbb{R}\right\}$

On a trouvé une solution sur tout intervalle de $\mathbb{R}_+^*$, sur tout intervalle de $\mathbb{R}_-^*$.
Est-il possible d'avoir une solution sur un intervalle de $\mathbb{R}$ (contenant 0) ? Pour cela on pratique un recollement :

Soit y une telle solution, alors il existe $C, C' \in \mathbb{R}$ tel que : $\forall\, t > 0$, $y(t) = 1 + Ce^{\frac{1}{t}}$ et $\forall\, t < 0$, $y(t) = 1 + C'e^{\frac{1}{t}}$.

Cette fonction y est nécessairement de classe $\mathscr{C}^1$ sur $I \subset \mathbb{R}$.

Elle est donc continue en 0. Or $\lim\limits_{t\to 0^+} y(t) = \begin{cases} 1 & \text{si } C = 0 \\ +\infty & \text{si } C > 0 \\ -\infty & \text{si } C < 0 \end{cases}$.

Il est donc nécessaire que $C = 0$ et dans ce cas $y(t) = 1$, pour tout $t \geqslant 0$.

De même $\lim\limits_{t\to 0^-} y(t) = 1$ (pour tout C'). Donc y est bien continue en 0

Il faut aussi que y soit dérivable sur I, donc dérivable en 0. Or $y'(t) = 0$, pour tout $t > 0$,

alors que pour tout $t < 0$, $y'(t) = \frac{-1}{t^2}Ce^{\frac{1}{t}} \underset{t\to 0^-}{\longrightarrow} 0$ (comment lever l'indétermination ?).

Bilan : l'ensemble des solutions y (fonctions de classe $\mathscr{C}^1$) solutions de (E) sur I contenant 0 est

$$\left\{t \mapsto \begin{cases} 1 & \text{si } t \geqslant 0 \\ 1 + Ce^{\frac{1}{t}} & \text{si } t < 0 \end{cases}, C \in \mathbb{R}\right\}$$

Notez bien la méthode de recollement !

Remarque - Règle de L'Hospital

Il n'est pas rare que pour faire le recollement, nous ayons besoin de la règle de L'Hospital pour lever l'indétermination que l'on obtient en calculant, pour s frontière de I $\lim_{t\to s} y'(t) = \lim_{t\to s} \dfrac{c(t) - b(t)y(t)}{a(t)}$.

A utiliser, sans modération !

4.3. Equation différentielle linéaire d'ordre 2 à coefficients constants

Enoncé

$\mathbb{K}$ désigne toujours $\mathbb{R}$ ou $\mathbb{C}$. Insistons : ici a, b, c **sont constants**, $a \neq 0$ (sinon on revient au cas précédent).
L'année prochaine, vous élargirez ce point de vue.

Définition - Equations différentielles linéaires du second ordre à coefficients constants

Soient $(a, b, c) \in \mathbb{K}^3$, $a \neq 0$ et $u : I \to \mathbb{K}$ une fonction continue sur l'intervalle I de $\mathbb{R}$.
On dit qu'une fonction $f : I \to \mathbb{K}$ est solution de l'équation différentielle du second ordre à coefficients constants

$$(E) \quad ay'' + by' + cy = u(t)$$

si

(1) f est deux fois dérivable sur I
(2) $\forall\, t \in I,\ af''(t) + bf'(t) + cf(t) = u(t)$

L'équation $ar^2 + br + c = 0$ est appelée *équation caractéristique associée.*

Résolution de l'équation homogène associée

On considère donc l'équation homogène (H) $\quad ay'' + by' + cy = 0 \quad a \neq 0$.

Analyse - Composition de $F_\alpha \circ F_\beta$

Conservons les mêmes notations et comme a, b et c sont constants, prenons des primitives affines.
On a donc $(F_{-\alpha} \circ F_{-\beta})(y) = (y' - \beta y)' - \alpha(y' - \beta) = y'' - (\alpha + \beta)y' + \alpha\beta y$.
Et donc, en reprenant les formules de Viète : α et β sont les racines $x^2 - (\alpha + \beta)x + \alpha\beta$.
Considérons donc les racines α et β du polynôme $ax^2 + bx + c = a(x - \alpha)(x - \beta)$.
Alors, $aF_{-\alpha} \circ F_{-\beta}(y) = ay'' + by' + cy$.
Cette analyse ne marche pas lorsque les racines sont les mêmes : $\alpha = \beta$.
On étudie les cas particuliers selon la nature des solutions (double ou simples, complexes ou réelles) de l'équation caractéristique associée à l'équation homogène.

Théorème - Cas complexe

— Si $ar^2 + br + c = 0$ possède deux racines distinctes r_1 et r_2 alors l'ensemble des solutions à valeurs dans $\mathbb{C}$ est :

$$S_H = \left\{t \mapsto \lambda e^{r_1 t} + \mu e^{r_2 t}; (\lambda, \mu) \in \mathbb{C}^2\right\}$$

— Si $ar^2 + br + c = 0$ possède une racine double $r_0 \in \mathbb{C}$ alors l'ensemble des solutions à valeurs dans $\mathbb{C}$ est :

$$S_H = \left\{t \mapsto (\lambda + \mu t)e^{r_0 t}; (\lambda, \mu) \in \mathbb{C}^2\right\}$$

Démonstration

Notons r_1 et r_2 les racines de $ax^2 + bx + c = a(x - r_1)(x - r_2)$. (On peut avoir $r_1 = r_2$).
Alors y solution de $ay'' + by' + cy = 0 \iff F_{-r_1 \cdot t} \circ F_{-r_2 \cdot t}(y) = 0$.
Si l'on compose (comme précédemment), on a :

$$\begin{aligned} ay'' + by' + cy = 0 &\iff \varphi_{r_1 \cdot t} \circ D \circ \varphi_{-r_1 \cdot t} \circ \varphi_{r_2 \cdot t} \circ D \circ \varphi_{-r_2 \cdot t}(y) = 0 \\ &\iff \exists\, C_1 \in \mathbb{C} \text{ tel que } \circ D \circ \varphi_{-r_2 \cdot t}(y) = C_1 \exp((r_1 - r_2)t) \\ &\iff \exists\, C_1 \in \mathbb{C} \text{ tel que } \circ D \circ \varphi_{-r_2 \cdot t}(y) = C_1 \exp((r_1 - r_2)t) \end{aligned}$$

— Si $r_1 = r_2$, $ay'' + by' + cy = 0 \iff \exists\, C_1, C_2 \in \mathbb{C}$ tels que $y = (C_1 t + C_2)\exp(r_2 t)$.
— Si $r_1 \neq r_2$, $ay'' + by' + cy = 0 \iff \exists\, C_1, C_2 \in \mathbb{C}$ tels que $y = \dfrac{C_1}{r_1 - r_2}\exp(r_1 \cdot t) + C_2 \exp(r_2 \cdot t)$.

□

Pour le cas réel, la partie correspondant aux racines complexes ($\Delta < 0$) est plus subtile.

Théorème - Cas réel

On suppose ici a, b, c réels, $a \neq 0$.

— Si $ar^2 + br + c = 0$ possède deux racines réelles distinctes r_1 et r_2 alors l'ensemble des solutions à valeurs dans $\mathbb{R}$ est :

$$S_H = \left\{t \mapsto \lambda e^{r_1 t} + \mu e^{r_2 t}; (\lambda, \mu) \in \mathbb{R}^2\right\}$$

— Si $ar^2 + br + c = 0$ possède une racine double $r_0 \in \mathbb{R}$ alors l'ensemble des solutions à valeurs dans $\mathbb{R}$ est :

$$S_H = \left\{t \mapsto (\lambda + \mu t)e^{r_0 t}; (\lambda, \mu) \in \mathbb{R}^2\right\}$$

— Si $ar^2 + br + c = 0$ possède deux racines complexes conjuguées $\alpha + i\beta$

et $\alpha - i\beta$ alors l'ensemble des solutions à valeurs dans $\mathbb{R}$ est :

$$S_H = \left\{ t \mapsto \lambda e^{\alpha t}\cos\beta t + \mu e^{\alpha t}\sin\beta t ; (\lambda,\mu)\in\mathbb{R}^2 \right\}$$

Pour la démonstration, commençons par un lemme

Lemme - Solution réelle d'une équation réelle
Soit (H) l'équation différentielle homogène $ay''+by'+cy=0$ où $(a,b,c)\in\mathbb{R}^3, a\neq 0$.
Si f est solution de (H) à valeurs dans $\mathbb{C}$ alors $\mathrm{Re}f$ est solution de (H) à valeurs réelles.
Plus précisément l'ensemble des solutions réelles de (H) est exactement l'ensemble des parties réelles des solutions complexes de (H).

Démonstration
Démonstration du lemme :
On rappelle que $a,b,c\in\mathbb{R}$.Supposons que $f=f_R+if_I$ est solution de (H).
Alors
$$0 = af''+bf'+cf = \left(af_R''+bf_R'+cf_R\right)+i\left(af_I''+bf_I'+cf_I\right)$$
Donc $af_R''+bf_R'+cf_R=0$ et f_R est à valeurs réelles.
On a donc : toute partie réelle de solutions complexes de (H) est une solution réelle de (H).
Réciproquement, si f est une solution réelle de (H),
alors $f+i0$ est une solution complexes de (H) dont f est la partie réelle.
Démonstration du théorème :
Les deux premiers cas se déduisent du cas complexe.
Supposons donc que le discriminant de l'équation caractéristique $\Delta<0$.
L'équation caractéristique est à coefficients réels donc les racines sont conjuguées : $\alpha+i\beta$ et $\alpha-i\beta$.
Les solutions sur $\mathbb{C}$ sont de la forme
$$f : t\mapsto \lambda e^{(\alpha+i\beta)t}+\mu e^{(\alpha-i\beta)t}$$
La partie réelle est alors une solution de (H) sur $\mathbb{R}$:
$$t\mapsto \frac{1}{2}(f+\overline{f})(t) = \frac{1}{2}(\lambda+\overline{\mu})e^{\alpha t+i\beta t}+\frac{1}{2}(\overline{\lambda}+\mu)e^{\alpha t-i\beta t}$$
$$t\mapsto e^{\alpha t}\left(\mathrm{Re}(\lambda+\mu)\cos(\beta t)+\mathrm{Im}(\mu-\lambda)\sin(\beta t)\right)$$
□

Remarque - Autre expression pour le cas $\Delta<0$
Dans le cas des racines complexes conjuguées, on peut poser $\lambda+i\mu=Ae^{-i\phi}$, où $A\geqslant 0$ et $\phi\in\mathbb{R}$. Les solutions s'écrivent alors $t\mapsto Ae^{\alpha t}\cos(\beta t+\phi)$
C'est un cas souvent préféré en physique.

Remarque - Base d'une espace vectoriel
Dans tous les cas (réel ou complexe) $S_H=\left\{\lambda f_1+\mu f_2;(\lambda,\mu)\in\mathbb{K}^2\right\}$ où f_1 et f_2 sont deux fonctions déterminées par l'équation caractéristique associée. On dira que la famille (f_1,f_2) est une *base* de S_H.
On en déduira que S_H est un espace vectoriel de dimension 2 (=nombre de vecteurs de la base).

Exercice
Résoudre les équations différentielles suivantes (on cherchera les solutions réelles).
1. $y''=\omega^2 y$
2. $y''=-\omega^2 y$
3. $y''-4y'+13y=0$
4. $y''-4y'+4y=0$

Correction
1. L'équation caractéristique est $x^2-\omega^2=0$, de racine $\pm\omega$.
   Les solutions de l'équation différentielle sont donc de la forme $t\mapsto Ae^{\omega t}+A'e^{-\omega t}$, avec $A,A'\in\mathbb{R}$

Pour aller plus loin - Paramètres
Considérons l'équation aux paramètres physiques : $y''+\frac{\omega}{Q}y'+\omega_0^2 y=0$.
On a $\Delta=\left(\frac{\omega_0}{Q}\right)^2\left(1-4Q^2\right)$.
- *si $\Delta<0$ ($Q>\frac{1}{2}$) : régime périodique, les solutions sont de la forme $e^{-\frac{\omega_0}{2Q}t}(A\cos(\omega t+\varphi)$ avec $\omega=\frac{\omega_0}{Q}\sqrt{Q^2-\frac{1}{4}}$. Comme $\omega_0,Q>0$, les solutions sont oscillantes, bornées et de fréquence $\omega=\frac{\omega_0}{Q}\sqrt{Q^2-\frac{1}{4}}$*
- *si $\Delta=0$ ($Q=\frac{1}{2}$) : régime critique, les solutions sont de la forme $e^{\omega_0 t}(At+B)$*
- *si $\Delta>0$ ($Q<\frac{1}{2}$) : régime a-périodique, les solutions sont de la forme $Ae^{-\frac{\omega_0}{Q}(1+\sqrt{\frac{1}{4}-Q^2})t}+Be^{-\frac{\omega_0}{Q}(1-\sqrt{\frac{1}{4}-Q^2})t}$*

2. L'équation caractéristique est $x^2+\omega^2=0$, de racine $0\pm i\omega$.
   Les solutions de l'équation différentielle sont donc de la forme $t\mapsto A\cos(\omega t)+A'\sin(\omega t)$, avec $A,A'\in\mathbb{R}$
3. L'équation caractéristique est $x^2-4x+13=0$, de racine $2\pm 3i$.
   Les solutions de l'équation différentielle sont donc de la forme $t\mapsto e^{2t}(A\cos(3t)+A'\sin(3t))$, avec $A,A'\in\mathbb{R}$
4. L'équation caractéristique est $x^2-4x+4=0$, de racine double 2.
   Les solutions de l'équation différentielle sont donc de la forme $t\mapsto (A+A't)e^{2t}s$, avec $A,A'\in\mathbb{R}$

Résolution avec second membre

On considère l'équation complète $(E)\quad ay''+by'+cy=u(t)$ avec $(a,b,c)\in\mathbb{K}^3, a\neq 0$.

Théorème - Structure de l'ensemble S_E
La solution générale de l'équation (E) est la somme d'une solution particulière et de la solution générale de l'équation homogène associée (H), ce qui peut aussi s'écrire :
Si $\tilde{y}$ est une solution particulière de l'équation (E) et (f_1,f_2) une base de S_H alors
$$S_E=\left\{t\mapsto \lambda f_1(t)+\mu f_2(t)+\tilde{y}(t);(\lambda,\mu)\in\mathbb{K}^2\right\}.$$

Démonstration
On démontre que $y-\tilde{y}$ est solution de (H) et donc de la forme $\lambda f_1(t)+\mu f_2(t)$ □

Proposition - Principe de superposition des solutions
Si le second membre de l'équation (E) est de la forme $u(t)=u_1(t)+\cdots+u_n(t)$
et si l'on connaît des solutions particulières $\tilde{y}_1,\ldots,\tilde{y}_n$ des équations avec les seconds membres $u_1(t),\ldots,u_n(t)$,
alors une solution particulière de (E) est $\tilde{y}=\tilde{y}_1+\cdots+\tilde{y}_n$.

Remarque - Démonstration
Il s'agit exactement de la même démonstration que dans le cas $n=1$.
Ce qui compte ici c'est la linéarité. (Le fait que les coefficients soient constants ne changent rien concernant ce théorème de superposition)

Avec second membre : exponentielle-polynôme

On va s'intéresser au cas où $u(t)=e^{mt}P(t)$ avec $m\in\mathbb{C}$ et P une fonction polynomiale à valeurs complexes.

Savoir faire - Second membre $e^{mt}P(t)$
Soit $m\in\mathbb{C}$ et P une fonction polynomiale de degré n. Alors on peut trouver une solution particulière de l'équation
$$(E)\quad ay''+by'+cy=e^{mt}P(t)$$
de la forme $\tilde{y}(t)=e^{mt}Q(t)$ où Q est une fonction polynomiale
- de degré n si m n'est pas racine de $ar^2+br+c=0$
- de degré $n+1$ si m est racine simple de $ar^2+br+c=0$
- de degré $n+2$ si m est racine double de $ar^2+br+c=0$

Pour aller plus loin - Méthode de Laplace
On note $\mathscr{L}:f\mapsto F$, telle que $F:p\mapsto\int_0^{+\infty}f(t)e^{-pt}\mathrm{d}t$ On montre (IPP) alors que $\mathscr{L}(f')(p)=pf(p)-f(0^+)$.
On transforme ainsi une dérivation en un produit et donc l'équation $ay''+by'+cy=g$ se transforme en
$$(ap^2+bp+c)F(p)=G(p)$$
et donc $F(p)=\frac{G(p)}{ap^2+bp+c}$, il reste donc à appliquer $\mathscr{L}^{-1}$ à F pour trouver la valeur de f…

Pour aller plus loin - Equations en physique
1. *Dans un circuit RC ou RL, τ étant la constante de temps, $E(t)$ la tension*

Démonstration
Le calcul donne :

$$a\widetilde{y}''(t)+b\widetilde{y}'(t)+c\widetilde{y}(t)=[(am^2+bm+c)Q(t)+(2am+b)Q'(t)+aQ''(t)]e^{mt}$$

Si $d=\deg(Q)$, alors $\deg(Q')=d-1$ et $\deg(Q'')=d-2$.

$$\widetilde{y} \text{ solution de } (E) \Longleftrightarrow \forall\, t\in I[(am^2+bm+c)Q(t)+(2am+b)Q'(t)+aQ''(t)]=P(t)$$

Nécessairement les polynômes doivent être de même degré. Donc :
- si m n'est pas racine de $ar^2+br+c=0$, $\deg(Q)=\deg(P)=n$
- si m est racine simple de $ar^2+br+c=0$, donc $2am+b\neq 0$, alors $\deg(Q')=\deg P$, donc $d-1=n$, i.e. $d=n+1$
- si m est racine double de $ar^2+br+c=0$ donc $2am+b=0$, alors $\deg(Q'')=\deg P$, donc $d-2=n$, i.e. $d=n+2$

La condition d'existence donne l'unicité (analyse). Il faut vérifier l'existence (synthèse). Il s'agit alors d'un système inversible de n équations à n inconnues à résoudre. □

Analyse - Polynôme × fonction trigonométrique

On peut utiliser ce qui précède pour le cas où $(a,b,c)\in\mathbb{R}^3$ et $u(t)=e^{\alpha t}(P(t)\cos\beta t+Q(t)\sin\beta t)$ avec P,Q des fonctions polynomiales à coefficients réels.
Dans ce cas le second membre est de la forme $T(t)e^{(\alpha+i\beta)t}$ où T est un polynôme complexe.
Or ce second membre est a priori réel. Le calcul suivant donne :

$$e^{\alpha t}(P(t)\cos\beta t+Q(t)\sin\beta t)=\mathrm{Re}\Big((P(t)-iQ(t))e^{(\alpha+i\beta)t}\Big)$$

on en déduit que $T=P(t)+iQ(t)$ et on peut chercher une solution particulière (sur $\mathbb{C}$) de la forme $R(t)e^{\alpha+i\beta t}$ avec :
- $\deg R=\deg T$ si $\alpha+i\beta$ n'est pas racine de $ar^2+br+c=0$
- $\deg R=\deg T$ si $\alpha+i\beta$ est racine simple $ar^2+br+c=0$.
  (Elle ne peut être racine double, sinon l'équation serait à coefficients complexes)

Si $\widetilde{y}$ est une solution à valeurs complexes de l'équation avec le second membre $(P(t)-iQ(t))e^{(\alpha+i\beta)t}$, alors $\mathrm{Re}(\widetilde{y})$ est une solution particulière à valeurs réelles.

Savoir faire - Second membre de la forme $e^{\alpha t}(P(t)\cos\beta t+Q(t)\sin\beta t)$

On peut trouver (par identification) une solution particulière de l'équation

$$(E)\quad ay''+by'+cy=e^{\alpha t}(P(t)\cos(\beta t)+Q(t)\sin(\beta t))$$

de la forme $\widetilde{y}(t)=e^{\alpha t}(T(t)\cos(\beta t)+R(t)\sin(\beta t))$ où T et R sont des fonctions polynomiales
- de degré $n=\max(\deg(P),\deg(Q))$ si $\alpha+i\beta$ n'est pas racine de $ar^2+br+c=0$
- de degré $n+1=\max(\deg(P),\deg(Q))+1$ si $\alpha+i\beta$ est racine simple de $ar^2+br+c=0$

Exercice
1. Résoudre $y''-y'-2y=3e^{-t}+1$.
2. Résoudre $y''+2y'+5y=\cos^2 t$.

Correction

1. L'équation homogène est (H) $y''-y'-2y=0$ d'équation caractéristique $r^2-r-2=(r-2)(r+1)$.
   Les solutions de (H) sont de la forme $t\mapsto Ae^{2t}+A'e^{-t}$.
   En exploitant le théorème précédent et le principe de superposition, on cherche une solution particulière sous la forme
   $$\widetilde{y}:t\mapsto C_1te^{-t}+C_2$$
   Or
   $$\widetilde{y}''(t)-\widetilde{y}'(t)-2\widetilde{y}(t)=C_1[(-2-1)+(1+1-2)t]e^{-t}+C_2=-3C_1e^{-t}+C_2$$
   Donc $C_1=-1$ et $C_2=1$ et les solutions de (E) sont :
   $$t\mapsto Ae^{-2t}+(A'-t)e^{-t}+1\qquad \text{avec } A,A'\in\mathbb{R}$$

2. L'équation homogène est (H) $y''+2y'+5y=0$ d'équation caractéristique r^2+2r+5, de discriminant $\Delta=-16$ et donc de racine $-1\pm 2i$.
   Les solutions de (H) sont de la forme $t\mapsto e^{-t}(A\cos 2t+A'\sin 2t)$.
   En outre $\cos^2 t=\frac{1}{2}(\cos 2t+1)$, donc le second membre est (en partie) de la forme $e^{\alpha t}(P(t)\cos\beta t+Q(t)\sin\beta t)$, avec $\alpha=0$, $\beta=2$, $P(t)=\frac{1}{2}$ et $Q(t)=0$.
   Pas besoin de monter en degré et on peut donc chercher une solution particulière de la forme
   $$\widetilde{y}:t\mapsto C_1\cos(2t)+C_2\sin(2t)+C_3$$
   Or
   $$\widetilde{y}''(t)+2\widetilde{y}'(t)+5\widetilde{y}(t)=(C_1+4C_2)\cos(2t)+(C_2-4C_1)\sin(2t)+5C_3$$
   Donc $C_1=\frac{1}{34}$, $C_2=\frac{4}{34}$ et $C_3=\frac{1}{10}$ et les solutions de (E) sont :
   $$t\mapsto e^{-t}(A\cos 2t+A'\sin 2t)+\frac{1}{34}(\cos 2t+4\sin 2t)+\frac{1}{10}\qquad \text{avec } A,A'\in\mathbb{R}$$

Résolution du problème de Cauchy

Théorème - Conditions initiales
Soit (E) $ay''+by'+cy=u(t)$ avec $(a,b,c)\in\mathbb{K}^3, a\neq 0$ et $u:I\to\mathbb{K}$ de l'une des formes précédentes. Soit $(t_0,y_0,y_0')\in I\times\mathbb{K}\times\mathbb{K}$.
Alors il existe une unique solution $f:I\to\mathbb{K}$ telle que $f(t_0)=y_0$ et $f'(t_0)=y_0'$.

La démonstration est simple : les deux conditions initiales fixent les deux valeurs des deux variables libres λ et μ.

Démonstration
• Cas $\Delta\neq 0$.
Soit y une solution de (E), alors il existe $\lambda,\mu\in\mathbb{C}$ tels que $y=\lambda e^{r_1t}+\mu e^{r_2t}$.
On a également $y(t_0)=y_0=\lambda e^{r_1t_0}+\mu e^{r_2t_0}$ et $y'(t_0)=y_0'=r_1\lambda e^{r_1t_0}+r_2\mu e^{r_2t_0}$.
Ce qui donne le système de Cramer de déterminant $(r_2-r_1)e^{(r_1+r_2)t}\neq 0$:

$$\begin{cases} e^{r_1t_0}\lambda & +e^{r_2t_0}\mu & =y_0\\ r_1e^{r_1t_0}\lambda & +r_2e^{r_2t_0}\mu & =y_0'\end{cases}\Longrightarrow\begin{cases}\lambda=\dfrac{r_2y_0-y_0'}{r_2-r_1}e^{-r_1t_0}\\ \mu=\dfrac{r_1y_0-y_0'}{r_1-r_2}e^{-r_2t_0}\end{cases}$$

On a donc trouvé au plus une solution au problème. La réciproque prouve que cette fonction est bien solution.
• Cas $\Delta=0$.
Soit y une solution de (E), alors il existe $\lambda,\mu\in\mathbb{C}$ tels que $y=(\lambda+\mu t)e^{rt}$.
On a également $y(t_0)=y_0=(\lambda+\mu t_0)e^{rt_0}$ et $y'(t_0)=y_0'=(r\lambda+\mu+r\mu t_0)+e^{rt_0}$.
Ce qui donne le système de Cramer de déterminant $1\neq 0$:

$$\begin{cases} e^{rt_0}\lambda & +e^{rt_0}t_0\mu & =y_0\\ re^{rt_0}\lambda & +(1+rt_0)e^{rt_0}\mu & =y_0'\end{cases}\Longrightarrow\begin{cases}\lambda=(y_0(1+rt_0)-y_0't_0)e^{rt_0}\\ \mu=(-y_0r+y_0')e^{rt_0}\end{cases}$$

On a donc trouvé au plus une solution au problème. La réciproque prouve que cette fonction est bien solution.
□

Exercice
Résoudre le problème de Cauchy : $y''-2y'+y=te^t$ avec les conditions $y(0)=0$ et $y'(0)=1$.

Correction
L'équation homogène est (H) $y''-2y'+y=0$ d'équation caractéristique $r^2-r+1=(r-1)^2$.
Les solutions de (H) sont de la forme $t\mapsto(A+A't)e^t$.
En exploitant le théorème de la partie précédente, on cherche une solution particulière sous la forme

$$\widetilde{y}:t\mapsto(C_1t^2+C_2t^3)e^t$$

Or

$$\widetilde{y}''(t)-2\widetilde{y}'(t)+\widetilde{y}(t)=\Big(C_1[(t^2-2t^2+t^2)+(4t-4t)+2)]+C_3[(t^3-3t^3+t^3)+(6t^2-6t^2)+6t]\Big)e^t$$

Donc $C_1=0$ et $C_2=\frac{1}{6}$ et les solutions de (E) sont :

$$t\mapsto(A+A't+\frac{1}{6}t^3)e^t\qquad \text{avec } A,A'\in\mathbb{R}$$

Avec les condition de Cauchy, cela donne :

$$\begin{cases} A & = & 0 \\ A & +A' & = & 1 \end{cases} \Leftrightarrow \begin{cases} A=0 \\ A'=1 \end{cases}$$

Donc la solution du problème de Cauchy est $y : t \mapsto (t+\frac{1}{6}t^3)e^t$

Exercice

Résoudre les équations différentielles de la physique (cadre)

Correction

5. Bilan

Synthèse

- ⇝ A toute fonction f, on associe (par un tableau) une fonction f' qui est sa dérivée. Réciproquement, on peut essayer de lui associer une fonction F dont elle (=f) serait la dérivée. Cette fonction F non unique s'appelle une primitive de f. On a un tableau de fonctions usuelles à APPRENDRE par coeur.
- ⇝ Il n'existe pas d'algorithme simple de primitivisation comme il en existe de dérivation. La seule chose que l'on sait (et que l'on démontrera plus tard) est que toute fonction continue sur un intervalle I admet une primitive sur cet intervalle I. On fait ce que l'on peut en reconnaissant localement des situations : pour une somme de fonctions, la linéarité suffit ; pour un produit, on exploite une intégration par parties ; pour une composition, on utilise un changement de variable.
- ⇝ Une équation différentielle est une équation (égalité) dont l'inconnue est une fonction et qui associe cette fonction à ses dérivées. L'équation peut être linéaire, d'ordre quelconque (un entier), écrite sous forme normale… On lui associe une courbe intégrale.
  L'ensemble des solutions apparait (pour les équations différentielles linéaires) sous forme d'un espace affine.
- ⇝ Le problème théorique consiste à trouver des hypothèses qui assure l'existence d'une solution (unique?) à une équation différentielle, sur un intervalle le plu grand possible.
  Pour les équations différentielles linéaires, une théorie satisfaisante est donné par le théorème de Cauchy. A connaître par coeur avec toutes ses hypothèses et toutes ses conclusions (ordre 1 ou 2)…
- ⇝ Le problème pratique consiste à résoudre l'équation. Nous avons mis au point des stratégies : la méthode de la variation de la constante (pour les EDL1). Au passage, on rencontre le problème du recollement de solutions sur des intervalles joints ; ainsi que l'étude des inéquations différentielles.
  Pour les EDL2, nous nous limitons cette année aux équations à coefficients constants. La méthode est simple : il s'agit de mettre en parallèle cette équation différentielle et l'équation caractéristique (polynomiale de degré 2), puis de résoudre cette seconde équation. La forme des solutions et les solutions de cette seconde équation (polynomiale) donnent la forme des solutions et les solutions de la première (différentielle).

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - $e^{\alpha x}\cos\beta x$ ou $e^{\alpha x}\sin\beta x$
- Savoir-faire - $\sin^n x\cos^m x$
- Savoir-faire - Fractions rationnelles $\dfrac{1}{ax^2+bx+c}$
- Truc & Astuce pour le calcul - Encadrer une intégrale

- Savoir-faire - Inégalité des accroissements finis (avec f de classe $\mathscr{C}^1$)
- Savoir-faire - Obtenir une primitive avec une IPP cachée
- Savoir-faire - $f(x)=P(x)e^{\alpha x}$
- Savoir-faire - $f(x)=P(x)\ln(Q(x))$
- Savoir-faire - Changement de variable - dans la pratique
- Savoir-faire - Calculer une primitive par changement de variable
- Savoir-faire - Bijection par morceaux
- Savoir-faire - Calcul pour $f(t)=\sin^n t\cos^m t$ avec n ou m impair.
- Savoir-faire - Cas général (tan $\frac{x}{2}$).
- Savoir-faire - Variable dans les bornes de l'intégrales.
- Savoir-faire - Découper I pour avoir des équations normalisées
- Savoir-faire - Méthode de « variation de la constante ».
- Savoir-faire - Etudier une inéquation différentielle.
- Savoir-faire - Cas non résolue (recollement).
- Savoir-faire - Second membre de la forme $e^{\alpha t}(P(t)\cos\beta t+Q(t)\sin\beta t)$.

Notations

Notations	*Définitions*	*Propriétés*	*Remarq*
$[\Phi(t)]_\cdot^x=\Phi(x)$	« Crochet » de Φ	Par extension : $[\Phi]_a^b=\Phi(b)-\Phi(a)$	On trou
$\int_a^b f(t)\mathrm{d}t$	Intégrale de f entre a et b. Il s'agit de l'aire « sous » la courbe	Pour tout $a\in\mathscr{D}_f$ et f continue, $x\mapsto\int_a^x f(t)\mathrm{d}t$ est une primitive de f	
$\int_\cdot^x f(t)\mathrm{d}t$	(Ensemble des) primitive(s) de f		Attentio primitiv

Retour sur les problèmes

25. Il est miraculeux qu'ils s'agissent des deux faces d'une même pièce. C'est Newton et Leibniz qui s'en rendirent compte les premiers, indépendamment et en prenant des chemins très différents. Certains pensent que Fermat l'avait compris… Un célèbre faux du XIX siècle fit croire à Michel Chasles que le premier avait été en réalité Blaise Pascal. Un mauvais pari de l'académicien français.
26. C'est l'application $x\mapsto 2^x u_0 = u_0 e^{x\ln 2}$
27. Rien de simple. D'où les deux méthodes : intégration par parties (pour un produit) et changement de variable (pour une composition).
28. Oui c'est possible, on l'aperçoit dans le cours. Mais le moins qu'on puisse dire c'est que la technique est très technique !
29. Toute fonction continue est intégrable (voir plus tard dans l'année). La réciproque est fausse : certaine fonction non continue sont néanmoins intégrable. En regardant la courbe, on trouve qu'il y a une compensation : $\int_0^\pi \tan(t)\mathrm{d}t=0$.
    Mais concrètement, une primitive de tan = $\frac{\sin}{\cos}$ est $-\ln(|\cos|)+K$, mal définie en $\frac{\pi}{2}$. On ne peut inopinément écrire : $+\infty-\infty=0$…
30. Cf. Cours de physique
31. Le théorème de Cauchy a pour but de répondre à cette question. Dans le cadre des équations linéaires, il allie nombre liberté (ordre de l'équation) et nombre de contraintes (conditions initiales).
32. Nous verrons une autre option pour étudier des équations différentielles : la force brute de calcul de l'ordinateur. La solution ne sera qu'approchée, mais l'approximation sera diablement efficace (méthode d'Euler, Heun…).

Chapitre 7

Calculs et opérations avec des sommes ou des produits

Résumé -

Pour commencer, nous apprenons à manipuler les symboles $\sum$ et $\prod$.
Nous prendrons également le temps d'étudier les méthodes d'étude des doubles sommes (finies).
Les résultats se basent sur la commutativité de l'addition. Tant que les sommes sont finies, il n'y a pas de surprise dans les résultats obtenus. Le cas infini sera étudié plus tard.
Nous obtenons alors un premier résultat intéressant : les coefficients binomiaux (point de vue complémentaire à celui vu au lycée) et leur application à la formule du binôme de Newton. Nous faisons un petit plongeon dans l'histoire des mathématiques au XVII : les coefficients binomiaux agitaient la communauté des mathématiciens de l'époque.

Enfin, voici une liste de petites vidéo ou conférence visionnable sur internet et en lien avec le sujet (de pénibilités variées) :
- *Yvan Monka - Symbole Sigma. https ://www.youtube.com/watch ?v=0zspJuzo7L8*
- *El Jj - Nombres de Catalan. http ://eljjdx.canalblog.com/archives/2017/02/20/34959863.html*
- *Maths moi ça - L'étonnant triangle de Pascal. https ://www.youtube.com/watch ?v=IzkfjbWffpc*

Sommaire

1. Quelques problèmes 138
2. Symboles $\sum$ et $\prod$ 138
2.1. Définition 138
2.2. Quatre règles opératoires 140
2.3. Avec Python 143
2.4. Des sommes connues 144
2.5. Sommes doubles (multiples...) 146
2.6. Exercice d'applications 150
3. Coefficients binomiaux et formule du binôme 151
3.1. Factorielles et coefficients binomiaux 151
3.2. Triangle de Pascal 152
3.3. Formule du binôme 153
4. Bilan 154

1. Quelques problèmes

Problème 33 - Nombres triangulaires

Lorsqu'on fait la somme 1+1+1+... 1, on peut décrire tous les nombres entiers.
Si on somme ensuite les résultats obtenus : $1+2+\cdots+n$*, quel nombre obtient-on ?*
Ce nombre est appelé nombre triangulaire d'ordre n, noté T_n. Par exemple : $T_4 = 1+2+3+4 = 10$.
Si on somme ensuite les résultats obtenus : $T_1+T_2+\cdots+T_n = 1+3+6+10+\cdots+T_n$*, quel nombre obtient-on ? Et si on continue, toujours ?*

Problème 34 - Développement

Donner, pour tout entier n, la forme développée des applications polynomiales $x \mapsto (x-1)(x-2)(x-3)\dots(x-n)$ et $x \mapsto (1+x)(1+2x)(1+3x)\dots(1+nx)$

Problème 35 - Suite de nombres. Et le suivant ?

Prenons la suite obtenue à la question précédente : $1, 4, 10, 20, 35$. Quel est le terme suivant ?
Et de manière générale étant donnée une suite quelconque de n termes donnés explicitement, comment trouver le terme suivant ?

Problème 36 - Interpolation à pas constant

Quelle est la fonction f de degré minimal tel $f(0) = 1$, $f(1) = -1$, $f(2) = 1$, $f(3) = 4$?
Généraliser la question et donner une réponse...

Problème 37 - Développement de puissance

Considérons le calcul typiquement algébrique : $(a+b)^n$ où a et b sont deux nombres quelconques et n en entier.
L'expérience montre que pour $n = 4$ (par exemple), on trouve en développant cette expression : $a^4+4a^3b+6a^2b^2+4ab^3+b^4$.
Est-il possible de décrire simplement cette expression : quels sont les facteurs a et b obtenus, est-il facile d'exprimer/calculer le nombre situé devant $a^i b^j$?
Et que se passe-t-il si l'on considère plutôt $(a+b+c+\dots)^m$?

2. Symboles $\sum$ et $\prod$

2.1. Définition

Remarque - Terme sans ambiguïté

La façon naturelle d'écrire une somme longue est de :

1. donner les premiers termes

2. s'assurer que la suite logique des termes est comprises, puis de remplacer ces termes (en grands nombres) par des points de suspension
3. donner la valeur du dernier terme.

Mais comment s'assurer qu'il n'y ait pas ambiguïté? On préfère souvent une formulation explicite :

5) qui utilise Σ pour désint utile pour pitre, Euler a portants aux

Définition - Notation ∑ et ∏
Soient $a_1,\dots,a_n$ n nombres réels ou complexes. L'addition dans $\mathbb{R}$ ou $\mathbb{C}$ étant commutative (on somme dans l'ordre que l'on souhaite) et associative (les parenthèses ne sont pas nécessaires), on note

$$\sum_{i=1}^{n} a_i = a_1 + \cdots + a_n$$

De même on note

$$\prod_{i=1}^{n} a_i = a_1 a_2 \dots a_n.$$

Le terme a_i s'écrit sous forme d'une formule dépendant de i.

Remarque - Bons usages et généralisation de notation
Bien évidemment, l'indice i (qui peut aussi s'appeler k, l, m, p ...) de la somme peut démarrer à une valeur entière autre que 1, toutefois la valeur de départ (sous le signe $\sum$) doit être inférieure à la valeur d'arrivée.

Exercice
Ecrire avec le symbole $\sum$, le calcul $1+2+4+\cdots+128$

Correction
On reconnait des puissances successives de 2. $1+2+4+\cdots+128 = \sum_{k=0}^{7} 2^k$

Plus généralement,

Définition - Extension de notation ∑ et ∏
Si I est un sous-ensemble fini de $\mathbb{N}$, $I = \{i_1, i_2, \dots, i_p\}$, on note

$$\sum_{i\in I} a_i = a_{i_1} + a_{i_2} + \cdots + a_{i_p} = \sum_i a_i \mathbb{1}_I(i)$$

où $\mathbb{1}_I : i \mapsto \begin{cases} 1 \text{ si } i \in I \\ 0 \text{ si } i \notin I \end{cases}$ est l'indicatrice de I.
On peut également noter, si $\mathscr{P}(i)$ désigne une propriété sur les entiers (parité, imparité...),

$$\sum_{i|\mathscr{P}(i)} a_i = \sum_{i\in\{j\in\mathbb{N}|\mathscr{P}(j) \text{ vraie }\}} a_i = \sum_i a_i [\mathscr{P}(i)]$$

où $[\mathscr{P}(i)]$ est *la notation d'Iverson* qui vaut 1 ssi $\mathscr{P}(i)$ est vraie et 0 sinon.
Ces notations se généralisant au produit.

Pour aller plus loin - Descriptions des ensembles
Nous verrons qu'un ensemble se définit en règle générale, soit par extension : $I = \{i_1, i_2, \dots, i_p\}$ soit par compréhension : $I = \{i \mid \mathscr{P}(i) \text{ (vraie)}\}$

Exemple - $\sum_{i=1}^{n} a_i$
Par exemple $\sum_{i=1}^{n} a_i = \sum_{i\in[\![1,n]\!]} a_i = \sum_{1\leqslant i\leqslant n} a_i$.
Cette dernière est un abus de $\sum_{i\in\mathbb{N}\,|\,1\leqslant i\leqslant n} a_i$.

Exercice
Sans utiliser la notation $\sum$, donner l'expression développée de

$$\sum_{i|0\leqslant i\leqslant 6} \frac{1}{2i+1}, \quad \sum_{i|0\leqslant 2i\leqslant 7} \left(3i + \frac{1}{i+1}\right), \quad \sum_{i|0\leqslant i^3\leqslant 10} \frac{1}{i^2+i+1}.$$

Pour aller plus loin - Notation $\mathbb{N}_n$
On note, tout au long de l'année :

$$\mathbb{N}_n = [\![1, n]\!]$$

Cet ensemble commence bien à 1.
Cette notation n'est pas standardisée

Correction
$\sum_{i|0\leqslant i\leqslant 6} \frac{1}{2i+1} = \frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{13}$ - $\sum_{i|0\leqslant 2i\leqslant 7} 3i + \frac{1}{i+1} = 3+6+9+1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}$ - $\sum_{i|0\leqslant i^3\leqslant 10} \frac{1}{i^2+i+1} = \frac{1}{1} + \frac{1}{3} + \frac{1}{7}$

Attention - Attention à ne pas donner une existence à une variable muette!
Que vaut $\left(\sum_{k=1}^{n} 2^k\right) + k$? Rien!

Exercice
Exprimer la somme des inverses de tous les nombres premiers inférieurs à N

Correction
Par exemple $\sum_p \frac{1}{p}[p \leqslant N][p \text{, premier}]$ ou encore $\sum_{p\leqslant N} \frac{1}{p}[p \text{, premier}]$ ou $\sum_{p\in\mathscr{P}\cap\mathbb{N}_N} \frac{1}{p}$...

2.2. Quatre règles opératoires

Nouvelle description de l'ensemble

Si on a un doute, on exploite **au brouillon** des points de suspension.

Analyse - Changement d'indice
Supposons que l'on ait à calculer $S = \sum_{a\in A} a$.
On peut supposons arbitrairement que $A = \{a_1, a_2, \dots a_n\}$.
Alors S peut s'écrire sous la forme $\sum_{i\in M} a_i$ où M est une description quelconque de l'ensemble $[\![1, n]\!]$.
Deux cas sont classiques : $M = \{1, 2, \dots n\}$ ou encore $M = \{n, n-1, n-2, \dots n-(n-1)\}$.
Ainsi, on a $S = \sum_{i=1}^{n} a_i = \sum_{h=0}^{n-1} a_{n-h}$, par exemple.
On peut imaginer d'autres écritures...

Savoir faire - Exemple de changement
Faire le changement d'indice $i = n-k$ pour $\sum_{k=1}^{n} (2k+1)$
On a donc $k = n-i$ et $2k+1 = 2n-2i+1 = (2n+1)-2i$.
Et le tableau de correspondance :

k	i
1	$n-1$
n	0

.
Donc $\sum_{k=1}^{10} (2k+1) = \sum_{i=0}^{n-1} [(2n+1)-2i]$

On notera que les termes i sont notés dans l'ordre croissant (ce qui inverse l'ordre du calcul effectivement réalisé).

Exercice
Compléter les expressions qui suivent :

$$\sum_{i=1}^{n} a_i = \sum_{\dots}^{\dots} a_{k-1} = \sum_{\dots}^{\dots} a_{n-h}$$

Correction
$\sum_{i=1}^{n} a_i = \sum_{k=2}^{n+1} a_{k-1} = \sum_{h=0}^{n-1} a_{n-h}$

Somme, par récurrence

Analyse - ∑ et récurrence
Le symbole somme est particulièrement liée au raisonnement par récurrence.

En effet celui-ci a également pour vocation de formaliser le raisonnement avec des points de suspension.

Plus précisément, si on note, pour tout $n \in \mathbb{N}$, $S_n = \sum_{k=0}^{n} a_k$, alors (S_n) est exactement la suite définie par $S_0 = a_0$ et par la relation de *récurrence* : pour tout $n \in \mathbb{N}$, $S_{n+1} = S_n + a_{n+1}$

Proposition - A savoir!
On a pour $(a_i)_i, (b_i)_i, \lambda \in \mathbb{R}$ ou $\mathbb{C}$, :

$$\sum_{i=0}^{n}(a_i+b_i) = \sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i \qquad \sum_{i=0}^{n} \lambda a_i = \lambda \sum_{i=0}^{n} a_i$$

$$\prod_{i=0}^{n} a_i b_i = \prod_{i=0}^{n} a_i \times \prod_{i=0}^{n} b_i \qquad \prod_{i=0}^{n} \lambda a_i = \lambda^{n+1} \prod_{i=0}^{n} a_i$$

Démonstration
On note $R_n = \sum_{i=1}^{n}(a_i+b_i)$, $S_n = \sum_{i=1}^{n} a_i$ et $T_n = \sum_{i=1}^{n} b_i$,
puis pour tout entier n, $\mathscr{P}_n : R_n = S_n + T_n$.
— $R_0 = (a_0 + b_0) = a_0 + b_0 = S_0 + T_0$, donc $\mathscr{P}_0$ est vraie.
— Soit $n \in \mathbb{N}$, supposons que $\mathscr{P}_n$ est vraie.

$$R_{n+1} = R_n + (a_{n+1} + b_{n+1}) = S_n + T_n + a_{n+1} + b_{n+1} = S_{n+1} + R_{n+1}$$

Donc $\mathscr{P}_{n+1}$ est alors vraie.
La récurrence est démontrée.
Pour le second résultat, on va exploiter une méthode : l'utilisation d'un invariant de boucle.
Notons, pour tout $n \in \mathbb{N}$, $A_n = \sum_{i=1}^{n} \lambda a_i - \lambda \sum_{i=1}^{n} a_i$.

$A_{n+1} = \sum_{i=1}^{n} \lambda a_i + \lambda a_{n+1} - \lambda(\sum_{i=1}^{n} a_i + a_{n+1}) = A_n$.
Donc (A_n) est une suite constante, égale à $A_0 = \lambda a_0 - \lambda a_0 = 0$.

Donc pour tout $n \in \mathbb{N}$, $\sum_{i=1}^{n} \lambda a_i = \lambda \sum_{i=1}^{n} a_i$.

De même :
D'après la commutativité de la multiplication :

$$\prod_{i=1}^{n} a_i b_i = (a_1 b_1) \times (a_2 b_2) \cdots (a_n b_n) = (a_1 a_2 \cdots a_n) \times (b_1 b_2 \cdots b_n) = \prod_{i=1}^{n} a_i \times \prod_{i=1}^{n} b_i$$

En conséquence du cas précédent ($b_i = \lambda$, pour tout $i \in \mathbb{N}_n$) $\prod_{i=1}^{n} \lambda a_i = (\lambda a_1 \times \lambda a_2 \cdots \times \lambda a_n) =$

$$\lambda^n (a_1 a_2 \cdots a_n) = \lambda^n \prod_{i=1}^{n} a_i$$

□

Remarque - le $n+1$ de λ^{n+1} dans le dernier produit
… est donc en fait le cardinal de I, ensemble sur lequel on fait le produit.

Sommation par paquets

Exercice
Si A et B sont deux ensembles disjoints de E, montrer que pour tout $i \in E$, $\mathbb{1}_{A\cup B}(i) - \mathbb{1}_A(i) - \mathbb{1}_B(i) = 0$.
En déduire que $\sum_{i\in A\cup B} a_i = \sum_{i\in A} a_i + \sum_{i\in B} a_i$.

Correction
Comme A et B sont disjoints, ou bien $i \in A$ et $i \notin B$, ou bien $i \notin A$ et $i \in B$ ou bien $i \notin A$ et $i \notin B$. Pour chacun de ces trois cas, on a respectivement :

$$\mathbb{1}_{A\cup B} - \mathbb{1}_A - \mathbb{1}_B = \begin{cases} 1-1-0=0 \\ 1-0-1=0 \\ 0-0-0=0 \end{cases}$$

Dans tous les cas : $\mathbb{1}_{A\cup B} = \mathbb{1}_A + \mathbb{1}_B$.
Puis, on multiplie par a_i et on additionne :

$$\sum_{i\in A\cup B} a_i = \sum_i a_i \mathbb{1}_{A\cup B}(i) = \sum_i a_i \mathbb{1}_A(i) + \sum_i a_i \mathbb{1}_B(i) = \sum_{i\in A} a_i + \sum_{i\in B} a_i$$

Généralisons ce résultat. Il faut commencer par définir une notation :

Définition - Réunion disjointe
On note $C = A \uplus B$, par signifier la double information :
— $C = A \cup B$
— $A \cap B = \emptyset$
Autrement écrit : $x \in C$ si et seulement si $x \in A$ ou (exclusif) $x \in B$.
On peut généraliser cette notation à plusieurs ensembles :
$C = \biguplus_{i=1}^{n} A_i$ signifie : $x \in C$ si et seulement si $\exists\, !\, i \in \mathbb{N}_n$ tel que $x \in A_i$.

On a alors la relation de Chasles pour les sommes :

Pour aller plus loin - Autre notation
On trouve parfois également la notation : $C = A \sqcup B$ ou encore $C = A \biguplus B$.
Ce + est là pour pourvoir signifier un résultat que l'on verra plus loin, si $C = \biguplus_{i=1}^{n} A_i$, alors $card(C) = \sum_{i=1}^{n} card(A_i)$.

Proposition - Sommation par paquets
Soit une famille $(E_r)_{r\in S}$ une famille d'ensembles indexés par S.
On suppose qu'il s'agit d'une famille d'ensembles disjoints 2 à 2 :
$\forall\, r \neq r' \in S,\ E_r \cap E_{r'} = \emptyset$.
Alors

$$\sum_{r\in S}\left(\sum_{k\in E_r} a_k\right) = \sum_{k\in \biguplus_{r\in S} E_r} a_k$$

On voit ici apparaître une double somme. On en reparlera plus loin.

Démonstration
On a là encore : $E = \biguplus_{r\in S} E_r$ et donc

$$\begin{array}{rcl} k \in E & \iff & \exists\, !\, r \in S \text{ tel que } k \in E_r \\ \mathbb{1}_E(k) = 1 & \iff & \exists\, r \in S \text{ tel que } \mathbb{1}_{E_r}(k) = 1 \text{ et } \forall\, s \in S \setminus \{r\}, \mathbb{1}_{E_s}(k) = 0 \\ & \iff & \sum_{r\in S} \mathbb{1}_{E_r}(k) = 1 \end{array}$$

Donc, ceci étant vrai pour tout k, on a l'égalité de fonctions

$$\mathbb{1}_E = \sum_{r\in S} \mathbb{1}_{E_r}$$

Alors, comme précédemment :

$$\begin{aligned} \sum_{k\in E} a_k &= \sum_k a_k \mathbb{1}_E(k) = \sum_k a_k \left(\sum_{r\in S} \mathbb{1}_{E_r}(k)\right) \\ &= \sum_k \sum_{r\in S} a_k \mathbb{1}_{E_r}(k) = \sum_{r\in S} \sum_k a_k \mathbb{1}_{E_r}(k) \\ &= \sum_{r\in S} \sum_{k\in E_r} a_k \end{aligned}$$

□

Remarque - Interversion des symboles Σ
Dans la démonstration, on a inversé deux symboles Σ. Cela sera justifié par la suite, car il s'agit d'une **somme finie**.
C'est comme si on sommait les termes dans un tableau : d'abord en ligne, puis en colonne ; ou d'abord en colonne, puis en ligne. Dans tous les cas, on obtient le même résultat car il s'agit d'additionner une et une seule fois tous les termes du tableau.

Savoir faire - Exploiter une sommation par paquets
On a parfois intérêt à découper l'ensemble E en (réunion de m) sous-ensembles disjoints $E = E_1 \uplus E_2 \cdots \uplus E_m$.
On calcule alors la somme par paquets :

$$\sum_{r=1}^{m}\left(\sum_{k\in E_r} a_k\right) = \sum_{k\in E} a_k$$

Télescopage

C'est la seule méthode ui donne une formule explicite.

Savoir faire - Méthode du télescopage (ou dominos)

Soit (u_n) une suite. Soient $p, n \in \mathbb{N}$ tels que $p \leqslant n$

Alors $\sum_{k=p}^{n} (u_{k+1} - u_k) = u_{n+1} - u_p$

$\left(= (u_{p+1} - u_p) + (u_{p+2} - u_{p+1}) + (u_{p+3} - u_{p+2}) + \cdots + (u_{n+1} - u_n)\right)$

Remarque - « Voir » le téléscopage

Deux remarques :

- Dans la plupart des situations, la somme ne se présente pas directement sous la forme $\sum_{k=p}^{n} (u_{k+1} - u_k)$, il faut commencer par faire "apparaître" cette forme.
- On peut aussi avoir intérêt à écrire la somme avec des points de suspension pour confirmer le télescopage aperçu

Exercice

Calculer $\sum_{k=1}^{n} \ln \frac{k+1}{k}$.

Correction

$\sum_{k=1}^{n} \ln \frac{k+1}{k} = \sum_{k=1}^{n} [\ln(k+1) - \ln(\mathbb{k})] = \ln(n+1) - \ln(1) = \ln(n+1)$

2.3. Avec Python

Il arrive souvent que l'on rencontre des calculs de sommes à effectuer sous Python. La méthode est simple, on emploie des boucles :

- `for`, si l'on connait bien l'ensemble sur lequel est definie i
- `while`, si i est définie par une propriété

Informatique - $\sum_{k=n}^{m} a(k)$

```
def Somme1(n,m):
    S=0
    for k in range(n,m+1):
        S=S+a(k)
    return(S)
```

Informatique - $\sum_{i \mid f(i) \leqslant n} a(i)$

```
def Somme2(n):
    S,i=0,0
    while f(i)<=n:
        S=S+a(i)
        i=i+1
    return(S)
```

Remarque - L'ordinateur (calculatrice) comme un obstacle?

L'une des principales raisons de la faiblesse des élèves pour le calcul est l'usage trop tôt de la calculatrice.
Il faut laisser le temps pour comprendre, maitriser, puis ne pas oublier le sens du calcul avant de passer à la calculatrice.
Néanmoins, il ne faut pas systématiquement tout jeter!

Pour aller plus loin - Théorème fondamentale de l'analyse entière?

Intégrer↔ Dériver sont les deux problèmes inverses l'un de l'autre. Ils sont définis pour des fonctions de la variable réelle.
Pour la variable entière, les fonctions sont des suites. Et intégrer consiste simplement à faire le calcul $\sum_{k=0}^{n} a_k$.
Alors à quoi correspond la dérivation de la variable entière? Au calcul $a_{n+1} - a_n$! (c'est pas exemple comme cela qu'on voit si une suite est croissante...).
La formule du télescopage présente ce lien : $\sum \leftrightarrow \delta$

Truc & Astuce pour le calcul - Écrire un programme pour mieux comprendre

Ecrire un programme permet souvent de mieux comprendre la nature du calcul.
C'est le cas en particulier :

- pour le calcul de somme.
- pour le calcul de probabilités.
  Dans ce cas, ce n'est pas le calcul mais la modélisation elle-même du problème qui est mieux comprise.

Exercice

Ecrire une boucle (double ?) pour faire le calcul :

$$\sum_{i=1}^{100} \sum_{j=i}^{200-i} i \times j$$

Correction

```
S=0
for i in range (101):
   for j in range(i,200-i+1):
      S=S+i*j
return(S)
```

Remarque - Varier les paramètres et informatique

L'informatique permet aussi de facilement faire varier les paramètres. On a vu la force de l'usage des paramètres dans le calcul. Mais c'est aussi, de manière générale, la force de l'excellent mathématicien. Python nous aidera largement : ce n'est que légèrement une boite noire pour nous, nous aurons donc pour ambition de bien maîtriser tous nos faits et gestes informatiques (pas de clicothérapie!).

2.4. Des sommes connues

Proposition - Sommes de puissances d'entiers consécutifs

Soit $n \in \mathbb{N}^*$. Alors :

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}; \quad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}; \quad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

On peut faire une récurrence, ou bien chercher à démontrer le résultat directement. Une méthode classique : user le télescopage.

Démonstration

Nous démontrons le second résultat en admettant le premier.
Notons d'abord que pour tout entier k : $(k+1)^3 - k^3 = 3k^2 + 3k + 1$.
Donc, en voyant un téléscopage :

$$(n+1)^3 - 1 = \sum_{k=1}^{n} [(k+1)^3 - k^3] = \sum_{k=1}^{n} [3k^2 + 3k + 1] = 3\sum_{k=1}^{n} k^2 + 3\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1$$

Ainsi (toujours d'abord factoriser!) :

$$3\sum_{k=1}^{n} k^2 = (n+1)^3 - 1 - \frac{3n(n+1)}{2} - n = \frac{(n+1)}{2}[2(n+1)^2 - 2 - 3n] = \frac{(n+1)(2n^2+n)}{2} = \frac{n(n+1)(2n+1)}{2}$$

□

Exercice

Démontrer par récurrence les résultats précédents

Correction

Posons pour tout $n \in \mathbb{N}^*$, $\mathscr{P}_n$:« $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$ ».

- $\sum_{k=1}^{1} k^3 = 1$ et $\left(\frac{1(1+1)}{2}\right)^2 = 1$

— Soit $n \in \mathbb{N}$ et supposons $\mathscr{P}_n$ vérifiée.

$$\sum_{k=1}^{n+1} k^3 = \sum_{k=1}^{n} k^3 + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3$$
$$(n+1)^2\left[\tfrac{1}{4}(n^2+4n+4)\right] = \frac{(n+1)^2(n+2)^2}{4}$$

Donc $\mathscr{P}_{n+1}$ est vraie.

Savoir faire - Se passer du formalisme d'une récurrence ou invariant de boucle

On peut souvent se passer de la formalisation de la récurrence (mais avec les mêmes calculs).

Ici on considère la suite $u_n = \sum_{k=1}^{n} k^3 - \left(\frac{n(n+1)}{2}\right)^2$.

On note que $u_{n+1} = u_n$ (même calcul que $\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1}$) et que $u_1 = 0$.
Donc pour tout $n \in \mathbb{N}^*$, $u_n = 0$. CQFD.

Proposition - Calcul d'une somme arithmétique

Pour une suite arithmétique :

$$\forall\, n \in \mathbb{N}, u_{n+1} = u_n + r$$

on a :

$$\sum_{k=n}^{m} u_k = (m-n+1) \times \frac{u_m + u_n}{2}$$

C'est-à-dire :

somme de termes succ. = (nb de termes) × (moyenne des termes extrêmes)

Démonstration

Pour tout k, $u_k = u_n + (k-n)r$.

$$\sum_{k=n}^{m} u_k = \sum_{k=n}^{m} u_n + r\sum_{k=n}^{m}(k-n) = (m-n+1)u_n + r\sum_{i=0}^{m-n} i$$

$$= (m-n+1)u_n + r\frac{1}{2}(m-n)(m-n+1) = \frac{m-n+1}{2}(u_n + r(m-n) + u_n) = (m-n+1) \times \frac{u_m+u_n}{2}$$

□

Exercice

Démontrer le résultat en suivant la « méthode de Gauss » (double somme inversée…)

Correction

On note S, la somme en question : $2S = S + S = \sum_{k=n}^{m} u_k + \sum_{k=n}^{m} u_k$. Dans la première somme on note $h = k$ et dans la seconde on fait le changement d'indice $h = m - k + n$:

$$2S = \sum_{h=n}^{m} u_h + \sum_{h=n}^{m} u_{m+n-h} = \sum_{h=n}^{m} (u_n + (h-n)r + u_n + (m+n-h-n)r)$$
$$= \sum_{h=n}^{m} (u_n + u_n + (m-n)r) = \sum_{h=n}^{m} (u_n + u_m) = (m-n+1)(u_n+u_m)$$

Proposition - Calcul d'une somme géométrique

Soit $x \in \mathbb{R}$ (ou $x \in \mathbb{C}$) et $n \in \mathbb{N}$. On a alors :

$$\sum_{k=0}^{n} x^k = \begin{cases} n+1 & \text{si } x = 1 \\ \dfrac{1-x^{n+1}}{1-x} & \text{si } x \neq 1 \end{cases}$$

Plus généralement pour une suite géométrique de raison $q \neq 1$, on a :

$$\text{somme de termes successifs} = \text{1er terme} \times \frac{1-q^{\text{nb de termes}}}{1-q}$$

Démonstration

Si $x = 1$, $\sum_{k=0}^{n} x^k = \sum_{k=0}^{n} 1 = n+1$

Si $x \neq 1$, $(1-x)\sum_{k=0}^{n} nx^k = \sum_{k=0}^{n}(x^k - x^{k+1}) = x^0 - x^{n+1}$, télescopage. □

Exercice

Calculer $1+2+4+8+16+32+64+128$

Correction

C'est la somme de 8 termes consécutifs d'une suite géométrique de raison 2.

Donc $1+2+4+8+16+32+64+128 = 1 \times \frac{1-2^8}{1-2} = 2^8 - 1 = 255$.

Quel lien avec l'écriture en binaire des nombres entiers sur 8 octets ?

On se rappelle, avec les petits Bernoulli :

Proposition - Une factorisation à connaître

Soient a et b deux réels (ou deux complexes), alors :

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$$

Application - $3^n - 2^n$, sous forme d'une addition de n termes

$3^n - 2^n = (3-2)(3^{n-1} + 2\ldots 3^{n-2} + 4\ldots 3^{n-3} + \cdots + 2^{n-2}\ldots 3 + 2^{n-1})$.

Application - Factoriser $a^5 - b^5$

Vu au chapitre précédent.

$a^5 - b^5 = (a-b)(a^4 + a^3b + a^2b^2 + ab^3 + b^4)$

Démonstration

On développe et utilisons la méthode du téléscopage :

$$(a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k = \sum_{k=0}^{n-1} a^{n-k}b^k - \sum_{k=0}^{n-1} a^{n-(k+1)}b^{k+1} = a^n b^0 + \sum_{i=1}^{n-1} a^{n-i}b^i - \sum_{j=1}^{n-1} a^{n-j}b^j - a^0 b^n = a^n - b^n$$

Puis en prenant $a = 1$, $1 - x^{n+1} = (1-x)\sum_{k=0}^{n} x^k \ldots$ □

Exercice

Peut-on factoriser $a^n + b^n$? Si oui, factoriser le.

Correction

Si $b = -a$, $a^n + b^n = a^n(1 + (-1)^n) = 0$ si n est impair.

On peut factoriser par $a+b$ dans ce cas :

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 + \cdots + (-1)^k a^{n-1-k}b^k + \cdots + b^{n-1})$$

car $n-1$ est alors pair

2.5. Sommes doubles (multiples…)

Heuristique - Somme à multiples indices

On peut faire une somme d'éléments pris dans un ensemble fini. Mais la description de ces éléments n'est pas toujours naturellement données sous la forme $x_i, i \in [\![0,n]\!]$.
Parfois les éléments apparaissent comme les éléments d'un tableau (*matrice*) et sont donc doublement (ou plus) indexés : $x_{i,j}, i \in \mathbb{N}_n, j \in \mathbb{N}_m$.
Les choses se présentent différemment selon que i et j sont « indépendants » entre eux ou non.

Cas i et j indépendants. Produit cartésien d'ensembles

Analyse - Du sens des formules
Comment décrire avec des symboles ∑ la somme suivante :

$$S = a_{1,1} + a_{1,2} + \cdots + a_{1,m} + a_{2,1} + \cdots + a_{2,m} + \cdots + a_{n,1} + \cdots + a_{n,m}$$

On peut voir cette somme de la façon suivante :

$$S = \left(a_{1,1} + a_{1,2} + \cdots + a_{1,m}\right) + \left(a_{2,1} + \cdots + a_{2,m}\right) + \cdots + \left(a_{n,1} + \cdots + a_{n,m}\right)$$

On y voit n sommes, chacune composée d'une somme de m termes :

$$S = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_{i,j}\right)$$

Evidemment, la somme étant finie, l'addition commutative, on a également :

$$S = a_{1,1} + a_{2,1} + \cdots + a_{n,1} + a_{1,2} + \cdots + a_{n,2} + \cdots + a_{1,m} + \cdots + a_{n,m} = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{i,j}\right)$$

Et finalement on peut écrire :

$$S = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_{i,j}\right) = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{i,j}\right) = \sum_{(i,j)\in\mathbb{N}_n\times\mathbb{N}_m} a_{i,j}$$

Définition - Somme double
On considère une famille de nombres réels ou complexes $(a_{i,j})$ indexée par deux indices i et j, i compris entre 1 et n, j compris entre 1 et m où n et m sont deux entiers non nuls donnés. On peut représenter ces nombres par un tableau où l'indice i désigne la ligne et l'indice j la colonne :

$$\begin{array}{ccccccc} a_{1,1} & \cdots & a_{1,j} & \cdots & \cdots & a_{1,m} \\ \vdots & & \vdots & & & \vdots \\ a_{i,1} & \cdots & a_{i,j} & \cdots & \cdots & a_{i,m} \\ \vdots & & \vdots & & & \vdots \\ a_{n,1} & \cdots & a_{n,j} & \cdots & \cdots & a_{n,m} \end{array}$$

La somme de tous les éléments de ce tableau est notée

$$\sum_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m} a_{i,j} = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]} a_{i,j}.$$

Savoir faire - Somme multiple (indépendance)
Pour la calculer on peut procéder d'au moins deux façons, la première consiste à faire d'abord la somme des termes ligne par ligne, puis d'additionner les résultats :

$$\sum_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m} a_{i,j} = \sum_{i=1}^{n} \underbrace{\left(\sum_{j=1}^{m} a_{i,j}\right)}_{\text{somme de la ligne } i} = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j},$$

une seconde étant de sommer d'abord les termes colonne par colonne puis d'additionner les résultats :

$$\sum_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m} a_{i,j} = \sum_{j=1}^{m} \underbrace{\left(\sum_{i=1}^{n} a_{i,j}\right)}_{\text{somme de la colonne } j} = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{i,j}.$$

Remarque - Diagonale
Il y a d'autres possibilités, par exemple en sommant suivant des lignes diagonales lorsque $n = m$.
On reverra cela plus loin.

Exercice
Calculer $\sum_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p} ij$

Correction
$S = \sum_{i=1}^{n}\left(\sum_{j=1}^{p} ij\right) = \sum_{i=1}^{n} i\left(\sum_{j=1}^{p} j\right) = \sum_{i=1}^{n} i\frac{p(p+1)}{2} = \frac{n(n+1)p(p+1)}{4}$
Comme le montre l'exercice précédent :

Proposition - Produit de deux sommes (développement ou factorisation)
Soient des réels (ou des complexes) a_i et b_j, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant p$. Alors :

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{p} b_j\right) = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_i b_j$$

Démonstration
C'est assez simple, par développement :

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{p} b_j\right) = \left(\sum_{i=1}^{n} a_i\left(\sum_{j=1}^{p} b_j\right)\right) = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_i b_j$$

□

Cas i et j dépendants

Heuristique - Cas : i et j dépendants
Ici on somme seulement certains termes du tableau rectangulaire $a_{i,j}$.
Et donc les indices sont dépendants l'un de l'autre!
Par exemple, dans cette situation, les valeurs prises par j (à l'intérieur de la somme) dépendent de celles prises par i (à l'extérieur de la somme). Il y a, en revanche, souvent liberté dans le choix de l'ordre de sommation (d'abord i ou d'abord j).

Analyse - $G = \{a_{i,j}, i \in \mathbb{N}_n, j \in A_i\}$
On suppose que G est décrit parfaitement ainsi : $\{a_{i,j}, i \in A, j \in A_i\}$.
Donc

$$\sum_{a\in G} a = \sum_{i,j} a_{i,j}\mathbb{1}_G(a_{i,j}) = \sum_{i\in A}\left(\sum_{j\in A_i} a_{i,j}\right)$$

Evidemment, la somme $\sum_{j\in A_i}\left(\sum_{i\in A} a_{i,j}\right)$ ne signifie rien (A_i ne peut exister car i n'existe pas) et donc les choses ne commutent pas facilement ici.

Proposition - Somme double classique $\sum_{1\leqslant j\leqslant i\leqslant n} a_{i,j}$
Soit $(a_{i,j})_{(i,j)\in\mathbb{N}^2}$ une famillle de nombres réels ou complexes :

$$\sum_{1\leqslant j\leqslant i\leqslant n} a_{i,j} = \sum_{i=1}^{n}\sum_{j=1}^{i} a_{i,j} = \sum_{j=1}^{n}\sum_{i=j}^{n} a_{i,j}.$$

Démonstration
On a les calculs suivants :

$$\begin{aligned}\sum_{1\leqslant j\leqslant i\leqslant n} a_{i,j} &= \sum_{i,j} a_{i,j}[1\leqslant j\leqslant i\leqslant n] = \sum_i \left(\sum_j a_{i,j}[1\leqslant j\leqslant i][1\leqslant i\leqslant n]\right)\\ &= \sum_i \left(\sum_j a_{i,j}[1\leqslant j\leqslant i]\right)[1\leqslant i\leqslant n] = \sum_{i=1}^{n}\left(\sum_{j=1}^{i} a_{i,j}\right)\\ &= \sum_j \left(\sum_i a_{i,j}[j\leqslant i\leqslant n][1\leqslant j\leqslant n]\right) = \sum_{j=1}^{n}\left(\sum_{i=j}^{i} a_{i,j}\right)\end{aligned}$$

□

Exercice
Calculer $\sum_{1\leqslant i\leqslant j\leqslant n} ij$

Correction
$$S=\sum_{j=1}^{n} j\left(\sum_{i=1}^{j} i\right)=\sum_{j=1}^{n}\frac{j^2(j+1)}{2}=\frac{1}{2}\left(\frac{n^2(n+1)^2}{4}+\frac{n(n+1)(2n+1)}{6}\right)$$
$$=\frac{n(n+1)(3n^2+7n+2)}{24}=\frac{n(n+1)(3n+1)(n+2)}{24}$$

Pour aller plus loin - Formalisme/sens
*On notera ici (mais c'est souvent le cas en mathématiques) que le formalisme est plus **efficace** que la recherche de sens : il permet une sorte d'automat(h)isation.*
Néanmoins, il est bon de toujours accompagné l'un par l'autre.

Savoir faire - Somme multiple (dépendance)
Pour la calculer on ordonne les indices de sommation :

1. on choisit celle qui sera le plus à l'extérieur (donc à gauche) des symboles ∑. Elle ne dépend que de paramètres fixés et d'aucun indice.
2. on choisit ensuite la suivante, la seconde dans l'ordre des sommes. Elle dépend des paramètres fixés et de l'indice précédent

…

Exemple : $\sum_{1\leqslant i<j\leqslant n} a_{i,j}=\sum_{i=1}^{n-1}\left(\sum_{j=i+1}^{n} a_{i,j}\right)=\sum_{j=2}^{n}\left(\sum_{i=1}^{j-1} a_{i,j}\right)$

Analyse - Sens de ces modes de sommations
On somme seulement certains termes du tableau (et pas tous).
Si E désigne l'ensemble des indices (i,j) des nombres que l'on désire sommer, on notera $\sum_{(i,j)\in E} a_{i,j}$ cette somme.
Pour le cas présent $E=\{(i,j)\in\mathbb{N}^2 | 1\leqslant j\leqslant i\leqslant n\}$ (termes sous ou sur la diagonale principale du tableau carré à n lignes et n colonnes), on a alors

$$\sum_{1\leqslant j\leqslant i\leqslant n} a_{i,j}=\sum_{i=1}^{n}\sum_{j=1}^{i} a_{i,j}=\sum_{j=1}^{n}\sum_{i=j}^{n} a_{i,j}.$$

Il est recommandé de comprendre les tableau suivants :
Première sommation :

$$\underbrace{\sum_{i=1}^{n}}_{\downarrow 2}\underbrace{\sum_{j=1}^{i}}_{\rightarrow 1} a_{i,j}:\quad \begin{array}{ccccc} a_{1,1} & & & & \\ \downarrow 2 & \searrow & & & \\ a_{h,1} & \rightarrow 1 & a_{h,h} & & \\ \downarrow 2 & & \downarrow 2 & \searrow & \\ a_{n,1} & \rightarrow 1 & a_{n,h} & \rightarrow 1 & a_{n,n}\end{array}$$

Deuxième sommation :

$$\underbrace{\sum_{j=1}^{n}}_{\rightarrow 2}\underbrace{\sum_{i=j}^{n}}_{\downarrow 1} a_{i,j}:\quad \begin{array}{ccccc} a_{1,1} & & & & \\ \downarrow 1 & \searrow & & & \\ a_{h,1} & \rightarrow 2 & a_{h,h} & & \\ \downarrow 1 & & \downarrow 1 & \searrow & \\ a_{n,1} & \rightarrow 2 & a_{n,h} & \rightarrow 2 & a_{n,n}\end{array}$$

2.6. Exercice d'applications

Exercice
Retrouver la valeur de $S=\sum_{k=1}^{n} k$, en notant que $S=\sum_{k=1}^{n}\sum_{i=1}^{k} 1$

Correction
$S=\sum_{k=1}^{n} k=\sum_{k=1}^{n}\sum_{i=1}^{k} 1=\sum_{i=1}^{n}\sum_{k=i}^{n} 1=\sum_{i=1}^{n}(n-i+1)=\sum_{i=1}^{n}(n+1)-\sum_{i=1}^{n} i.$
Donc $2S=n(n+1)$ et donc $S=\frac{n(n+1)}{2}$.

Exercice
Montrer que $\left(\sum_{k=1}^{n} d_k\right)^2=\sum_{k=1}^{n} d_k^2+2\sum_{1\leqslant i<j\leqslant n} d_i d_j$.

Correction
$\left(\sum_{k=1}^{n} d_k\right)^2=\left(\sum_{k=1}^{n} d_k\right)\times\left(\sum_{k=1}^{n} d_k\right)^2=\sum_{(k,h)\in\mathbb{N}_n^2} d_k d_h.$
Or $\mathbb{N}_n^2=\{(k,k),k\in\mathbb{N}_n\}\uplus\{(k,h),k<h\in\mathbb{N}_n\}\uplus\{(k,h),k>h\in\mathbb{N}_n\}$.
On peut aussi exploiter la notation d'Iverson $\mathbb{N}^2=\{(k,h)\mid[k=h]\}\uplus\{(k,h)\mid[k<h]\}\uplus\{(k,h)\mid[k>h]\}$.
Par sommation par paquets :
$\left(\sum_{k=1}^{n} d_k\right)^2=\sum_{k=1}^{n} d_k^2+\sum_{1\leqslant k<h\leqslant n} d_k d_h+\sum_{1\leqslant k>h\leqslant n} d_k d_h=\sum_{k=1}^{n} d_k^2+2\sum_{1\leqslant k<h\leqslant n} d_k d_h,$
en faisant $k\leftrightarrow h$ dans la dernière somme.
On peut aussi démontrer l'inégalité célèbre de Cauchy-Schwarz :
Exercice

1. En développant $\sum_{1\leqslant i<j\leqslant 3}(a_i b_j-a_j b_i)^2$, montrer que $\left(\sum_{k=1}^{3} a_k b_k\right)^2\leqslant\left(\sum_{k=1}^{3} a_k^2\right)\left(\sum_{k=1}^{3} b_k^2\right)$.
2. De même, montrer l'inégalité de Cauchy-Schwarz :
$$\left(\sum_{k=1}^{n} a_k b_k\right)^2\leqslant\left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right)$$
3. A quelle condition a-t-on : $\sum_{k=1}^{n}(a_i b_i)^2=\left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right)$

Correction

1. On a
$$\begin{aligned}0\leqslant &\sum_{1\leqslant i<j\leqslant 3}(a_i b_j-a_j b_i)^2=(a_1b_2-a_2b_1)^2+(a_1b_3-a_3b_1)^2+(a_2b_3-a_3b_2)^2\\ 0\leqslant &(a_1b_2)^2+(a_1b_3)^2+(a_2b_1)^2+(a_2b_3)^2+(a_3b_1)^2+(a_3b_2)^2\\ &-2(a_1a_2b_1b_2)-2(a_1a_3b_1b_3)-2(a_2a_3b_2b_3)\\ 0\leqslant &\sum_{i\neq j}(a_i b_j)^2+\sum_i(a_i b_i)^2-\sum_i(a_i b_i)^2-2\sum_{i<j}(a_i a_j b_i b_j)\\ 0\leqslant &\sum_{i,j}a_i^2b_j^2-\sum_{i,j}(a_i b_i a_j b_j)=\sum_{\mathbb{k}}a_k^2\sum_{\mathbb{k}}b_k^2-\left(\sum_{\mathbb{k}}(a_k b_k)\right)^2\end{aligned}$$
Donc $\left(\sum_{k=1}^{3} a_k b_k\right)^2\leqslant\left(\sum_{k=1}^{3} a_k^2\right)\left(\sum_{k=1}^{3} b_k^2\right)$.
2. De même en remplaçant 3 par n :
$$\begin{aligned}0\leqslant &\sum_{1\leqslant i<j\leqslant n}(a_i b_j-a_j b_i)^2\\ 0\leqslant &\sum_{i=1}^{n}\sum_{j\neq i}a_i^2b_j^2+\sum_{i=1}^{n}(a_i b_i)^2-\sum_{i=1}^{n}(a_i b_i)^2-\sum_{i<j}(a_i a_j b_i b_j)-\sum_{i<j}(a_j a_i b_j b_i)\\ 0\leqslant &\sum_{k=1}^{n}a_k^2\sum_{k=1}^{n}b_k^2-\left(\sum_{k=1}^{n}(a_k b_k)\right)^2\end{aligned}$$
Donc $\left(\sum_{k=1}^{n} a_k b_k\right)^2\leqslant\left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right)$

3. Il y a égalité, si et seulement si (il faut bien être attentif à chaque signe !) (si $b_n \neq 0$) :

$$\forall\, i<j,\qquad a_i b_j - a_j b_i = 0 \Longleftrightarrow \forall\, i \leqslant n a_i = \frac{a_n}{b_n} b_i$$

Exercice

Ecrire le développement polynomiale de

$$\prod_{i=1}^{n}(x-a_i)$$

Correction

Il s'agit d'une fonction polynomiale. Plus largement (en notant $|I|$, le cardinal de I) :

$$\prod_{i=1}^{n}(x_i-a_i) = \sum_{I\subset\mathbb{N}_n}\left(\prod_{i\in I} x_i \times \prod_{j\in\mathbb{N}_n\setminus I}(-a_j)\right)$$

$$\prod_{i=1}^{n}(x-a_i) = \sum_{I\subset\mathbb{N}_n}\left(\prod_{i\in I} x \times \prod_{j\in\mathbb{N}_n\setminus I}(-a_j)\right) = \sum_{I\subset\mathbb{N}_n}\left(x^{|I|}\times(-1)^{n-|I|}\prod_{j\in\mathbb{N}_n\setminus I} a_j\right)$$

On range alors en fonction des valeurs du cardinal de I, afin de trouver des monômes de même degré.

Il s'agit d'une sommation par paquets $\{I\subset\mathbb{N}_n\} = \bigsqcup_{k=0}^{n}\{I\subset\mathbb{N}_n, |I|=k\}$:

$$\prod_{i=1}^{n}(x-a_i) = \sum_{k=0}^{n}\left[\sum_{\substack{I\subset\mathbb{N}_n\\|I|=k}}\left(x^{|I|}\times(-1)^{n-|I|}\prod_{j\in\mathbb{N}_n\setminus I} a_j\right)\right] = \sum_{k=0}^{n}(-1)^{n-k}x^k\left(\sum_{\substack{I\subset\mathbb{N}_n\\|I|=k}}\prod_{j\in J} a_j\right)$$

Cela peut s'écrire aussi :

$$\prod_{i=1}^{n}(x-a_i) = \sum_{k=0}^{n}(-1)^{n-k}x^k\left(\sum_{\substack{J\subset\mathbb{N}_n\\|J|=n-k}}\prod_{j\in J} a_j\right)$$

3. Coefficients binomiaux et formule du binôme

3.1. Factorielles et coefficients binomiaux

Définitions

Les remarques en marge permettent de s'intéresser aux nombres :

Définition - Factorielle et coefficient binomial

Pour n et p éléments de $\mathbb{N}$, $p\leqslant n$, on pose :

$0! = 1$ et pour $n\geqslant 1$, $n! = n\times(n-1)\times\cdots\times 1$ qui se lit "factorielle n"

$\binom{n}{p} = \frac{n(n-1)\ldots(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}$ qui se lit « p parmi n »

On généralise la notation à tout $p\in\mathbb{Z}$: si $p<0$ ou $p>n$ (si on n'a pas $0\leqslant p\leqslant n$), alors $\binom{n}{p}=0$.

Remarque - Plus tard...

• Il n'est pas évident que pour $p\leqslant n$, $\binom{n}{p}$ est un nombre entier.
Si tel est le cas (on le verra plus loin) cela signifie que $p!$ divise tout nombre de la forme $n(n-1)\ldots(n-p+1)\ldots$.

• Nos reprendrons la notion de coefficient binomial lorsque nous ferons du dénombrement. Cela expliquera véritablement l'origine de ce calcul.

Informatique - Calcul de la factorielle avec une boucle

```
def factorielle(n):
    f=1
    for k in range(1,n):
        f=f*(k+1)
    return(f)
```

Pour aller plus loin - Coefficients binomiaux réels

On sent qu'on pourrait s'intéresser plutôt au nombres

$$\binom{x}{p} = \frac{x(x-1)\ldots(x-p+1)}{p!}$$

avec $x\in\mathbb{C}$ et $p\in\mathbb{N}$.
Dans ce cas, la méthode du triangle de Pascal doit s'adapter, alors que la formule du binôme de Newton reste vraie!

Propriétés immédiates

Proposition - Propriétés

Pour tout nombres entiers $n\in\mathbb{N}$ (naturels) et $p\in\mathbb{Z}$ (relatifs) :

$$\binom{n}{0}=\binom{n}{n}=1;\quad \binom{n}{1}=n;\quad \binom{n}{2}=\frac{n(n-1)}{2};$$

$$\binom{n}{p}=\binom{n}{n-p}$$

$$\binom{n}{p}=\frac{n}{p}\binom{n-1}{p-1}\text{ (fausse pour } p=0\text{ !)}$$

$$\binom{n}{p}=\binom{n-1}{p-1}+\binom{n-1}{p}\text{ (Relation de Pascal)}$$

Histoire - Blaise Pascal



Blaise PASCAL (1623-1662) est un français, génie des mathématiques (mais pas uniquement). Il redémontre tout Euclide, seul à 12 ans. Il fonde la géométrie projective (avec Desargues) et la « géométrie du hasard » avec Fermat.
Mais c'est aussi l'inventeur de la brouette, de la première machine à calculer ou du premier transport en commun parisien...
Il présente le triangle de Pascal dans le traité du triangle arithmétique (mais ce n'est pas lui le premier à le découvrir).

Démonstration

Les premiers résultats sont immédiats (simple jeu d'écriture).
Le second est assez simple, mais il faut différencier : $p\in[\![0,n]\!]$ ou $p<0\Longleftrightarrow n-p>n$ ou $p>n\Longleftrightarrow n-p>0$.
Démontrons les deux derniers. Si $1\leqslant p\leqslant n$,

$$\binom{n}{p}=\frac{n!}{p!(n-p)!}=\frac{n(n-1)!}{p(p-1)!((n-1)-(p-1))!}=\frac{n}{p}\binom{n-1}{p-1}$$

si $p<0$, alors $\binom{n}{p}=0$ et $\binom{n-1}{p-1}=0$; si $p>n$, alors $\binom{n}{p}=0$ et $\binom{n-1}{p-1}=0$.
Plus intéressant, si $1\leqslant p\leqslant n-1$,

$$\binom{n-1}{p-1}+\binom{n-1}{p}=\frac{(n-1)!}{(p-1)!(n-p)!}+\frac{(n-1)!}{p!(n-1-p)!}=\frac{(n-1)![p+(n-p)]}{p!(n-p)!}=\binom{n}{p}$$

Si $p=n$: $\binom{n-1}{p-1}+\binom{n-1}{p}=1+0=1=\binom{n}{n}$.
Si $p>n$: $\binom{n-1}{p-1}+\binom{n-1}{p}=0+0=0=\binom{n}{n}$.
De même si $p<0$. □

Exercice

Pour n,p, simplifier $\sum_{k=p}^{n}\binom{k}{p}$. *On pourra y « voir » un télescopage*

Correction

$$\sum_{k=p}^{n}\binom{k}{p}=\binom{p}{p}+\sum_{k=p+1}^{n}\left(\binom{k+1}{p+1}-\binom{\mathbb{k}}{p+1}\right)=1+\binom{n+1}{p+1}-\binom{p+1}{p+1}=\binom{n+1}{p+1}$$

3.2. Triangle de Pascal

De ces propriétés on déduit un moyen simple de calculer les coefficients binomiaux :

Savoir faire - Triangle de Pascal

On peut alors construire le triangle de Pascal pour pouvoir calculer facilement (addition et non multiplication) les coefficients binomiaux. On écrit ainsi dans un tableau :

$$
\begin{array}{ccccccccccc}
\binom{0}{0} & & & & & & & & 1 & & \\
\binom{1}{0} & \binom{1}{1} & & & & & & & 1 & 1 & \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & & & & & 1 & 2^{=1+1} & 1 \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & & & \longrightarrow & & 1 & 3 & 3 & 1 \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & & & & 1 & 4 & 6^{=3+3} & 4 & 1 \\
\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} & & & 1 & 5 & 10 & 10 & 5 & 1 \\
\vdots & & & \vdots & & & & & \vdots & & & & \vdots &
\end{array}
$$

On l'a déjà dit :

Proposition - Nombres entiers

Pour n et p éléments de $\mathbb{N}$, $p \leqslant n$, $n!$ et $\binom{n}{p}$ sont des entiers naturels.

Démonstration
Pour la factorielle : il s'agit d'un produit d'entiers naturels.
Pour le coefficient binomial, on réalise une récurrence sur le niveau n.
On pose, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$: « $\forall\ p \in \mathbb{Z}$, $\binom{n}{p} \in \mathbb{N}$.

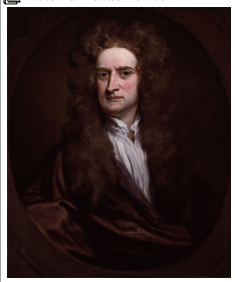
- $\mathscr{P}_0$ est vraie car $\binom{0}{0} = 1$ et pour tout $p \neq 0$, $\binom{n}{p} = 0$.
- Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}_n$ est vraie.
  Soit $p \in \mathbb{Z}$, alors $\binom{n+1}{p} = \binom{n}{p} + \binom{n}{p-1}$, addition de deux entiers d'après $\mathscr{P}_n$.
  Donc $\mathscr{P}_{n+1}$ est vraie.

□

Informatique - Triangle de Pascal
En exploitant des listes (de listes) en informatique, il est possible de créer la n^e ligne du triangle de Pascal.

```
def Pascal(n):
    L=[0]*(n+1)
    for h in range(n+1):
        L[h]=[1]+[0]*n
    print(L)
    for h in range(n):
        for k in range(h+1):
            L[h+1][k+1]=L[h][k]+L[h][k+1]
    return(L)
```

Histoire - Isaac Newton



On attribue couramment à Isaac NEWTON *(1642-1707) la révolution scientifique de la science moderne, grâce à son travail mathématique sur les calculs différentiel et intégral et son travail en mécanique (relation fondamentale de la dynamique, loi des forces…).*
La formule du binôme qui apparait ici est en fait du à Pascal (1654), et généralisée une première fois par Newton (avec son travail d'interpolation polynomiale - 1671) puis par Abel avec tout exposant $n \in \mathbb{R}$ au début du XIX siècle.

3.3. Formule du binôme

Proposition - Formule du binôme (de Newton)
Soient $n \in \mathbb{N}$ et a, b deux réels ou deux complexes (ou éléments de tout anneau et tels que $a \times b = b \times a$). Alors :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Avec $a = b = 1$:

Corollaire -

$$\sum_{p=0}^{n} \binom{n}{p} = 2^n$$

Démonstration
Démontrons ce résultat par récurrence.
Notons, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$: « $(a+b)^n = \sum_{k=0}^{n} \binom{n}{\mathbb{K}} a^{\mathbb{K}} b^{n-k}$ ».

- $(a+b)^0 = 1$ et $\sum_{k=0}^{0} \binom{n}{\mathbb{K}} a^{\mathbb{K}} b^{n-k} = \binom{0}{0} a^0 b^0 = 1$.
  donc $\mathscr{P}_0$ est vraie.
- Soit $n \in \mathbb{N}$, supposons que $\mathscr{P}_n$ est vraie.
  On a alors

$$(a+b)^{n+1} = (a+b) \times \sum_{k=0}^{n} \binom{n}{\mathbb{K}} a^{\mathbb{K}} b^{n-k} = \binom{n}{n} a^{n+1} + \underbrace{\sum_{k=0}^{n-1} \binom{n}{\mathbb{K}} a^{k+1} b^{n-k}}_{h=k+1} + \underbrace{\sum_{k=1}^{n} \binom{n}{\mathbb{K}} a^{\mathbb{K}} b^{n-k+1}}_{h=k} + \binom{n}{0} b^{n+1}$$

$$= a^{n+1} + \sum_{h=1}^{n} \left(\binom{n}{h-1} + \binom{n}{h} \right) a^h b^{n+1-h} + b^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{\mathbb{K}} a^{\mathbb{K}} b^{n+1-k}$$

  d'après la formule de Pascal et comme $\binom{n+1}{n+1} = 1 = \binom{n+1}{0}$.
  Donc $\mathscr{P}_{n+1}$ est alors vérifiée.

On a ainsi démontré par récurrence le résultat attendu. □

Pour aller plus loin - De qui parle-t-on?
« Il est de bonne famille et il a reçu une excellente éducation. Prodigieusement doué pour les mathématiques, à vingt et un ans il publiait une étude sur le binôme de Newton, qui fit sensation dans toute l'Europe et lui valut de devenir titulaire de la chaire de mathématiques dans une de nos petites universités. Tout donnait à penser qu'il allait faire une carrière extrêmement brillante. Mais l'homme avait une hérédité chargée, qui faisait de lui une sorte de monstre, avec des instincts criminels d'autant plus redoutables qu'ils étaient servis par une intelligence exceptionnelle. Des bruits fâcheux coururent bientôt sur lui dans l'Université, qui l'obligèrent à se démettre. Il vint à Londres où il se mit à donner des cours destinés aux officiers de l'armée. »

Exercice

Calculer $\sum_{0 \leqslant p \leqslant n ; p \text{ pair}} \binom{n}{p}$ et $\sum_{0 \leqslant p \leqslant n ; p \text{ impair}} \binom{n}{p}$.

Correction

Notons P_n et I_n ces deux sommes. On a vu que $P_n + I_n = \sum_{k=0}^{n} \binom{n}{\mathbb{K}} = 2^n$.

Puis, $I_n = \sum_{0 \leqslant p \leqslant n ; p \text{impair}} \binom{n}{p} = \sum_{0 \leqslant p \leqslant n ; p \text{impair}} \binom{n-1}{p} + \sum_{0 \leqslant p \leqslant n ; p \text{impair}} \binom{n-1}{p-1} = I_{n-1} + P_{n-1} = 2^{n-1}$.
Et ainsi $P_n = 2^n - I_n = 2^n - 2^{n-1} = 2^{n-1}(2-1) = 2^{n-1} = I_n$

4. Bilan

Synthèse

- En mathématique, la sélection (naturelle) opère également et un langage se crée. Des définitions et concepts sont sélectionnés, comme des mots de la langue ; et le formalisme comme l'écriture de ce langage.
  Le formalisme doit être compact (souvent), ressemblant à sa notion attachée (rarement) et efficace calculatoirement (absolument). C'est le cas de la notation $\sum$ (ou $\prod$) qu'on utilise comme un « auto-mathisme » avec un peu d'habitude : changement de variable, sommation par paquets, télescopage, somme multiple…
- Pour bien comprendre cette utilisation, on se rend compte que l'enjeu est de maîtriser la manipulation de l'ensemble des indices. Cette notion d'ensemble est au coeur des mathématiques, nous reviendrons dessus aux chapitres 9 et 10. (Il faut aussi que l'ensemble des nombres soit commutatif).
- Le nombres de sous-ensemble à k éléments à partir d'un ensemble à n élément est également un calcul qui se présente dans de très nombreuses branches des mathématiques. Il est formalisé par le coefficient binomial et une expression de langage : « k parmi n ».
- De nombreuses propriétés (issues de domaines variés) peuvent lui être attachés : triangle de Pascal, binôme de Newton, nombre de chemins dans des arbres binaires fusionnés, inversion de Pascal…

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Changement d'indice
- Savoir-faire - Sommation par paquets
- Savoir-faire - Méthode de téléscopage
- Truc & Astuce pour le calcul - Ecrire un programme pour mieux comprendre
- Truc & Astuce pour le calcul - Invariant de boucle
- Savoir-faire - Somme multiple (indépendance)
- Savoir-faire - Somme multiple (dépendance)
- Savoir-faire - Triangle de Pascal

Notations

	Propriétés	*Remarques*
Iverson pour la propriété $\mathscr{P}$	$\forall\ i,\ [\mathscr{P}(i)] \in \{0,1\}$ avec $[\mathscr{P}(i)] = 1$ ssi $\mathscr{P}(i)$ vraie	
le n (lire dans ce sens !)	$n! = \prod_{k=1}^{n} k$	$0! = 1$ et par récurrence $n! = n \times (n-1)!$
binomial de k parmi n	$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{(n-k+1)_k}{k!}$ (si n n'est pas entier)	C'est le nombre de sous-ensemble à k éléments pris dans un ensemble E à n éléments.
	$(1+x)^r = \sum_{k=0}^{+\infty} \binom{k}{r} x^k$ (même si $r \notin \mathbb{N}\ldots$)	

Retour sur les problèmes

33. Nombres triangulaires. $T_n = \frac{n(n+1)}{2} = \binom{n+1}{2}$.
    Si on note T_n^k, telle que $T_n^k = \sum_{h=1}^{n} T_h^{k-1}$ et $T_n^0 = n$.
    On trouve alors par récurrence : $T_n^k = \binom{n+k}{k+1}$.
34. Développement.
    A calculer... Il n'y a pas de résultats intéressants, sauf en petite taille ou en expression formelle.
35. Suite de nombres. Et le suivant ?
    Une stratégie : apprendre des évolutions sur les premiers nombres, donc calculer la suite $\delta(u)_n = u_{n+1} - u_n$. Pour en déduire $u_m = u_{m-1} + \delta(u)_{m-1}$.
    Si ce n'est pas suffisant, évaluer (par récurrence) : $\delta^k(u)_n = \delta^{k-1}(u)_{n+1} - \delta^{k-1}(u)_n \ldots$
36. Interpolation à pas constant. Voir activités
37. Développement de puissance.
    C'est le coefficient multinomial de Newton : $(a_1 + a_2 + \cdots + a_k)^n = \sum_{m_1+m_2+\cdots+m_k=m} \frac{n!}{m_1!m_2!\ldots m_k!} \prod_{i=1}^{k} a_i^{m_i}$.
    Vous comprenez ?

Chapitre 8

Résolution de systèmes linéaires.

Résumé -

Il n'est pas rare également d'avoir à résoudre des équations algébriques sous forme de systèmes d'équations linéaires.
Le but de ce (tout petit) chapitre est de mettre en place les définitions efficaces, les méthodes (algorithmes) de résolution adéquates (ce que n'est pas la substitution…) et de voir apparaître par le calcul bien mené, la structure sous-jacente.
On voit ici l'exemple typique du calcul linéaire, ou matriciel et la structure clé d'espaces vectoriels.

Enfin, voici une liste de petites vidéo ou conférence visionnable sur internet et en lien avec le sujet. A visionner à loisir :
- *Exo7Math - Systèmes linéaires - partie 1 : introduction. https ://www.youtube.com/watch ?v=0uYJ3RNL5SU*
- *Mathéma-TIC - Règle de Cramer. https ://www.youtube.com/watch ?v=CNzVk1evqac*

Sommaire

1. Quelques problèmes 158
2. Systèmes linéaires. Equivalence 158
2.1. Vocabulaire 159
2.2. Systèmes équivalents 159
3. Résolution explicite. cas des petits systèmes $n = p = 2$ ou $n = p = 3$ 160
3.1. Vers la formule de Cramer 160
4. Algorithme su pivot de GAUSS 162
4.1. Systèmes équivalents : opérations élémentaires . . . 162
4.2. Algorithme du pivot de GAUSS 162
4.3. Applications. Différents formes de l'ensemble des solutions 163
5. Bilan 164

1. Quelques problèmes

Problème 38 - Résolution d'un système linéaire

Il n'est pas rare que l'on rencontre en SI ou en physique (ou en mathématiques) un système d'équation de la forme suivante à résoudre :

$$\begin{cases} 2x + 3y - 4z = 1 \\ x - 3y + z = -1 \\ x + y - z = 1 \end{cases}$$

Est-il possible de trouver la/les solution(s) en (x,y,z) de ce système directement ?
On peut croire et anticiper que ces solutions s'expriment sous la forme d'un calcul différent (mais équivalent, d'une certaine façon) pour x, y et z, à partir des nombres $2;3;-4;1\ldots$
Comment expliciter ce calcul ?

Problème 39 - Résolution « au petit bonheur »

Lorsque le système est gros (plus de quatre équations), les méthodes aléatoires de résolution ne fonctionnent pas bien.
Il faut s'organiser. Qu'avons-nous le droit de faire ? Existe-t-il une méthode, un algorithme (programmable informatiquement, par exemple) qui donne à coup sûr l'ensemble des solutions d'un système d'équations linéaires ?

Problème 40 - Forme de l'ensemble des solutions

Dans la pratique, lorsqu'on rencontre un système de 3 équations à 3 inconnues, on trouve une unique solution.
Est-ce toujours vrai ? Sinon, qu'est-ce qui fait que cela peut être faux ?
Et, plus généralement, s'il y a n équations et p inconnues, combien y a-t-il de solutions ?

Problème 41 - Impact des paramètres

Il arrive aussi en science appliquée (et en mathématiques (en interne) également) que l'on trouve un système à paramètre. Par exemple :

$$\begin{cases} ax + 3y - 4z = 1 \\ (a-1)x - 3y + z = -1 \\ x + y - z = 1 \end{cases}$$

Dans ce cas là, à quoi ressemble l'ensemble des solutions ?

2. Systèmes linéaires. Equivalence

Dans cette partie, même si nous énonçons des résultats (sous forme de définitions et propositions à apprendre), nous ne faisons pas (encore) de démonstration comme annoncé au cours inaugural.

2.1. Vocabulaire

Remarque - Le formalisme de LEIBNIZ
On commence par **paramétrer notre problème** : on l'élargit en donnant une écriture symbolique (paramétre lettré) aux nombres. Puis on élargit la problème : pourquoi seulement trois équations et trois inconnues ?
Pour permettre l'étude systématique des systèmes linéaires, on a besoin d'une suite de nombre doublement indexé les $(a_{i,j})$. C'est Leibniz qui en a eu l'idée (1678). Et comme souvent, à partir du moment où le formalisme et les définitions associées sont bons, les théorèmes tombent comme des fruits mûrs…

Définition - Système linéaire de n équations à p inconnues
Un **système linéaire** à n équations et p inconnues à coefficient dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ est un système S d'équations de la forme :

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,p}x_p &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,p}x_p &= b_2 \\ \vdots & \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,p}x_p &= b_n \end{cases}$$

où
— les $a_{i,j} \in \mathbb{K}$;
— $(b_1, b_2, \dots b_n) \in \mathbb{K}^n$ est appelé le second membre de l'équation ;
— $(x_1, x_2 \dots x_p) \in \mathbb{K}^p$ est appelé l'inconnue du système.
On appelle **système homogène** le système obtenu en remplaçant chaque b_i par 0 (second membre nul).

On appelle **solution** du système S, l'ensemble $\mathscr{S} \subset \mathbb{R}^p$ des p-uplets $(\overline{x}_1, \overline{x}_2, \dots \overline{x}_p)$ qui vérifient les n équations :
$\forall\, i \in \mathbb{N}_n,\ a_{i,1}\overline{x}_1 + a_{i,2}\overline{x}_2 + \cdots + a_{i,p}\overline{x}_p = b_i$

Histoire - Mathématiques des neuf livres
Le plus vieux traité mathématique proposant l'étude de système d'équations linéaires est le Chiu chang suan shu, que l'on appelle les mathématiques des neufs livres, écrit en 160 av. JC. Bien que de nature différentes (moins géométrique et plus algorithmique), ce livre est au mathématiques chinoise, ce que les éléments d'Euclide sont aux mathématiques européennes.

Remarque - Notations
On a pour habitude de noter S les systèmes et de manière plus stylisé l'ensemble des solutions $\mathscr{S}$.
On associe parfois des indices.

Remarque - Solution(s) du système homogène
Un système linéaire homogène admet toujours au moins la solution nulle : $\mathscr{S}_0 = (x_1, x_2 \dots x_p) = (0, 0 \dots, 0) = O_p$

Heuristique - Résolution
Il y a en gros deux méthodes pour résoudre un tel système.
La méthode de Leibniz (fin du XVII) fonctionne très bien pour les petites dimensions $n, p \leqslant 3$ et la formule de Cramer que l'on donnera ensuite. Elle marche bien également *en théorie* pour les grandes dimensions.
La méthode (dite) de Gauss est algorithmique, nous la privilégierons pour les plus grandes dimensions.

2.2. Systèmes équivalents

Analyse - Sens des flèches $\Rightarrow$, $\Leftarrow$
« Naturellement », lorsqu'on écrit $S_1 \Rightarrow S_2$, cela signifie qu'on peut passer du système S_1 au système S_2.
Ainsi, tous les éléments qui vérifient les équations de S_1 vérifient aussi celles de S_2.
En terme d'ensemble solution : toutes les solutions de S_1 sont soolutions de S_2.
Donc $\mathscr{S}_1 \subset \mathscr{S}_2$.
On peut donc résumer : $S_1 \Rightarrow S_2$ si et seulement si $\mathscr{S}_1 \subset \mathscr{S}_2$.

Définition - Systèmes équivalents
Deux systèmes S_1 et S_2 sont dits équivalents, relation notée

$$S_1 \iff S_2$$

si et seulement si les ensembles de solutions sont les mêmes : $\mathscr{S}_1 = \mathscr{S}_2$.

Exercice
Les systèmes $S_1 : \begin{cases} 2x+y=1 \\ -x-y=0 \end{cases}$ et $S_2 : \begin{cases} 2x+y=1 \end{cases}$ sont-ils équivalents ?

Correction
Non.
Le couple $(0,1) \in \mathscr{S}_2$, c'est une solution du second système d'équations mais pas du premier car $0-1 \neq 0$

Attention - Pas d'abus
Typiquement ici, il ne faut pas abuser du symbole d'équivalence !
Dans l'exercice, on écrit donc jamais :

$$S_1 : \begin{cases} 2x+y=1 \\ -x-y=0 \end{cases} \iff 2x+y=1$$

Il n'y a ici qu'une implication.

3. Résolution explicite. cas des petits systèmes $n = p = 2$ ou $n = p = 3$

3.1. Vers la formule de Cramer

Etude formelle du système simple $n = p = 2$

Comme Leibniz, commençons par étudier le système

$$S : \begin{cases} ax + by &= \alpha \\ cx + dy &= \beta \end{cases}$$

où a, b, c, d et α, β sont des paramètres, alors que x, y sont les inconnues.

Analyse - Etude « à la lycéenne »
On substitue (évidemment : **si** $a \neq 0$) :

$$S \Longrightarrow x = \frac{\alpha - by}{a}$$

Donc (on a définitivement perdu l'équivalence) (**si** $ad - bc \neq 0$) :

$$S \Longrightarrow \frac{c\alpha - cby}{a} + dy = \beta \Longrightarrow \frac{ad-bc}{a}y = \frac{a\beta - c\alpha}{a} \Longrightarrow y = \frac{a\beta - c\alpha}{ad-bc}$$

On trouve alors en réinjectant : $S \Longrightarrow x = \dfrac{\alpha(ad-bc) - b(a\beta - c\alpha)}{a(ad-bc)} = \dfrac{\alpha d - \beta b}{ad-bc}$.

Remarque - Avons-nous trouver les solutions ?
Non !!
Ici, on a $\mathscr{S} \subset \left\{\left(\dfrac{\alpha d - \beta b}{ad-bc}, \dfrac{-\alpha c + \beta a}{ad-bc}\right)\right\}$.
Mais peut-être que $\mathscr{S}$ est l'ensemble vide !
Il faut donc faire une réciproque. Sinon, il y a une faute (courante) de logique.

Analyse - Réciproque
Toujours dans le cas $ad - bc$, on vérifie que

$$\begin{aligned} a\frac{\alpha d - \beta b}{ad-bc} + b\frac{-\alpha c + \beta a}{ad-bc} &= \alpha \frac{ad-bc}{ad-bc} = \alpha \\ c\frac{\alpha d - \beta b}{ad-bc} + d\frac{-\alpha c + \beta a}{ad-bc} &= \beta \frac{ad-bc}{ad-bc} = \beta \end{aligned}$$

Donc la réciproque est vérifiée. On a bien l'égalité : $\mathscr{S} = \left\{\left(\frac{\alpha d - \beta b}{ad - bc}, \frac{-\alpha c + \beta a}{ad - bc}\right)\right\}$.

Remarque - $a \neq 0$?
Dans l'analyse, il a fallut faire séparer le cas $a \neq 0$.
Mais le résultat obtenu ne dépend pas de $a = 0$ ou $a \neq 0$. Donc on aurait sûrement pu s'en passer.
D'ailleurs, la réciproque montre que ce n'est pas un cas important.
Seule la situation $ad - bc \neq 0$ ou $ad - bc = 0$ est importante!

Définition - Déterminant d'un système 2×2
On appelle **déterminant du système** 2×2 (i.e. $n = 2$ et $p = 2$)

$$S \quad \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 &= b_2 \end{cases}$$

le nombre $\delta_S = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$ souvent noté $\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix}$.

Cas d'un système 3×3

Leibniz propose d'étendre sa méthode pour $n > 2$.

Définition - Déterminant d'un système 3×3
On appelle **déterminant du système** 3×3 (i.e. $n = 3$ et $p = 3$)

$$S \quad \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + a_{2,3}x_3 &= b_2 \\ a_{3,1}x_1 + a_{3,2}x_2 + a_{3,3}x_3 &= b_3 \end{cases}$$

le nombre $\delta_S = a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} - a_{3,1}a_{2,2}a_{1,3} - a_{1,1}a_{3,2}a_{2,3}$ souvent noté $\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}$.

Pour aller plus loin - Extension de taille n
Lorsque l'on souhaite généraliser la notion de déterminant, on comprend qu'il faut prendre une combinaison linéaire des termes constitués exactement de nombre tous pris dans des lignes et des colonnes différentes.
Mais il y a une règle de signe à respecter. Il n'est pas clair que Leibniz ait bien compris cette règle.
Cramer, 50 ans plus tard l'a retrouvé (sans avoir connaissance des travaux de Leibniz).
Un mathématicien japonais Seki Kowa *(1642-1708) a effleuré toute cette découverte.*

Formule de Cramer

Nous verrons dans le cours sur les déterminants, au second semestre, une petite notice sur Gabriel Cramer (1704-1752)

Savoir faire - Formule de Cramer
Si le déterminant du système S (n=p=2) est non nul, la solution de $\mathscr{S}$ de

$$(S) \quad \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 &= b_2 \end{cases}$$

est $\mathscr{S} = \{(\overline{x}_1, \overline{x}_2)\} = \left\{\left(\frac{\begin{vmatrix} b_1 & a_{1,2} \\ b_2 & a_{2,2} \end{vmatrix}}{\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix}}, \frac{\begin{vmatrix} a_{1,1} & b_1 \\ a_{2,1} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix}}\right)\right\}$.
Si le déterminant du système S (n=p=3) est non nul, la solution de $\mathscr{S}$ de

$$(S) \quad \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + a_{2,3}x_3 &= b_2 \\ a_{3,1}x_1 + a_{3,2}x_2 + a_{3,3}x_3 &= b_3 \end{cases}$$

Pour aller plus loin - Sytème de taille $n \times n$
Dans le calcul du déterminant qui donne x_i, on remplace la i-ème colonne par la colonne du second membre.
La formule de Cramer se généralise à tout système carré, avec une bonne définition du déterminant généralisée.

est $\mathscr{S} = \{(\overline{x}_1, \overline{x}_2, \overline{x}_3)\} = \left\{\left(\frac{\begin{vmatrix} b_1 & a_{1,2} & a_{1,3} \\ b_2 & a_{2,2} & a_{2,3} \\ b_3 & a_{3,2} & a_{3,3} \end{vmatrix}}{\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}}, \frac{\begin{vmatrix} a_{1,1} & b_1 & a_{1,3} \\ a_{2,1} & b_2 & a_{2,3} \\ a_{3,1} & b_3 & a_{3,3} \end{vmatrix}}{\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}}, \frac{\begin{vmatrix} a_{1,1} & a_{1,2} & b_1 \\ a_{2,1} & a_{2,2} & b_2 \\ a_{3,1} & a_{3,2} & b_3 \end{vmatrix}}{\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix}}\right)\right\}$

4. Algorithme su pivot de Gauss

Heuristique - Il y a une bonne méthode et une mauvaise méthode...
La **mauvaise méthode** est la SUBSTITUTION.
On perd des équations et cela est **plus long**.
La **bonne méthode** consiste à faire des OPERATIONS ELEMENTAIRES.
Il faut les connaître, mais ce n'est pas sufffisant.
Il faut aussi savoir **bien** les mener. C'est la partie difficile de l'algorithme.

4.1. Systèmes équivalents : opérations élémentaires

On commence par trouver des invariants de l'ensemble des solutions. Cela permet de raisonner avec des systèmes équivalents

Définition - Opérations élémentaires
On appelle **opérations élémentaires** sur le système dont la ligne i est noté L_i, les opérations suivantes :
— pour tout $i, j \leqslant n$, échange des lignes L_i et L_j codé : $L_i \leftrightarrow L_j$
— pour tout $i \leqslant n$, $\lambda \neq 0$, la multiplication de la ligne L_i par λ codé : $L_i \leftarrow \lambda L_i$
— pour tout $i, j \leqslant n$, $\alpha \in \mathbb{K}$, l'ajout à la ligne L_i de α fois la ligne L_j codé : $L_i \leftarrow L_i + \alpha L_j$

Proposition - Invariant des solutions
Les opérations élémentaires conservent exactement les solutions du système

Démonstration
Il est évident que chaque opération conduit à une implication $\Rightarrow$ sur les systèmes.
Et par ailleurs, pour chacune de ces opérations, il est possible de « revenir en arrière ».
Pour cela, il suffit de voir que
1. l'opération $L_i \leftrightarrow L_j$ répétée deux fois redonne le système initiale.
2. l'opération $L_i \leftarrow \frac{1}{\lambda}L_i$ ($\lambda \neq 0$), après l'opération $L_i \leftarrow \lambda L_i$, redonne le système initiale.
3. l'opération $L_i \leftarrow L_i - \alpha L_j$, après l'opération $L_i \leftarrow L_i + \alpha L_j$, redonne le système initiale.

On trouve donc $\mathscr{S} \Rightarrow \mathscr{S}' \Rightarrow \mathscr{S}$.
Cela signifie bien : $\mathscr{S} \Longleftrightarrow \mathscr{S}'$. □

4.2. Algorithme du pivot de Gauss

Il reste à bien exploiter ces opérations élémentaires afin de **toujours** trouver la solution d'un système linéaire.

Histoire - Algorithme de Fang-Cheng
On ne prête qu'au riche : en occident, nous associons l'algorithme ici étudié (central en mathématiques de l'algèbre linéaire) au grand Carl-Freidrich Gauss, mais il semble qu'il soit bien connu et expliqué dans les mathématiques des neuf livres (première impression en 1084, 5 siècle avant Gutemberg...).
L'auteur de cet ouvrage est un certain Chang Ts'ang, *et sa méthode s'appelle le modèle rectangulaire écrit Fang-Cheng.*

Savoir faire - Algorithme du pivot de Gauss
Pour résoudre un système linéaire, on applique des opérations élémentaires pour le rendre triangulaire.
1. On cherche un coefficient non nul dans la première colonne (devant la première inconnue) le plus simple possible (on va devoir

diviser par ce nombre).
Si tous les coefficients sont nuls, on passe à l'inconnue suivante.

2. On échange la ligne où l'on a trouvé ce coefficient avec la ligne 1.
3. Pour $j \in [\![2,n]\!]$, on effectue l'opération $L_j \leftrightarrow L_j - \frac{a_{1,j}}{a_{1,1}} L_1$ (ce qui permet d'annuler le coefficient devant x_1 pour la ligne j puis pour toute la colonne.
4. On recommence la première étape, en oubliant la première équation et en s'intéressant à l'inconnue suivante, tant qu'il reste des inconnues.

Après avoir appliqué cet algorithme, le système obtenu est triangulaire, et l'on peut déterminer ses solutions en partant de la dernière équation et en remontant à la première (sans substitution : cela demande un « mouvement » supplémentaire…).
Il peut arriver que l'on retrouve en dernière équation plus d'une inconnue. Dans ce cas, on garde une seule inconnue, les autres deviennent des variables libres que l'on considère alors en second membre.

4.3. Applications. Différents formes de l'ensemble des solutions

Application - Trois systèmes à résoudre : $S_1 : \left\{ \begin{array}{rrrl} x & -y & +z & =1 \\ -x & -y & +z & =3 \\ 2x & +y & +z & =0 \end{array} \right.$,

$S_2 : \left\{ \begin{array}{rrrl} x & +y & +2z & =1 \\ 2x & -y & +z & =-1 \\ x & -2y & -z & =-2 \end{array} \right.$ **et** $S_3 : \left\{ \begin{array}{rrrl} x & +y & +2z & =1 \\ 2x & -y & +z & =-1 \\ x & -2y & -z & =2 \end{array} \right.$

On applique la méthode du pivot de Gauss, on trouve :

$$S_1 \Leftrightarrow \left\{ \begin{array}{rrrl} \underline{x} & -y & +z & =1 \\ & -2y & +2z & =4 \\ & 3y & -z & =-2 \end{array} \right| \begin{array}{l} \\ L_2 \leftarrow L_2 + L_1 \\ L_3 \leftarrow L_3 - 2L_1 \end{array}$$

$$\Leftrightarrow \left\{ \begin{array}{rrrl} x & -y & +z & =1 \\ & \underline{-2y} & +2z & =4 \\ & & 2z & =4 \end{array} \right| \begin{array}{l} \\ \\ L_3 \leftarrow L_3 + \frac{3}{2} L_2 \end{array} \Leftrightarrow \left\{ \begin{array}{rl} x & =-1 \\ y & =0 \\ z & =2 \end{array} \right.$$

Donc $\mathscr{S}_1 = \{(-1,0,2)\}$
Pour le second système

$$S_2 \Leftrightarrow \left\{ \begin{array}{rrrl} \underline{x} & +y & +2z & =1 \\ & -3y & -3z & =-3 \\ & -3y & -3z & =-3 \end{array} \right| \begin{array}{l} \\ L_2 \leftarrow L_2 - 2L_1 \\ L_3 \leftarrow L_3 - L_1 \end{array}$$

$$\Leftrightarrow \left\{ \begin{array}{rrl} x & +y & =1-2z \\ & y & =3-z \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rl} x & =-2-z \\ y & =3-z \end{array} \right.$$

Donc $\mathscr{S}_2 = \{(-2-z, 3-z, z), z \in \mathbb{R}\}$ que l'on prend l'habitude de noter : $\{(-2,3,0) + z(-1,-1,1), z \in \mathbb{R}\}$.
Pour le troisième système

$$S_3 \Leftrightarrow \left\{ \begin{array}{rrrl} \underline{x} & +y & +2z & =1 \\ & -3y & -3z & =-3 \\ & -3y & -3z & =1 \end{array} \right| \begin{array}{l} \\ L_2 \leftarrow L_2 - 2L_1 \\ L_3 \leftarrow L_3 - L_1 \end{array}$$

$$\Leftrightarrow \left\{ \begin{array}{rrrl} x & +y & 2z & =1 \\ & y & z & =3 \\ & & 0 & =4 \end{array} \right.$$

Donc $\mathscr{S}_3 = \emptyset$.

Remarque - Nombre de solution
Notons de cette application qu'un système carré (ici 3×3) peut avoir :

Pour aller plus loin - Début du second semestre
Ceci est le début historique de l'algèbre linéaire que nous verrons longuement en début de second semestre (avec la question des déterminants). N'anticipons pas trop pour le moment…

— aucune solution
— une unique solution
— une infinité de solution

Attention - Lorsqu'il y a infinité de solution…
il n'y a pas unicité d'écriture de cet ensemble

5. Bilan

Synthèse

- Pour la résolution d'un système linéaire il existe une méthode infaillible : l'algorithme du pivot de Gauss.
  Plus la taille du système est grande, plus il est nécessaire d'exploiter cette méthode.
- Pour des systèmes plus petits, on peut exploiter directement la formule de Cramer
- L'ensemble des solutions est soit un ensemble vide, soit l'addition d'une solution particulière et de l'ensemble (*espace vectoriel*) des solutions de l'équation homogène. L'écriture de cet ensemble n'est pas unique.
- Il faut être très attentif au symbole $\Longleftrightarrow$ parfois employé abusivement…

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Formule de CRAMER
— Savoir-faire - Algorithme du pivot de GAUSS

Notations

Notations	*Définitions*	*Propriétés*	*Remarq*
$S_1 \Longleftrightarrow S_2$	Les systèmes S_1 et S_2 ont les mêmes solutions	$\mathscr{S}_1 = \mathscr{S}_2$	On pass rations
$S_1 \Longrightarrow S_2$	Les solutions de S_1 sont des solutions de S_2	$\mathscr{S}_1 \subset \mathscr{S}_2$	On pass « non lé
$\delta_S = a_{1,1}a_{2,2} - a_{1,2}a_{2,1} = \left\vert \begin{array}{cc} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{array} \right\vert$	Déterminant du système S (de taille 2) ou de la matrice associée		On exp formule

Retour sur les problèmes

38. Résolution d'un système linéaire. $\mathscr{S} = \{(1,1,1)\}$.
39. Résolution « au petit bonheur ». Voir l'algorithme de Gauss.
40. Forme de l'ensemble des solutions.
    Il peut y avoir :
    — aucune solution (dans ce cas le système n'est pas homogène)
    — une solution de la forme $\mathscr{S} = \{(\overline{x}_1, \dots \overline{x}_p) + \sum_{k=1}^{r} \lambda_k \overrightarrow{u_k}\}$ où r est le rang du système, $(\overline{x}_1, \dots \overline{x}_p)$ est une solution particulière et pour tout k, $\overrightarrow{u_k}$ est un vecteur de $\mathbb{K}^p$, solution non nulle de l'équation homogène.
    (Ces vecteurs sont linéairement indépendants).
41. Impact des paramètres.
    — Si $a = 8$, alors $\mathscr{S} = \emptyset$,
    — Si $a \neq 8$, alors $\mathscr{S} = \left\{ \left(\frac{2}{8-a}, \frac{a-16}{a-8}, \frac{10}{8-a} \right) \right\}$

Chapitre 9

Calcul matriciel

Résumé -

Dans un premier temps nous (re)définissons les opérations matricielles : addition, multiplication par un nombre (ce qui donne un espace vectoriel) et multiplication (ce qui donne avec l'addition un anneau).
Puis nous nous concentrons sur les matrices carrées; elles jouent un rôle très important, puisque très fréquemment, on est amené à multiplier une matrice par elle-même (pour cela elle doit être carrée). C'est l'occasion de définir et de voir les propriétés des puissances de matrice, ainsi que de la trace.
On cherche également à inverser de telle matrice (si possible). Le meilleur moyen est d'utiliser un algorithme de Gauss (pivot de Gauss ou algorithme de Gauss-Jordan).

Sommaire

1. Problèmes 166
2. Esnsemble $\mathcal{M}_{n,p}(\mathbb{K})$ 167
2.1. Ensemble des matrices 167
2.2. Opérations (vectorielles) sur les matrices 168
2.3. Transposition 170
3. Multiplication matricielle 171
3.1. Définition 171
3.2. Interprétation en terme de systèmes linéaires 172
3.3. Propriété du produit 173
3.4. Produit par blocs 175
4. Les matrices carrées 176
4.1. L'anneau $(\mathcal{M}_n(\mathbb{K}),+,\times)$ 176
4.2. Puissance de matrices 176
4.3. Inversibilité d'une matrice 177
4.4. Quelques sous-ensembles remarquables 180
4.5. Trace d'une matrice carrée 181
5. Opérations élémentaires sur les matrices 182
5.1. Opérations élémentaires sur les lignes d'une matrices 182
5.2. Opérations élémentaires sur les colonnes d'une matrice 185
5.3. Méthode du pivot de Gauss pour obtenir l'inverse d'une matrice 185
6. Bilan 189

Dans tout le chapitre, m,n,p,q sont des entiers naturels non nuls et $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$ (on pourrait plus généralement considérer que $\mathbb{K}$ est un corps (commutatif)).

1. Problèmes

? Problème 42 - Pourquoi des matrices ?

Pour comprendre le monde qui nous entoure, on mesure des objets puis des dépendances entre ces objets.
Ces dépendances peuvent être multidimensionnelles, elles sont souvent enregistrées dans un tableau. C'est ce que l'on voit en particulier en économétrie, ou des domaines encore plus large : biologie, géographie…
Additionner des nombres a du sens lorsqu'on a des mesures de même unité d'objets de même nature. C'est seulement au XV-ième siècle que les additions se sont généralisées et se sont dégagées de leur signifiants.
Peut-on définir une addition des tableaux, qui ait du sens? Peut-on généraliser cette addition à tous tableaux?
Quelles sont les propriétés naturelles qui découlent : associativité, commutativité, élément neutre (Groupe)? Voire : espace vectoriel, avec une multiplication par un scalaire.

? Problème 43 - Pourquoi un tel produit ?

On peut addition des tableaux, peut-on les multiplier?
Donner une incarnation naturelle dans un problème physique qui justifie la règle de multiplication matricielle :

$$[AB]_{i,j}=\sum_{k=0}^{n}[A]_{i,k}[B]_{k,j}$$

? Problème 44 - Racines carrées

Puisque le produit de deux matrices existe, la puissance entière en découle : $A^2=A\times A$ et par récurrence : $A^n=A\times A^{n-1}$.
Peut-on définir des puissances entières négatives : A^{-4}?
Et plus largement des puissances non entières. Par exemple, la racine carrée de A serait une matrice B tel que $B^2=A$.
Concrètement, la matrice $A=\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}$ admet-elle une racine carrée? Plusieurs (combien?)?

? Problème 45 - Anneau non commutatif des matrices

L'anneau des matrices carrées de taille n : $(\mathcal{M}_n(\mathbb{K}),+,\times)$ est un exemple d'anneau non commutatif : $A\times B\neq B\times A$. Cela suggère quelques questions :

- Parmi les propriétés classiques d'anneaux, lesquelles ne sont plus vraies dans cet anneau?
- Et inversement, existe-t-il des matrices A tel que pour tout B : $A\times B=B\times A$
- Etant donnée A, existe-t-il une condition simple, nécessaire et/ou suffisante sur B pour que $A\times B=B\times A$?

— On sait que les éléments du groupe $\mathcal{M}_n(\mathbb{K})^\times := GL_n(\mathbb{K})$ sont les matrices inversibles et ne sont nécessairement pas des diviseurs de 0.

? Problème 46 - Matrices inversibles

Existe-t-il un moyen simple, algorithmique, pour étudier l'inversibilité d'une matrice? Peut-on l'exploiter pour obtenir également A^{-1} (dans le cas où A est inversible)?

2. Esnsemble $\mathcal{M}_{n,p}(\mathbb{K})$

Cet ensemble est considéré comme un espace vectoriel ici.

2.1. Ensemble des matrices

Définition - Matrices

Une matrice à n lignes et p colonnes à coefficients dans $\mathbb{K}$ est une famille $(a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ d'éléments de $\mathbb{K}$ indexée par $[\![1,n]\!]\times[\![1,p]\!]$. On parle aussi de matrice de type (n,p) ou de matrice $n\times p$. On note $\mathcal{M}_{n,p}(\mathbb{K})$ l'ensemble des matrices à n lignes et p colonnes à coefficients dans $\mathbb{K}$. Si $A\in\mathcal{M}_{n,p}(\mathbb{K})$,

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1p}\\ a_{21} & a_{22} & \cdots & a_{2p}\\ \vdots & \vdots & \vdots & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{np}\end{pmatrix}=(a_{ij})_{1\leqslant i\leqslant n;1\leqslant j\leqslant p}=(a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$$

a_{ij} est le coefficient de la i-ième ligne, j-ième colonne.
Deux matrices A et B sont donc égales si elles ont même nombre de lignes, même nombre de colonnes et mêmes coefficients.
Si $n=p$ on note $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées d'ordre n.

Exemple - Premier exemple

$$(i-j)_{\substack{1\leqslant i\leqslant 2\\1\leqslant j\leqslant 3}}=\begin{pmatrix}0 & -1 & -2\\ 1 & 0 & -1\end{pmatrix}$$

Définition - Quelques cas particuliers

Quelques matrices « de référence » sont à connaître :

— La matrice nulle de $\mathcal{M}_{n,p}(\mathbb{K})$ est la matrice qui ne contient que des coefficients nuls :

$$(0)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}=(0)=O_{n,p}$$

— si $n=1$, on dit que $A=\begin{pmatrix}a_1 & \dots & a_p\end{pmatrix}$ est une matrice ligne.

— si $p=1$, $B=\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}$ est appelée matrice colonne.

Parmi les matrices carrées d'ordre n, quelques matrices joueront un rôle particulier :

— La matrice identité de $\mathcal{M}_n(\mathbb{K})$ est la matrice I_n qui possède des 1 sur la diagonale et des 0 en dehors de la diagonale :

$$I_n=\begin{pmatrix}1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{pmatrix}=(a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}=(a_{ij})_{1\leqslant i,j\leqslant n}$$

où $a_{ij}=0$ si $i\neq j$ et $a_{ii}=1$ pour $i=1$ à n.

— une matrice diagonale est une matrice carrée dont seuls les éléments diagonaux sont non nuls :

$$\operatorname{diag}(a_{11},\dots,a_{nn})=\begin{pmatrix}a_{11} & 0 & \cdots & \cdots & 0\\ 0 & a_{22} & 0 & \cdots & 0\\ 0 & 0 & a_{33} & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & a_{nn}\end{pmatrix}\quad(i\neq j\Rightarrow a_{ij}=0)$$

Ainsi $I_n=\operatorname{diag}(\underbrace{1,1,\dots 1}_{n})$.

— une matrice scalaire est une matrice diagonale dont tous les éléments sont identiques :

$$\begin{pmatrix}\lambda & 0 & \cdots & \cdots & 0\\ 0 & \lambda & 0 & \cdots & 0\\ 0 & 0 & \lambda & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & \lambda\end{pmatrix}\quad(i\neq j\Rightarrow a_{ij}=0 \text{ et } a_{ii}=a_{jj}=\lambda)$$

— une matrice triangulaire supérieure est une matrice carrée dont les éléments au-dessous de la diagonale sont nuls :

$$\begin{pmatrix}a_{11} & a_{12} & a_{13} & \cdots & a_{1n}\\ 0 & a_{22} & a_{23} & \cdots & a_{2n}\\ 0 & 0 & a_{33} & \cdots & a_{3n}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & a_{nn}\end{pmatrix}\quad(i>j\Rightarrow a_{ij}=0);$$

— une matrice triangulaire inférieure est une matrice carrée dont les éléments au-dessus de la diagonale sont nuls.

$$\begin{pmatrix}a_{11} & 0 & \cdots & \cdots & 0\\ a_{21} & a_{22} & 0 & \cdots & 0\\ a_{31} & a_{32} & a_{33} & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn}\end{pmatrix}\quad(i<j\Rightarrow a_{ij}=0);$$

2.2. Opérations (vectorielles) sur les matrices

Addition

Définition - Addition de deux matrices de même taille

La somme de deux matrices $A=(a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ et $B=(b_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ de $\mathcal{M}_{n,p}(\mathbb{K})$

est la matrice définie par la formule suivante :

$$A+B=(a_{ij}+b_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}},$$

on ajoute les coefficients qui ont la même position.
Il s'agit d'une loi interne sur $\mathcal{M}_{n,p}(\mathbb{K})$.

Application - Exemple

$$\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}+\begin{pmatrix}2&3&4\\5&6&7\end{pmatrix}=\begin{pmatrix}3&5&7\\9&11&13\end{pmatrix}.$$

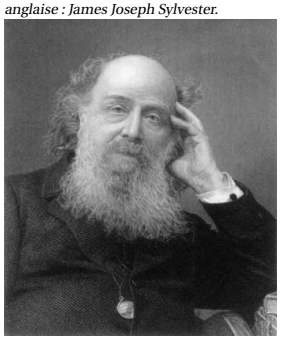
Analyse - Groupe $(\mathcal{M}_{n,p}(\mathbb{K}),+)$
On remarque que pour A, B, $C\in\mathcal{M}_{n,p}(\mathbb{K})$,

- $A+(0)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}=(0)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}+A=A$.
- $(A+B)+C=A+(B+C)$;
- $A+B=B+A$.
- $(a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}+(-a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}=(0)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$;

Le théorème suivant en découle :

Théorème - Le groupe $(\mathcal{M}_{n,p}(\mathbb{K}),+)$
L'ensemble $\mathcal{M}_{n,p}(\mathbb{K})$ muni de l'addition + est donc un groupe commutatif, d'élément neutre la matrice nulle de $\mathcal{M}_{n,p}(\mathbb{K})$.

Histoire - Le terme de matrice
Le terme de matrice pour désigner les tableaux rectangulaires considérées ici fut introduit en 1850 par le mathématicien américain d'origine anglaise : James Joseph Sylvester.



James Joseph Sylvester est né 1814 et mourut en 1897. Son origine juive l'obligea à aller enseigner en Amérique.

Multiplication par un scalaire

Définition - Multiplication par un scalaire
Le produit d'une matrice A de $\mathcal{M}_{n,p}(\mathbb{K})$ par $\alpha\in\mathbb{K}$ est la matrice notée αA définie par :

$$\alpha(a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}=(\alpha a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}.$$

On définit ainsi une loi externe sur $\mathcal{M}_{n,p}(\mathbb{K})$ à domaine d'opérateur $\mathbb{K}$

Et on vérifie facilement les propriétés suivantes :

Proposition - Propriétés de la multiplication scalaire

- $1A=A$
- $\alpha(\beta A)=(\alpha\beta)A$
- $(\alpha+\beta)A=\alpha A+\beta A$,
- $\alpha(A+B)=\alpha A+\alpha B$.

Espace vectoriel de dimension finie

Analyse - Pour définir explicitement, sans quiproquo, une matrice, il faut…
$n\times p$ coefficients de $\mathbb{K}$ qu'il faut placer aux différentes positions de la matrice.
Il s'agit donc d'un espace vectoriel de dimension $n\times p$, et dont la base *canonique* est donnée par la référence de position.
Chaque élément de la base correspond à une position. Chaque élément de la base a donc un double indice : k et ℓ.

Théorème - L'espace vectoriel $(\mathcal{M}_{n,p}(\mathbb{K}),+,.)$
$(\mathcal{M}_{n,p}(\mathbb{K}),+,.)$ est un $\mathbb{K}$-e.v de dimension np.
La base canonique est formée par les $n\times p$ matrices $E_{k\ell}$ ($1\leqslant k\leqslant n; 1\leqslant\ell\leqslant p$) où $E_{k\ell}$ est la matrice ne contenant que des 0 sauf l'élément d'indices k,ℓ qui vaut 1, soit

$$E_{k\ell}=(\delta_{ki}\delta_{j\ell})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$$

On a donc $\dim_{\mathbb{K}}\mathcal{M}_{n,p}(\mathbb{K})=n\times p$.

Savoir faire - Notations
Par la suite, on notera ${}^{i}[A]_{j}$ ou $\mathrm{Coef}_{i,j}(A)$, le coefficient en ligne i et colonne j de la matrice A.
On a donc

$${}^{i}[\lambda A+\mu B]_{j}=\lambda\,{}^{i}[A]_{j}+\mu\,{}^{i}[B]_{j}\qquad \mathrm{Coef}_{i,j}(\lambda A+\mu B)=\lambda\mathrm{Coef}_{i,j}(A)+\mu\mathrm{Coef}_{i,j}(B)$$

$\forall\, i,j,\quad {}^{i}[\cdot]_{j}$ ou $\mathrm{Coef}_{i,j}$ est une application linéaire de $\mathcal{M}_{n,p}(\mathbb{K})$

On notera également $L_i(A)$ (respectivement $C_j(A)$), la ligne i (respectivement colonne j de A).
On note que ${}^{i}[AB]_{j}=L_i(A)\times C_j(B)$, c'est un nombre.

2.3. Transposition

Définition - Matrice transposée
Soit $A=(a_{ij})_{1\leqslant i\leqslant n,1\leqslant j\leqslant p}\in\mathcal{M}_{n,p}(\mathbb{K})$,
on définit la **transposée** de A, notée ${}^{t}A$ ou A^{T} par

$$\forall\, i\leqslant p, j\leqslant n:\qquad {}^{i}[A^{T}]_{j}={}^{i}[{}^{t}A]_{j}={}^{j}[A]_{i}$$

On a $A^{T}\in\mathcal{M}_{p,n}(\mathbb{K})$.

La transposée d'une matrice s'obtient en "échangeant" lignes et colonnes :

Exemple - Matrice 3×3

Si $A=\begin{pmatrix}1&-1&-1&-3\\0&1&3&1\\-1&1&1&3\end{pmatrix}$ alors ${}^{t}A=\begin{pmatrix}1&0&-1\\-1&1&1\\-1&3&1\\-3&1&3\end{pmatrix}$

Théorème - Isomorphisme
Sous réserve que la taille des matrices permette d'effectuer les différentes opérations, on a :

$$(A+B)^{T}=A^{T}+B^{T};\quad (\lambda A)^{T}=\lambda A^{T};\quad (A^{T})^{T}=A$$

La transposition est donc un isomorphisme entre les espaces vectoriels $\mathcal{M}_{n,p}(\mathbb{K})$ et $\mathcal{M}_{p,n}(\mathbb{K})$.

Exercice
Faire la démonstration

Correction
Jeu d'écriture

3. Multiplication matricielle

3.1. Définition

Définition - Produit de deux matrices
Le produit d'une matrice $A = (a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ de $\mathcal{M}_{n,p}(\mathbb{K})$ par une matrice $B = (b_{ij})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant q}}$ de $\mathcal{M}_{p,q}(\mathbb{K})$ est une matrice de $\mathcal{M}_{n,q}(\mathbb{K})$ définie par

$$C = AB = (c_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant q}}$$

où

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{ip}b_{pj} = \sum_{k=1}^{p} a_{ik}b_{kj}.$$

Savoir faire - Notation et multiplication matricielle
Par la suite, on notera $\text{Coef}_{i,j}(A)$, le coefficient en ligne i et colonne j de la matrice A.
On a donc

$${}^{i}[AB]_{j} = \sum_{k=1}^{p} {}^{i}[A]_{k}\,{}^{k}[B]_{j}$$

Il faut savoir passer d'un sens vers l'autre : $\text{Coef}_{i,j}(AB) = \sum_{k=1}^{p} \text{Coef}_{i,k}(A)\text{Coef}_{k,j}(B)$

et aussi $\sum_{k=1}^{p} \text{Coef}_{i,k}(A)\text{Coef}_{k,j}(B) = \text{Coef}_{i,j}(AB)$.

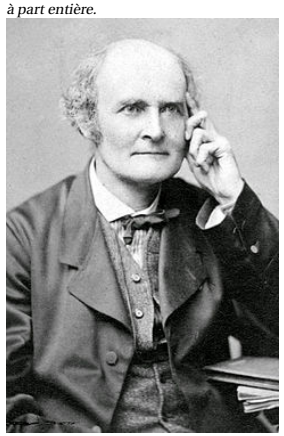
Pour aller plus loin - La convention d'Einstein
La convention d'Einstein en physique consiste à voir dans toute répétition de deux lettres muettes une somme. Ainsi le symbole $\sum$ peut être enlevé.
Le fait qu'une telle convention existe signifie la fréquence importante des opérations du type

$$\sum_{k=1}^{n} a_{i,k}b_{k,j}$$

écrit par Einstein : $a_{i,k}b_{k,j}\ldots$

Attention - Taille des matrices
On ne peut pas multiplier une matrice de $\mathcal{M}_{3,4}(\mathbb{K})$ avec une matrice de $\mathcal{M}_{5,6}(\mathbb{K})$! Il faut que le nombre de colonnes de la première matrice soit égal au nombre de lignes de la seconde.

Histoire - Arthur Cayley
C'est Arthur Cayley qui définit le produit matriciel, dans le premier article (1855) qui étudie les matrices comme objets mathématiques à part entière.



Arthur Cayley est un brillant avocat puis mathématicien anglais né en 1821 et mort en 1895. C'est un génie très hétéroclite.

Savoir faire - Présentation des calculs
Une méthode pratique de présentation des calculs :

$$\begin{pmatrix} \vdots & \vdots & b_{1j} & \ldots \\ \ldots & \ldots & b_{2j} & \ldots \\ \vdots & \vdots & \vdots & \vdots \\ \ldots & \ldots & b_{pj} & \ldots \end{pmatrix}$$

$$\begin{pmatrix} \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{ip} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \ldots & \ldots & c_{ij} & \ldots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

Application - Produit de deux matrices

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \quad \begin{pmatrix} 1+6+15 & 2+8+18 \\ 4+15+30 & 8+20+36 \end{pmatrix} \quad = \quad \begin{pmatrix} 22 & 28 \\ 49 & 64 \end{pmatrix}$$

Pour aller plus loin - Interprétation en terme de graphes
Un dessin permettra d'expliquer au mieux ce à quoi peut servir une matrice. Il faut d'abord considérer :

1. *un ensemble de départ ; par exemple : $A = \{a_1, a_2\}$*
2. *un ensemble d'arrivée ; par exemple : $B = \{b_1, b_2, b_3\}$*
3. *un jeu de flèches entre les deux ensembles, associés à des nombres.*
   Par exemple, la flèche $a_i \to b_j =_i X^j$ indique la relation entre a_i et b_j.

C'est cette flèche qui est abstraite, la plus ouverte possible. Elle peut être par exemple un temps de trajet, un coefficient de proportionalité… Ainsi la figure 1 suivante est représentée par la matrice $\begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,1} & x_{2,2} & x_{2,3} \end{pmatrix}$.

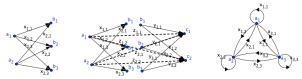


FIG.1-GRAPHE - FIG.2-PRODUIT -FIG.3- CARRÉE MATRICIEL

La figure 3 représente un matrice d'un ensemble dans lui-même (comme pour les endomorphismes), elle est nécessairement carrée.
La figure 2 représente alors le produit matriciel. En effet, il s'agit de savoir comment aller alors de $A = \{a_1, a_2\}$ à $C = \{c_1, c_2\}$. La réponse est obtenue sous forme de matrice $z_{i,j}$, où $z_{i,j}$ indique les chemins de a_i à c_j. Il y a en fait trois possibilités : passer par b_1, b_2 ou b_3, cela donne donc exactement :

$$\begin{aligned} z_{i,j} &= x_{i,1}y_{1,j} + x_{i,2}y_{2,j} + x_{i,3}y_{3,j} \\ &= \sum_{k=1}^{3} x_{i,k}y_{k,j} \\ &= \sum_{k=1}^{3} Coef_{i,k}(X)Coef_{k,j}(Y) \end{aligned}$$

Exemple - Petits calculs
Soient $A = \begin{pmatrix} 2 & -3 & -4 \\ 3 & 1 & 5 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & -3 & 2 \\ -1 & 5 & -2 \\ -1 & 3 & 0 \end{pmatrix}$. Calculer, si cela est possible, AB, BA, A^2, B^2.

Exercice
Simplifier le produit :

$$\sum_{h=1}^{n}\sum_{\ell=1}^{n}\sum_{j=1}^{n} a_{\ell,j}b_{i,h}c_{h,\ell}d_{j,m}$$

Correction
Il est évident que le résultat dépend de i et de m et d'aucun autre nombre.
Les nombres ${}_{\ell}[A]^{j}\ldots$ sont des nombres réels, on peut donc les faire commuter.

$$\sum_{h=1}^{n}\sum_{\ell=1}^{n}\sum_{j=1}^{n} a_{\ell,j}b_{i,h}c_{h,\ell}d_{j,m} = \sum_{h=1}^{n}\sum_{\ell=1}^{n}\sum_{j=1}^{n} b_{i,h}c_{h,\ell}a_{\ell,j}d_{j,m} = \text{Coef}_{i,m}(BCAD)$$

Il s'agit du nombre en ligne i et colonne m de la matrice $B \times C \times A \times D$.

3.2. Interprétation en terme de systèmes linéaires

Analyse - Multiplication par une matrice colonne
Si $A = (a_{ij})_{1\leqslant i\leqslant n,\,1\leqslant j\leqslant p}$, et $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$, alors

$$AX = \begin{pmatrix} a_{11} & \ldots & \ldots & a_{1p} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \ldots & \ldots & a_{np} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1p}x_p \\ \vdots \\ \vdots \\ a_{n1}x_1 + \ldots + a_{np}x_p \end{pmatrix}$$

Proposition - $(S) \Leftrightarrow AX = B$
L'équation $AX = B$ pour des matrices est une manière compacte d'écrire un système linéaire général avec n équations, p inconnues et un second

membre $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$

$$(S)\begin{cases} a_{11}x_1 & +\ldots & +a_{1p}x_p & = b_1 \\ a_{21}x_1 & +\ldots & +a_{2p}x_p & = b_2 \\ \vdots & + & +\vdots & = \vdots \\ a_{n1}x_1 & +\ldots & +a_{np}x_p & = b_n. \end{cases}$$

Nous reviendrons sur ce parallèle lorsque nous prendrons le temps de résoudre des systèmes linéaires.

3.3. Propriété du produit

Proposition - Associativité du produit
Le produit de matrices est associatif.
Plus précisément si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $B \in \mathcal{M}_{p,q}(\mathbb{K})$, $C \in \mathcal{M}_{q,m}(\mathbb{K})$ alors on a

$$(AB)C = A(BC)$$

qui est une matrice de $\mathcal{M}_{n,m}(\mathbb{K})$.

Démonstration
Le seul problème réside dans la manipulation des indices.
Appelons $D = (d_{ih})$ la matrice AB; le coefficient de la $i$ème ligne et de la $h$ème colonne est donné par

$$d_{ih} = \sum_{k=1}^{n} a_{ik}b_{kh},$$

donc le coefficient $i,\ j$ de $(AB)C = E$ est donné par

$$\sum_{h=1}^{p} d_{ih}c_{hj} = \sum_{h=1}^{p}\left(\sum_{k=1}^{n} a_{ik}b_{kh}\right)c_{hj}$$
$$= \sum_{h=1}^{p}\sum_{k=1}^{n} a_{ik}b_{kh}c_{hj} = e_{ij}.$$

Calculons maintenant le coefficient $k,\ j$ de $D' = BC = (d'_{kj})$

$$d'_{kj} = \sum_{h=1}^{p} b_{kh}c_{hj},$$

le coefficient $i,\ j$ de $E' = A(BC) = (e'_{ij})$ est obtenu en faisant :

$$e'_{ij} = \sum_{k=1}^{n} a_{ik}d'_{kj} = \sum_{k=1}^{n} a_{ik}\left(\sum_{h=1}^{p} b_{kh}c_{hj}\right)$$
$$= \sum_{k=1}^{n}\sum_{h=1}^{p} a_{ik}b_{kh}c_{hj}$$

d'où l'égalité que l'on appelle associativité. □

Remarque - En terme de Coef$_{i,j}$
Ce que l'on a démontré c'est :

$$^{i}[(AB)C]_{j} = \sum_{h,k}^{i} [A]^{h}_{h}[B]^{k}_{k}[C]_{j} = {}^{i}[A(BC)]_{j}$$

Proposition - Bilinéarité
Si A et B sont des matrices de $\mathcal{M}_{n,p}(\mathbb{K})$ et C, D de $\mathcal{M}_{p,q}(\mathbb{K})$, $\lambda, \mu \in \mathbb{K}$ alors

$$A(\lambda C + \mu D) = \lambda AC + \mu AD \quad \text{et} \quad (\lambda A + \mu B)C = \lambda AC + \mu BC$$

En résumé l'application $(A, C) \in \mathcal{M}_{n,p}(\mathbb{K}) \times \mathcal{M}_{p,q}(\mathbb{K}) \mapsto AC \in \mathcal{M}_{n,q}(\mathbb{K})$ est bilinéaire.

Pour aller plus loin - Application aux probabilités
Ecrire : « $z_{i,j}$ indique les chemins de a_i à c_j. Il y a en fait trois possibilités : passer par b_1, b_2 ou b_3 » nous rappelle la formule des probabilités totales.
En effet, on se souvient que si (B_1, B_2, B_3) forme un système complet d'événements, alors :

$$\mathbf{P}(A_i) = \mathbf{P}(B_1) \times \mathbf{P}_{B_1}(A_i) + \mathbf{P}(B_2) \times \mathbf{P}_{B_2}(A_i)$$
$$+\mathbf{P}(B_3) \times \mathbf{P}_{B_3}(A_i)$$

Ce se résume en

$$(A+B)(C+D) = AC + AD + BC + BD$$

Démonstration
On ne fera qu'un calcul.

$$\text{Coef}_{i,j}\left(A(\lambda C + \mu D)\right) = \lambda \sum_{h=1}^{p} \text{Coef}_{i,h}(A)\text{Coef}_{h,j}(C) + \mu \sum_{h=1}^{p} \text{Coef}_{i,h}(A)\text{Coef}_{h,j}(D)$$

(...) □

Proposition - Cas à connaître!
$(E_{i,j})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}}$ désigne la base canonique de $\mathcal{M}_{n,p}(\mathbb{K})$ i.e. ${}^{a}[E_{i,j}]_{b} = \delta_{a,i}\delta_{b,j}$
et $(F_{i,j})_{\substack{1\leqslant i\leqslant p \\ 1\leqslant j\leqslant q}}$ celle de $\mathcal{M}_{p,q}(\mathbb{K})$.
Alors $E_{i,j} \times F_{k,\ell} = \delta_{k,j}G_{i,\ell}$, avec $(G_{s,t})_{\substack{1\leqslant s\leqslant n \\ 1\leqslant r\leqslant q}}$ base canonique de $\mathcal{M}_{n,q}(\mathbb{K})$

Démonstration
Il s'agit de calculer $E_{i,j}F_{k,\ell}$ pour les différents quadruplets possibles (i, j, k, ℓ).
Résultat à retenir (ou à savoir retrouver rapidement). Il faut quatre lettres muettes (2 pour E et 2 pour F), et deux lettres (provisoires) pour préciser la position :

$$\text{Coef}_{a,b}(E_{i,j}F_{k,\ell}) = \sum_{h=1}^{p} \text{Coef}_{a,h}(E_{i,j})\text{Coef}_{h,b}(F_{k,\ell}) = \sum_{h=1}^{p} \delta_{a,i}\delta_{h,j}\delta_{h,k}\delta_{b,\ell} = \begin{cases} 0 & \text{si } k \neq j \\ \delta_{a,i}\delta_{b,\ell} & \text{si } k = j \end{cases}$$

Donc si $a \neq i$ ou $b \neq \ell$, $\text{Coef}_{a,b}(E_{i,j}F_{k,\ell}) = 0$.
Et si $k = j$, alors pour $a = i$, $b = \ell$, on a $\text{Coef}_{a,b}(E_{i,j}F_{k,\ell}) = 1$.
Donc $E_{i,j} \times F_{k,\ell} = \delta_{k,j}G_{i,\ell}$, avec $(G_{s,t})_{\substack{1\leqslant s\leqslant n \\ 1\leqslant r\leqslant q}}$ base canonique de $\mathcal{M}_{n,q}(\mathbb{K})$. □

Pour aller plus loin - Transposition et graphe
La matrice transposée est la matrice associée au graphe où le sens des flèches s'inverse par rapport à la situation initiale

Exercice
Comment écrire la matrice $AE_{i,j}$ à partir de la matrice A ?
De même pour $E_{i,j}A$?

Correction
Pour tout k, h,

$$^{k}[AE_{i,j}]_{h} = \sum_{s=1}^{n} {}^{k}[A]_{s}\delta_{i,s}\delta_{j,h} = \delta_{j,h}\,{}^{k}[A]_{i}$$

Donc si $h \neq 0$, on trouve le nombre nul et si $h = j$, on obtient le nombre ${}^{k}[A]_{i}$, situé précédemment en colonne i de A.
On obtient donc une matrice formée d'une unique colonne non nulle, l'ancienne colonne i de A, située en colonne j.
De même $E_{i,j}A$ est la matrice formée d'une unique ligne non nulle, l'ancienne ligne j de A, située en colonne i.
On peut aussi exploiter la formule précédente et la linéarité du produit (et distribution)

Proposition - Transposition d'un produit
Pour $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$, on a

$${}^{t}(A \times B) = {}^{t}B \times {}^{t}A$$

Attention - Eviter d'écrire des bêtises
Notons bien que ${}^{t}B \in \mathcal{M}_{q,p}(\mathbb{K})$ et ${}^{t}A \in \mathcal{M}_{p,n}(\mathbb{K})$.
Donc le produit ${}^{t}A \times {}^{t}B$ n'aurait aucun sens (aucune raison que $n = q$.)

Démonstration
Pour tout $(i,j) \in \mathbb{N}_n \times N_q$,

$$\begin{aligned}\text{Coef}_{j,i}\left({}^t(A\times B)\right) = \text{Coef}_{i,j}\left((A\times B)\right) &= \sum_{h=1}^{p} \text{Coef}_{i,h}(A)\times\text{Coef}_{h,j}(B)\\ = \sum_{h=1}^{p} \text{Coef}_{h,i}({}^tA)\times\text{Coef}_{j,h}({}^tB) &= \sum_{h=1}^{p} \text{Coef}_{j,h}({}^tB)\times\text{Coef}_{h,i}({}^tA)\\ &= \text{Coef}_{j,i}({}^tB\times{}^tA)\end{aligned}$$

□

3.4. Produit par blocs

Proposition - Produit par blocs
Soient deux matrices $M \in \mathcal{M}_{n,p}(\mathbb{K})$, $M' \in \mathcal{M}_{p,q}(\mathbb{K})$.
Considérons des entiers $k \leqslant n, \ell \leqslant p, m \leqslant q$ et des matrices $A \in \mathcal{M}_{k,\ell}(\mathbb{K})$, $B \in \mathcal{M}_{k,p-\ell}(\mathbb{K})$, $C \in \mathcal{M}_{n-k,\ell}(\mathbb{K})$, $D \in \mathcal{M}_{n-k,p-\ell}(\mathbb{K})$, $A' \in \mathcal{M}_{\ell,m}(\mathbb{K})$, $B' \in \mathcal{M}_{\ell,q-m}(\mathbb{K})$, $C' \in \mathcal{M}_{p-\ell,m}(\mathbb{K})$, $D' \in \mathcal{M}_{p-\ell,q-m}(\mathbb{K})$ telles que M et N s'écrivent par blocs

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad M' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$$

Alors, on peut calculer le produit MM' par blocs de la manière suivante :

$$MM' = \begin{pmatrix} AA'+BC' & AB'+BD' \\ CA'+DC' & CB'+DD' \end{pmatrix}$$

Attention - Bien faire attention aux dimensions
Il est nécessaire que les dimensions correspondent bien.
Sinon, le calcul écrit n'aurait pas de sens

Démonstration
On calcule $\text{Coef}_{i,j}(MM')$ suivant la position de i par rapport à k et celle de j par rapport à m.
On va faire un cas : $i \leqslant k$ et $j \geqslant m+1$. Donc $\text{Coef}_{i,j}(M\times M')$ se trouve en haut à droite.

$$\begin{aligned}\text{Coef}_{i,j}(MM') &= \sum_{h=1}^{p} \text{Coef}_{i,h}(M)\text{Coef}_{h,j}(M')\\ &= \sum_{h=1}^{\ell} \text{Coef}_{i,h}(M)\text{Coef}_{h,j}(M') + \sum_{h=\ell+1}^{p} \text{Coef}_{i,h}(M)\text{Coef}_{h,j}(M')\\ &= \sum_{h=1}^{\ell} \text{Coef}_{i,h}(A)\text{Coef}_{h,j-m}(B') + \sum_{h=\ell+1}^{p} \text{Coef}_{i,h-\ell}(B)\text{Coef}_{h-\ell,j-m}(D')\end{aligned}$$

Car pour
- $i \leqslant k$, $h \leqslant \ell$, $\text{Coef}_{i,h}(M) = \text{Coef}_{i,h}(A)$,
- $i \leqslant k$, $h \geqslant \ell+1$, $\text{Coef}_{i,h}(M) = \text{Coef}_{i,h-\ell}(B)$,
- $h \leqslant \ell$, $j \geqslant m+1$, $\text{Coef}_{h,j}(M') = \text{Coef}_{h,j-m}(B')$,
- $h \leqslant \ell$, $j \leqslant m+1$, $\text{Coef}_{h,j}(M') = \text{Coef}_{h-\ell,j-m}(D')$,

Donc

$$\text{Coef}_{i,j}(MM') = \text{Coef}_{i,j-m}(AB') + \text{Coef}_{i,j-m}(BD') = \text{Coef}_{i,j-m}(AB'+BD')$$

□

On peut avoir intérêt à considérer les matrices sous forme d'une association de colonnes ou de lignes.
On peut voir ces opérations, comme une forme de calculs parallèles, à la physicienne.

Proposition - Matrice et association de colonnes ou de lignes
Soient $A, B \in \mathcal{M}_n(\mathbb{K})$.
Il nous arrivera de noter $A = \begin{pmatrix} \frac{L_1}{L_2} \\ \hline \vdots \\ \hline L_n \end{pmatrix}$
comme une association de n (matrices ou vecteurs) lignes, avec $L_i(A) = L_i$
Il nous arrivera de noter $B = (C_1|C_2|\dots|C_n)$
comme une association de n (matrices ou vecteurs) colonnes, avec $C_j(B) = C_j$
On a alors $AB = (AC_1|AC_2|\dots|AC_n) = \begin{pmatrix} \frac{L_1B}{L_2B} \\ \hline \vdots \\ \hline L_nB \end{pmatrix}$ mais aussi ${}^i[A\times B]_j = L_i \times C_j$.

Exercice
Comment écrire la matrice $E_{i,j}A$ à partir de la matrice A et $AE_{i,j}$, en raisonnant par blocs ?

Correction
$L_k(E_{i,j}A) = L_k(E_{i,j})A = \delta_{k,i}L_i(E_{i,j})A = \delta_{k,i}(L_i(E_{i,j}C_1(A)|\cdots|L_n(E_{i,j}C_1(A)) = \delta_{k,i}({}^jL_1|{}^jL_2|\cdots{}^jL_n) = \delta_{k,i}L_j(A)$

4. Les matrices carrées

4.1. L'anneau $(\mathcal{M}_n(\mathbb{K}),+,\times)$

Pour aller plus loin - Algèbre ?
On appelle $\mathbb{K}$-algèbre un ensemble $\mathcal{A}$ muni de deux opérations interne (notées ici $+$ et $\times$) et une opération externe (notée ici $\cdot$) telle que $(\mathcal{A},+,\cdot)$ est un $\mathbb{K}$-espace vectoriel et $(\mathcal{A},+,\times)$ est un anneau.

Pour aller plus loin - Algèbre
$(\mathcal{M}_n(\mathbb{K}),+,\times,.)$ est une $\mathbb{K}$-algèbre de dimension n^2.

Heuristique - Pourquoi les matrices carrées ?
Si on multiplie deux matrices de $\mathcal{M}_n(\mathbb{K})$ on trouve un élément de $\mathcal{M}_n(\mathbb{K})$, la multiplication est donc interne dans $\mathcal{M}_n(\mathbb{K})$.
On peut ainsi effectuer les calculs $A\times B$ et $B\times A$, mais aussi A^k pour tout entier k…
Nous verrons qu'ains $(\mathcal{M}_n(\mathbb{K}),+,\times)$ est un anneau.

Théorème - La $\mathbb{K}$-algèbre $(\mathcal{M}_n(\mathbb{K}),+,\times,.)$
$(\mathcal{M}_n(\mathbb{K}),+,\times)$ est un anneau non commutatif et non intègre dès que $n \geqslant 2$, d'élément unité I_n.

Exemple - Non commutativité et non intégrité
Vérifiez que

$$\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix} \neq \begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}$$

puis que

$$\begin{pmatrix}0&1\\0&1\end{pmatrix}\begin{pmatrix}2&1\\0&0\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

Exemple - L'inverse d'une matrice d'ordre 2
Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Alors en notant $A' = \begin{pmatrix} d & -b \\ c & a \end{pmatrix}$, on a :

$$A\times A' = A'\times A = (ad-bc)I_2$$

Donc si $ad-bc \neq 0$, A est inversible et $A^{-1} = \frac{1}{ad-bc}A'$.

4.2. Puissance de matrices

Définition - Puissance d'une matrice
Soit $A \in \mathcal{M}_n(\mathbb{K})$, on définit par récurrence :

$$A^0 = I_n, \quad \forall\, k \in \mathbb{N}, A^{k+1} = A \times A^k$$

On a alors, par commutation :

$$A^k = \underbrace{A \times \ldots \times A}_{k \text{ fois}} = A^m \times A^{k-m} \quad \text{(pour tout } m \leqslant k)$$

Les règles de calcul dans un anneau (comme dans $\mathbb{R}$ ou $\mathbb{C}$) s'appliquent d'où :

Proposition - Formules matricielles
Pour $A, B \in \mathcal{M}_n(\mathbb{K})$, si $AB = BA$ alors

$$(A+B)^p = \sum_{k=0}^{p} \binom{p}{\mathbb{K}} A^k B^{p-k} \text{ (Formule du binôme de Newton)}$$

$$A^p - B^p = (A-B)(A^{p-1} + A^{p-2}B + \cdots + AB^{p-2} + B^{p-1})$$

$$I_n - A^p = (I_n - A)(I_n + A + A^2 + \cdots + A^{p-1})$$

4.3. Inversibilité d'une matrice

Définition - Inversibilité de A
On dit qu'une **matrice carré d'ordre** n A est inversible, si elle admet un inverse pour la loi $\times$, c'est-à-dire s'il existe une matrice carrée d'ordre n B telle que

$$BA = AB = I_n$$

(où I_n est la matrice identité). B est alors notée A^{-1} et appelée inverse de A.

Remarque - Des matrices non inversibles
On ne peut pas inverser de matrices de $\mathcal{M}_{n,p}(\mathbb{K})$ si $n \neq p$.
Une matrice carrée n'est pas nécessairement inversible :
par exemple, la matrice nulle O_n n'a pas d'inverse car

$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ AO_n = O_n \neq I.$$

Exemple - Matrice non inversible, moins triviale
De plus il y a des matrices non nulles qui n'ont pas d'inverse.
Par exemple $N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ n'a pas d'inverse.
En effet, pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$A \times N = \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix}$$

Elle ne peut pas être égale à I_2.

Remarque - Rappels
Nous avons vu que l'ensemble des inverses d'un anneau forme un groupe.
On l'avait noté $A^\times$.

Définition - Le groupe $GL_n(\mathbb{K})$
L'ensemble $(GL_n(\mathbb{K}), \times)$ des inversibles de l'anneau $\mathcal{M}_n(\mathbb{K})$ est un groupe, non commutatif.
On l'appelle le groupe linéaire.
On a donc pour A, $B \in GL_n(\mathbb{K})$, $(AB)^{-1} = B^{-1}A^{-1}$.

Proposition - Inverse de la transposé
Si A est une matrice carrée inversible alors ${}^tA$ est aussi inversible et $({}^tA)^{-1} = {}^t(A^{-1})$.

Démonstration
« Le coup des chaussettes dans le tiroir… »
$(AB) \times (B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AA^{-1} = I_n$ et $(B^{-1}A^{-1}) \times (AB) = B^{-1}(A^{-1}A)B = B^{-1}B = I_n$
Donc $(AB)^{-1} = B^{-1}A^{-1}$.
De même, en transposant un produit :

$$I_n = {}^t(I_n) = {}^t(A \times A^{-1}) = {}^t(A^{-1}) \times {}^tA \qquad I_n = {}^t(I_n) = {}^t(A^{-1} \times A) = {}^tA \times {}^t(A^{-1})$$

Donc $({}^tA)^{-1} = {}^t(A^{-1})$ □

Pour aller plus loin - Polynôme annulateur
On montrera en seconde année que pour tout matrice $M \in \mathcal{M}_n(\mathbb{K})$, l'ensemble des polynômes annulateurs de M

$$\{P \in \mathbb{K}[X] \mid P(M) = 0\}$$

est non vide. On sait assurément qu'il existe au moins un polynôme de degré n dans cet ensemble (le polynôme caractéristique de M - d'après le théorème de Cayley-Hamilton).
Et mieux, comme $\mathbb{K}[X]$ est un anneau euclidien, cet ensemble est forcément de la forme

$$\{P \in \mathbb{K}[X] \mid P(M) = 0\} = \mu_P \mathbb{K}[X]$$

où μ_P est un polynôme particulier : minimal (en degré), unitaire et propre à P. On l'appelle le polynôme minimal de P

Exercice
Soit $J \in \mathcal{M}_n(\mathbb{R})$ la matrice dont tous les coefficients sont des 1.
1. On suppose $n = 2$. Calculer J^2, J^3, J^k pour $k \in \mathbb{N}$.
2. Mêmes questions avec $n \geqslant 2$ quelconque. J est-elle inversible ?
3. Calculer A^p où $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$.

Correction
1. Pour $n = 2$, on montre aisément que $J^2 = 2J$, $J^3 = 4J$ et pour tout $k \in \mathbb{N}$, $J^k = 2^{k-1}J$ (récurrence).
2. Maintenant, on suppose que $n \geqslant 2$.

$$\text{Coef}_{i,j}(J^2) = \sum_{h=1}^{n} \text{Coef}_{i,h}(J)\text{Coef}_{h,j}(J) = \sum_{h=1}^{n} 1 = n = n\text{Coef}_{i,j}(J)$$

Donc $J^2 = nJ$ Par récurrence, supposons $J^k = n^{k-1}J$.

$$J^{k+1} = J^k J = n^{k-1}JJ = n^{k-1}nJ = n^k J = n^{(k+1)-1}J$$

Si J était inversible, on aurait les égalités :

$$J = J^{-1} \times J^2 = nJ^{-1}J = nI_n$$

Ce qui est faux.
3. $A = I_3 + J_3$, I_3 commute avec J_3 et donc on peut appliquer la formule de Newton :

$$A^p = \sum_{k=0}^{p} \binom{p}{\mathbb{K}} I_3^{p-k} J^k = I_3 + \sum_{k=1}^{p} \binom{p}{\mathbb{K}} I_3^{p-k} 3^{k-1} J$$

$$= I_3 + \frac{1}{3}\left(\sum_{k=1}^{p} \binom{p}{\mathbb{K}} 3^k\right) J = I_3 + \frac{1}{3}((3+1)^p - 1)J$$

$$= \frac{1}{3}\begin{pmatrix} 4^p+2 & 4^p-1 & 4^p-1 \\ 4^p-1 & 4^p+2 & 4^p-1 \\ 4^p-1 & 4^p-1 & 4^p+2 \end{pmatrix}$$

(On peut vérifier pour $p = 1$ que cela fonction bien…

Savoir faire - Exploiter un polynôme annulateur pour trouver M^{-1}
Soit $M \in \mathcal{M}_n(\mathbb{K})$. Supposons que le polynôme $P = \sum_{k=0}^{d} a_k X^k$ annule M, c'est-à-dire que $P(M) = \sum_{k=0}^{d} a_k M^k = 0$. Alors
— si $a_0 \neq 0$, on a alors $I_n = \frac{-1}{a_0}\left(\sum_{k=1}^{d} a_k M^k\right) = M \times \frac{-1}{a_0}\left(\sum_{k=1}^{d} a_k M^{k-1}\right)$.
Et donc nécessairement M est inversible et $M^{-1} = \frac{-1}{a_0}\left(\sum_{k=0}^{d-1} a_{k+1} M^{\mathbb{K}}\right)$
— si $a_0 = 0$, alors il faut faire un raisonnement par l'absurde :
si M était inversible alors en multipliant par M^{-1}, on a

$$M^{-1}\times P(M)=\sum_{k=1}^{d}a_kM^{k-1}=0 \text{ et donc } \sum_{k=0}^{d-1}a_{k+1}M^{\mathbb{K}}=0.$$

Il y a alors deux options,
ou bien cette somme n'est pas nulle, et par l'absurde, M n'est pas inversible,
ou bien cette somme vaut bien 0 et donc on recommence au point initial.

Savoir faire - Exploiter un polynôme annulateur pour trouver M^n

Soit $M\in\mathcal{M}_n(\mathbb{K})$. Supposons que le polynôme $P=\sum_{k=0}^{d}a_kX^k$ annule M, c'est-à-dire que $P(M)=\sum_{k=0}^{d}a_kM^k=0$.
Alors, on peut faire la division euclidienne de X^n par P :
il existe $Q_n,R_n\in\mathbb{K}[X]$ tels que $X^n=Q_n(X)\times P(X)+R_n(X)$ avec $\deg(R_n)<\deg(P)=d$.
On a alors, puisque $M^n=0+R_n(M)$ car $P(M)=0$.
Cela permet de
— démontrer que $\{M^n,\in\mathbb{Z}\}\subset \text{vect}(I_n,M,M^2,\dots M^{d-1})$ (résultat théorique classique)
— calculer explicitement M^n, si l'on sait faire explicitement cette division euclidienne. Pour faire celle-ci, il arrive souvent qu'on utilise les racines de P…

Application - Inverse et puissance de $M=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$

On remarque que $(M-I_3)^3=0$, donc on a un polynôme annulateur de M :

$$P(X)=(X-1)^3=X^3-3X^2+3X-1$$

Ainsi : $M(M^2-3M+3I_3)=M^3-3M^2+3M=I_3$.

Donc M est inversible d'inverse $M^{-1}=M^2-3M+3I_3=\begin{pmatrix}1&-1&1\\0&1&-1\\0&0&1\end{pmatrix}$ De même, si l'on fait la division euclidienne, on a :

$$X^n=Q_n(X-1)^3+R_n \qquad \text{où } \deg(R_n)\leqslant 2$$

On peut exploiter la formule de Taylor, en 1 (en notant $P(X)=X^n$) :

$$X^n=\sum_{k=0}^{n}\frac{P^{(\mathbb{K})}(1)}{k!}(X-1)^k=\underbrace{P(1)+P'(1)(X-1)+\frac{P''(1)}{2}(X-1)^2}_{=R_n}+(X-1)^3\underbrace{\sum_{k=3}^{n}\frac{P^{(\mathbb{K})}(1)}{k!}(X-1)^{k-3}}_{=Q_n}$$

Or $P(1)=1$, $P'(1)=n$ et $P''(1)=n(n-1)$. Ainsi

$$R_n(X)=1+n(X-1)+\frac{1}{2}n(n-1)(X-1)^2$$

Ainsi $M^n=\begin{pmatrix}1&n&\frac{n(n-1)}{2}\\0&1&n\\0&0&1\end{pmatrix}$

Exercice

Soit $A=(a_{pq})\in\mathcal{M}_n(\mathbb{C})$ définie par $a_{pq}=\exp(\frac{2i\pi pq}{n})$ et $\overline{A}=(\overline{a_{pq}})$.
Calculer $A\overline{A}$ et en déduire que A est inversible.

Correction
(On ne prendra pas i, à cause du i imaginaire pure).
Pour tout $k,\ell\in\mathbb{N}_n$,

$$\text{Coef}_{k,\ell}(A\overline{A})=\sum_{h=1}^{n}a_{k,h}\overline{a_{h,\ell}}=\sum_{h=1}^{n}\exp(\frac{2i\pi}{n}(kh-h\ell))$$

$$=\sum_{h=1}^{n}\exp(\frac{2hi\pi}{n}(k-\ell))$$

$$=\begin{cases}\sum_{h=1}^{n}1=n & \text{si } k=\ell\\ \sum_{h=1}^{n}\left(\exp(\frac{2i\pi}{n}(k-\ell))\right)^h=\frac{1-\exp(\frac{2ni\pi}{n}(k-\ell))}{1-\exp(\frac{2i\pi}{n}(k-\ell))}=0 & \text{si } k\neq\ell\end{cases}$$

Donc $A\overline{A}=nI_n$.
Notons alors que $\overline{A}A=\overline{A\overline{A}}=nI_n$.
Ainsi A est inversible et $A^{-1}=\frac{1}{n}\overline{A}$.

4.4. Quelques sous-ensembles remarquables

Matrices diagonales

Proposition - Matrices scalaires
L'ensemble des matrices scalaires d'ordre n, à coefficients dans $\mathbb{K}$, est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ de dimension 1, contenant I_n et stable par la multiplication (c'est un sous-anneau commutatif et aussi une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$).

Pour aller plus loin - Base 1
Donc l'espace des matrices scalaires est $\text{vect}(I_n)$*, de dimension 1.*

Proposition - Espace des matrices diagonales
L'ensemble des matrices diagonales d'ordre n, à coefficients dans $\mathbb{K}$, est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ de dimension n, contenant I_n et stable par la multiplication (c'est un sous-anneau commutatif et une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$).

Pour aller plus loin - Base 2
Donc l'espace des matrices diagonales est $\text{vect}\big((E_{i,i})_{i\in\mathbb{N}_n}\big)$*, de dimension n.*

Proposition - Inverse de matrices diagonales
Si D est diagonale, $D=\text{diag}(d_1,\dots,d_n)$, alors D est inversible si et seulement pour tout $i\in\{1,\dots,n\}$, $d_i\neq 0$ et alors $D^{-1}=\text{diag}(\frac{1}{d_1},\dots,\frac{1}{d_n})$.
Donc D^{-1} est elle-même une matrice diagonale.

Démonstration
Pour tout $i,j\in\mathbb{N}_n$, par définition de D

$$\text{Coef}_{i,j}(A\times D)=\sum_{h=1}^{n}\text{Coef}_{i,h}(A)\text{Coef}_{h,j}(D)=d_j\text{Coef}_{i,j}(A)$$

Donc pour que $A\times D=I_n$,
il faut pour tout $i\in\mathbb{N}_n$, $\text{Coef}_{i,i}(AD)=d_i\text{Coef}_{i,i}(A)=1$, il est nécessaire que $d_i\neq 0$.
En prenant alors $\text{Coef}_{i,i}(A)=\frac{1}{d_i}$, on a donc $\text{Coef}_{i,i}(AD)=1$.
il faut également pour tout $j\neq i$, $\text{Coef}_{i,j}(AD)=0=d_i\text{Coef}_{i,j}(A)$,
donc nécessairement $\text{Coef}_{i,j}(A)=0$.
Par conséquent, pour que D soit inversible, il faut $d_i\neq 0$, pour tout i.
Et la seule matrice qui conviendrait pour inverse est $A=\text{diag}(\frac{1}{d_1},\dots\frac{1}{d_n})$ (car $AD=I_n$).
Un calcul simple confirme : $D\times A=I_n$ également.
On a trouvé alors une condition nécessaire et suffisante avec, alors, une expression de D^{-1}. □

Matrices symétriques et antisymétriques

Pour aller plus loin - Bases 3
Donc $\mathcal{S}_n(\mathbb{K})=\text{vect}\big((E_{i,j}+E_{j,i})_{i\leqslant j\in\mathbb{N}_n}\big)$*, espace de dimension* $\frac{1}{2}n(n+1)$.
Et $\mathcal{A}_n(\mathbb{K})=\text{vect}\big((E_{i,j}-E_{j,i})_{i<j\in\mathbb{N}_n}\big)$*, espace de dimension* $\frac{1}{2}n(n-1)$.

Définition - Matrices symétriques et antisymétriques
Soit $A\in\mathcal{M}_n(\mathbb{K})$.
A est dite **symétrique** si ${}^tA=A$, soit si pour tout (i,j), $a_{ij}=a_{ji}$ (ou ${}^i[A]_j={}^j[A]_i$) ;
on note $\mathcal{S}_n(\mathbb{K})$ l'ensemble des matrices symétriques d'ordre n à coefficients dans $\mathbb{K}$.
A est dite **antisymétrique** si ${}^tA=-A$, soit si pour tout (i,j), $a_{ij}=-a_{ji}$ (ou ${}^i[A]_j=-{}^j[A]_i$) ;

on note $\mathcal{A}_n(\mathbb{K})$ (ou $\mathcal{AS}_n(\mathbb{K})$) l'ensemble des matrices antisymétriques d'ordre n à coefficients dans $\mathbb{K}$.

En l'absence d'ambiguité, on peut noter $\mathcal{S}_n$ et $\mathcal{A}_n$.

Proposition - Diagonale d'une matrice antisymétrique
Les éléments diagonaux d'une matrice antisymétrique sont nuls.

Pour aller plus loin - Matrices et graphes
Que signifie pour un graphe que sa matrice associée est symétrique? Antisymétrique?

Démonstration
A, antisymétrique. Pour tout $i \in \mathbb{N}_n$,

$$\text{Coef}_{i,i}(A) = -\text{Coef}_{i,i}(A) \Longrightarrow 2\text{Coef}_{i,i}(A) = 0$$

□

Ensemble des matrices triangulaires (supérieures)

Théorème - Espace des matrices triangulaires
L'ensemble des matrices triangulaires supérieures (respectivement inférieures) d'ordre n, à coefficients dans $\mathbb{K}$, est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ de dimension $\frac{n(n+1)}{2}$, contenant I_n.
Il est stable pour la multiplication (donc est un sous-anneau et une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$).

Pour aller plus loin - Base 4
Donc il s'agit de $\text{vect}\left((E_{i,j})_{i\leqslant j\in\mathbb{N}_n}\right)$, *espace de dimension* $\frac{1}{2}n(n+1)$.

Attention - Pas trop vite
L'ensemble des matrices triangulaires d'ordre n, à coefficients dans $\mathbb{K}$, n'est pas un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$.
L'addition d'une matrice triangulaire supérieure et d'une matrice triangulaire inférieure ne donne pas une matrice triangulaire, la plupart du temps

Pour aller plus loin - Inverse d'une matrice triangulaire supérieure
Nous verrons que si T une matrice triangulaire supérieure, carrée.
Alors T est inversible ssi $\forall\ i \in \mathbb{N}_n$, $Coef_{i,i}(T) \neq 0$.
Et dans ce cas, T^{-1} est également triangulaire supérieure

Remarque - Mais notons :
Une matrice à la fois triangulaire inférieure et supérieure est diagonale.

Savoir faire - Montrer qu'une matrice est triangulaire supérieure
Il faut montrer (condition nécessaire et suffisante) :

$$\forall\ i, j \in \mathbb{N}_n, \quad i > j \quad \Longrightarrow \quad \text{Coef}_{i,j}(T) = 0$$

Il faut démontrer la stabilité par somme (facile) et par multiplication de matrices triangulaires supérieures.

Démonstration
Soit T_1 et T_2 deux matrices triangulaires supérieures.
Pour tout $i > j$:

$$\begin{aligned}\text{Coef}_{i,j}(T_1T_2) &= \sum_{k=1}^{n} \text{Coef}_{i,k}(T_1)\text{Coef}_{k,j}(T_2)\\ &= \sum_{k=1}^{i-1} \underbrace{\text{Coef}_{i,k}(T_1)}_{=0\,:\,i>k}\text{Coef}_{k,j}(T_2) + \sum_{k=i}^{n} \text{Coef}_{i,k}(T_1)\underbrace{\text{Coef}_{k,j}(T_2)}_{=0\,:\,k\leqslant i>j} = 0\end{aligned}$$

Donc T_1T_2 est triangulaire supérieure. □

4.5. Trace d'une matrice carrée

Définition - Trace d'une matrice
Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice carrée. On appelle trace de A le scalaire égal à la somme de ses coefficients diagonaux :

$$\text{Tr}\,A = \sum_{i=1}^{n} a_{ii} = \sum_{i=1}^{n} {}^{i}[A]_i = \sum_{i=1}^{n} \text{Coef}_{i,i}(A)$$

Proposition - Propriété de la trace
L'application

$$\begin{aligned}\text{Tr}: \quad \mathcal{M}_n(\mathbb{K}) &\to \mathbb{K}\\ A &\mapsto \text{Tr}\,A\end{aligned}$$

est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$: $\text{Tr}(\lambda A + \mu B) = \lambda\text{Tr}\,A + \mu\text{Tr}\,B$ et

$$\forall (A,B) \in \mathcal{M}_n(\mathbb{K})^2,\ \text{Tr}(AB) = \text{Tr}(BA).$$

Démonstration
Par linéarité de $\text{Coef}_{i,i}$:

$$\text{Tr}(\lambda A + \mu B) = \sum_{i=1}^{n} \text{Coef}_{i,i}(\lambda A + \mu B) = \lambda \sum_{i=1}^{n} \text{Coef}_{i,i}(A) + \mu \sum_{i=1}^{n} \text{Coef}_{i,i}(B) = \lambda\text{Tr}(A) + \mu\text{Tr}(B)$$

$$\text{Tr}(AB) = \sum_{i=1}^{n} {}^{i}[AB]_i = \sum_{i=1}^{n}\sum_{h=1}^{n} {}^{i}[A]_h^h[B]_i = \sum_{h=1}^{n}\sum_{i=1}^{n} {}^{h}[B]_i^i[A]_h = \text{Tr}(BA)$$

□

5. Opérations élémentaires sur les matrices

5.1. Opérations élémentaires sur les lignes d'une matrices

Heuristique - Lien résolution de système/inversion de matrice
Le calcul $A \times X = b$ où X et b sont des matrices colonnes est exactement l'écriture d'un système linéaire.
La résolution $X = A^{-1}b$ (si A est inversible donc carrée) exploite les opérations élémentaires sur les lignes du système pour appliquer l'algorithme de Gauss.
Essayons de transférer directement la même idée sur les colonnes de A.

Définition - Opérations élémentaires sur les lignes
On appelle opération élémentaire sur les lignes L_i de la matrice A l'une des transformations suivantes effectuée sur A :
- **Permutation (ou échange)de deux lignes**
  Pour $i \neq j$, $L_i \leftrightarrow L_j$ signifie que l'on permute la i-ième et la j-ième lignes de la matrice.
- **Addition d'un multiple d'une ligne à une autre ligne**
  Pour $i \neq j$, $L_j \leftarrow L_j + \lambda L_i$ signifie que l'on remplace la j-ième ligne L_j de la matrice par $L_j + \lambda L_i$, où $\lambda \in K$.
- **Multiplication d'une ligne par un scalaire NON NUL**
  Pour tout $\alpha \in K$, $\alpha \neq 0$, $L_i \leftarrow \alpha L_i$ signifie que l'on remplace la i-ième ligne par αL_i.

Chacune des manipulations précédentes correspond à un produit matriciel :

Proposition - Transformation élémentaire sur les lignes comme un produit

Effectuer une transformation élémentaire sur les lignes d'une matrice $A \in \mathcal{M}_{n,p}(\mathbb{K})$ revient à calculer le produit matriciel à gauche de A : EA où E est l'une des matrices suivantes :

— Pour $L_i \leftrightarrow L_j$,

$$E = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$$

C'est une matrice de transposition, notée habituellement $P_{i,j} (= P_{j,i})$

— Pour $L_i \leftarrow L_i + \lambda L_j$

$$E = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & \lambda & & \ddots & \\ & & & & 1 \end{pmatrix} = I_n + \lambda E_{ij} \quad \lambda \text{ en ligne } i, \text{ colonne } j$$

C'est une matrice de transvection, notée habituellement $T_{i,j}(\lambda)$

— Pour $L_i \leftarrow \alpha L_i$

$$E = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & 0 & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & \alpha & & \\ & & 0 & & & \ddots & \\ & & & & & & 1 \end{pmatrix} = I_n + (\alpha - 1)E_{ii}$$

C'est une matrice de dilatation, notée habituellement $D_i(\alpha)$

Démonstration

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $E_{ij} \in \mathcal{M}_n(\mathbb{K})$ une des matrices de la base canonique.

On rappelle que ${}^h[BA]_k = \sum_{r=1}^{n} {}^h[B]_r \, {}^r[A]_k$.

Donc ${}^h[E_{i,j}A]_k = \sum_{r=1}^{n} {}^h[E_{i,j}]_r \, {}^r[A]_k = {}^h[E_{i,j}]_j \, {}^j[A]_k = \begin{cases} 0 & \text{si } h \neq i \\ {}^j[A]_k & \text{si } h = i \end{cases}$

On a donc $L_h(E_{i,j}A) = \begin{cases} 0 & \text{si } h \neq i \\ L_j(A) & \text{si } h = i \end{cases} = \delta_{h=i} L_j(A)$ Alors $E_{ij}A$ est la matrice de $\mathcal{M}_{n,p}(\mathbb{K})$ dont toutes les lignes sont nulles sauf la i-ième , qui est la j-ième ligne de A :

$$\forall\, h \neq i \, L_h(E_{i,j}A) = 0 \qquad L_i(E_{i,j}A) = L_j(A)$$

$$\forall\, h \neq i, \ell \in \mathbb{N}_n \text{Coef}_{h,\ell}(E_{i,j}A) = 0 \qquad \text{Coef}_{i,\ell}(E_{i,j}A) = \text{Coef}_{j,\ell}(A)$$

Puis comme $I_n A = A$ et en examinant chacune des opérations élémentaires on obtient le résultat.

• $L_k\big((I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i})A\big) = L_k(A) - \delta_{k,i}L_i(A) - \delta_{k,j}L_j(A) + \delta_{k,i}L_j(A) + \delta_{k,j}L_i(A)$.

$L_k(EA) = \begin{cases} L_i(A) - L_i(A) + L_j(A) = L_j(A) & \text{si } k = i \\ L_j(A) - L_j(A) + L_i(A) = L_i(A) & \text{si } k = i \\ L_k(A) & \text{sinon} \end{cases}$

• $L_k\big((I_n + \lambda E_{i,j})A\big) = L_k(A) + \delta_{k,i}\lambda L_j(A)$.

$L_k(EA) = \begin{cases} L_i(A) + \lambda L_j(A) & \text{si } k = i \\ L_k(A) & \text{sinon} \end{cases}$

• $L_k\big((I_n + (\alpha - 1)E_{i,i})A\big) = L_k(A) + (\alpha - 1)\delta_{k,i}L_i(A)$.

$L_k(EA) = \begin{cases} L_i(A) + (\alpha - 1)L_i(A) = \alpha L_i(A) & \text{si } k = i \\ L_k(A) & \text{sinon} \end{cases}$ □

Proposition - Opération élémentaire en I_n

On considère une opération élémentaire, notée φ, qui transforme une matrice $A \in \mathcal{M}_{n,p}(\mathbb{K})$ en la matrice $\varphi(A) \in \mathcal{M}_{n,p}(\mathbb{K})$ et la matrice I_n en $\varphi(I_n)$.

Alors $\varphi(A) = \varphi(I_n) \times A$.

Et par récurrence, si $\varphi_1, \varphi_2, \ldots \varphi_k$ sont k transformations élémentaires (sur les lignes) qui s'appliquent à des matrices possèdant n lignes, alors, pour tout $A \in \mathcal{M}_{n,p}(\mathbb{K})$:

$[\varphi_k \circ \cdots \circ \varphi_1](A) = \varphi_k(I_n) \times \cdots \times \varphi_1(I_n) \times A$.

Démonstration

Cela a bien un sens de considérer que φ peut s'appliquer à A et à I_n, car il s'agit d'opération sur les lignes et A et I_n ont le même nombre de lignes.

Pour prouver ce résultat il suffit de vérifier que pour les trois transformations possibles on a bien $E = \varphi(I_n)$, puisque $\varphi(A) = EA$.

On démontre ensuite l'hérédité de la récurrence : Supposons que $\varphi_k \circ \cdots \circ \varphi_1(A) = \varphi_k(I_n) \times \cdots \times \varphi_1(I_n) \times A$.

Notons $A' = \varphi_k \circ \cdots \circ \varphi_1(A)$.

Alors

$$[\varphi_{k+1} \circ \varphi_k \circ \cdots \circ \varphi_1(A) = \varphi_{k+1}(\varphi_k \circ \cdots \varphi_1(A)) = \varphi_{k+1}(A') = \varphi_{k+1}(I_n) \times A' = \varphi_{k+1}(I_n) \times \varphi_k(I_n) \times \cdots \times \varphi_1(I_n) \times A$$

□

Cela se concrétise dans le savoir faire suivant

Savoir faire - Retenir les opérations matricielles codant les opérations élémentaires

Pour une opération sur les lignes de A, il s'agit toujours de produit à gauche de A.

(On verra pour les colonnes, il s'agit de produits à droites de A)

Par quelle matrice?

C'est toujours par la matrice qu'on obtient lorsqu'on applique la transformation élémentaire en question à I_n.

Ainsi, par exemple, si l'on veut faire $L_3 \leftarrow L_3 - 2L_2$, pour $n = 3$, on multiplie par la matrice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[L_3 \leftarrow L_3 - 2L_2]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix}$$

Proposition - Inversibilité des opérations élémentaires

Si une matrice B est déduite de A par une opération élémentaire φ, alors A peut se déduire de B par l'opération inverse φ^{-1} suivant le tableau suivant :

φ	φ^{-1}
$L_i \leftrightarrow L_j$	$L_i \leftrightarrow L_j$
$L_j \leftarrow L_j + \lambda L_i$	$L_j \leftarrow L_j - \lambda L_i$
$L_i \leftarrow \alpha L_i$	$L_i \leftarrow \frac{1}{\alpha} L_i$

Proposition - Inversibilité des matrices élémentaires
Si φ est une opération élémentaire sur les lignes alors la matrice carrée $\varphi(I_n)$ est inversible et $\varphi(I_n)^{-1} = \varphi^{-1}(I_n)$.
On a alors $P_{i,j}^{-1} = P_{i,j}$ (symétrique, involutif),
$\big(T_{i,j}(\lambda)\big)^{-1} = T_{i,j}(-\lambda)$, et $\big(D_i(\alpha)\big)^{-1} = D_i(\frac{1}{\alpha})$.

Démonstration
D'après la proposition précédente $\varphi^{-1}(I_n)\varphi(I_n) = \varphi^{-1}(\varphi(I_n)) = I_n$ □

5.2. Opérations élémentaires sur les colonnes d'une matrice

On définit les mêmes opérations élémentaires sur les colonnes que sur les lignes. On obtient alors les résultats suivants :

Proposition - Transformation élémentaire sur les colonnes comme un produit
Effectuer une transformation élémentaire sur les colonnes d'une matrice $A \in \mathcal{M}_{n,p}(\mathbb{K})$ revient à calculer le produit matriciel AF où F est l'une des matrices suivantes :
— Pour $C_i \leftrightarrow C_j$,
$$F = I_p - E_{ii} - E_{jj} + E_{ij} + E_{ji}$$
— Pour $C_i \leftarrow C_i + \lambda C_j$
$$F = I_p + \lambda E_{ji}$$
— Pour $C_i \leftarrow \alpha C_i$
$$F = I_p + (\alpha - 1)E_{ii}$$

Démonstration
Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $E_{ij} \in \mathcal{M}_p(\mathbb{K})$ une des matrices de la base canonique. Alors AE_{ij} est la matrice de $\mathcal{M}_{n,p}(\mathbb{K})$ dont toutes les colonnes sont nulles sauf la i-ième , qui est la j-ième colonne de A. $AI_p = A$ et en examinant chacune des opérations élémentaires on obtient le résultat. □

Proposition - Opération élémentaire en I_p
On considère une opération élémentaire, notée ψ, qui transforme une matrice $A \in \mathcal{M}_{n,p}(\mathbb{K})$ en la matrice $\psi(A) \in \mathcal{M}_{n,p}(\mathbb{K})$ et la matrice I_p en $\psi(I_p)$.
Alors $\psi(A) = A\psi(I_p)$.
Et par récurrence, si $\psi_1, \psi_2, \dots \psi_k$ sont k transformations élémentaires (sur les colonnes) qui s'appliquent à des matrices possédant p lignes, alors, pour tout $A \in \mathcal{M}_{n,p}(\mathbb{K})$:
$\psi_k \circ \cdots \circ \psi_1(A) = A \times \psi_1(I_p) \times \cdots \times \psi_k(I_p)$.

Démonstration
On démontre le résultat par récurrence :
$$\psi_{k+1}(\psi_k \circ \cdots \circ \psi_1)(A) = \psi_{k+1}(A') = A'\psi_{k+1}(I_p) = A \times \psi_1(I_p) \times \cdots \times \psi_k(I_p) \times \psi_{k+1}(A)$$
par hypothèse de récurrence. □

5.3. Méthode du pivot de Gauss pour obtenir l'inverse d'une matrice

Conservation de l'inversibilité

Histoire - Gauss et le calcul matriciel linéaire
Encore Gauss… Voir le cours d'arithmétique.

Proposition - Conservation de l'inversibilité
Soient $A, B \in \mathcal{M}_n(\mathbb{K})$. On suppose que A est inversible.
Alors AB est inversible si et seulement si B est inversible

Démonstration
Si B est inversible, alors AB est inversible (d'inverse $B^{-1}A^{-1}$).
Si AB est inversible, alors $B = A^{-1}(AB)$ est inversible (d'inverse $(AB)^{-1}A$) □

Corollaire - Conservation d'inversibilité par les opérations élémentaires
Les opérations élémentaires sur les lignes (ou sur les colonnes) d'une matrice carrée conservent le caractère inversible/non inversible d'une matrice.

Démonstration
Une opération élémentaire sur une matrice est un produit à gauche par une matrice inversible.
D'après le théorème précédent, on en déduit la conservation du critère d'inversibilité □

Critère d'inversibilité des matrices triangulaires (supérieures)

Analyse - Inversibilité d'une matrice triangulaire
Si $a_{n,n} \neq 0$, les opérations $\forall i \leqslant n-1, L_i \leftarrow L_i - \frac{a_{i,n}}{a_{nn}} L_n$ transforme

$$T = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix} \text{ en } T' = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n-1} & 0 \\ 0 & a_{22} & a_{23} & \cdots & a_{2,n-1} & 0 \\ 0 & 0 & a_{33} & \cdots & a_{3,n-1} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-1,n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

Notons que les opérations précédentes sont codés par des matrices $T_{n,i}(-\frac{a_{n,i}}{a_{n,n}})$, triangulaires supérieures, et dont le produit est également triangulaire supérieure.
On en déduit un résultat par récurrence (ou par algorithme).

Remarque - Ni dilatation, ni permutation
Là encore, à ce stade là, pour passer de la matrice T triangulaire supérieure à la matrice D diagonale (avec les mêmes coefficients sur la diagonale), on n'a pas utiliser de dilatation, seulement des transvections (il n'y a pas non plus de permutations).

Proposition - Inverse d'une matrice triangulaire supérieure
Si T est une matrice (carrée) triangulaire supérieure, avec des coefficients non nuls sur la diagonale.
Alors il existe T', triangulaire supérieure et inversible telle que $T' \times T = I_n$.
On a alors T inversible.

Histoire - Fang-cheng
« Cette méthode est connue des Chinois depuis au moins le Ier siècle de notre ère. Elle est référencée dans le livre chinois Jiuzhang suanshu (Les Neuf Chapitres sur l'art mathématique), dont elle constitue le huitième chapitre, sous le titre « Fang cheng » (la disposition rectangulaire). La méthode est présentée au moyen de dix-huit exercices. Dans son commentaire daté de 263, Liu Hui en attribue la paternité à Chang Ts'ang, chancelier de l'empereur de Chine au IIe siècle avant notre ère. » (pompage sans scrupule de Wikipedia…)

Démonstration
On va démontrer le résultat par récurrence sur n, l'ordre de la matrice T.
— Si $n = 1$, alors T' est la matrice à un élément : $\frac{1}{|T|_1}$.
— Soit $n \in \mathbb{N}$. Supposons le résultat vraie pour toute matrice triangulaire supérieure d'ordre n.
Soit T, triangulaire supérieure d'ordre $n+1$.
D'après l'analyse précédente, il existe T_1, triangulaire supérieure inversible telle que $T_1 \times T = \begin{pmatrix} \tilde{T} & 0_{n-1,1} \\ 0_{1,n-1} & {}^{n}|T|_n \end{pmatrix}$.
$\tilde{T}$ est l'extraction de T sur les n premières lignes et colonnes, elle est donc triangulaire supérieure, sans coefficient nul sur la diagonale.
On peut appliquer l'hypothèse de récurrence.

Il existe $\tilde{T}'$ triangulaire supérieure et inversible telle que $\tilde{T}' \times \tilde{T} = I_n$.

Considérons T_2, définie par blocs par : $\begin{pmatrix} \tilde{T}' & 0_{n-1,1} \\ 0_{1,n-1} & \frac{1}{\pi_{[T]_n}} \end{pmatrix}$, triangulaire supérieure.

On a alors (par blocs) :

$$T_2 \times T_1 \times T = \begin{pmatrix} \tilde{T}' & 0_{n-1,1} \\ 0_{1,n-1} & \frac{1}{\pi_{[T]_n}} \end{pmatrix} \times \begin{pmatrix} \tilde{T} & 0_{n-1,1} \\ 0_{1,n-1} & \pi_{[T]_n} \end{pmatrix} = \begin{pmatrix} \tilde{T}'\tilde{T} & 0_{n-1,1} \\ 0_{1,n-1} & 1 \end{pmatrix} = I_{n+1}$$

Et comme le produit de deux matrices triangulaires supérieures et inversible est triangulaire supérieure et inversible, l'hypothèse de récurrence est héréditaire.

Enfin, comme T' est inversible, en multipliant à gauche par T'^{-1}, on trouve $T = T'^{-1}$ et donc $T \times T' = I_n$ □

Proposition - Matrices triangulaires supérieures non inversible

Réciproquement, si T est une matrice (carrée) triangulaire supérieure, avec (au moins) un coefficients non nuls sur la diagonale, T n'est pas inversible.

Démonstration

Notons $h = \max\{i \mid {}^{i}[T]_i = 0\}$, ensemble non vide.

Alors pour tout $i > h$, ${}^{i}[T]_i \neq 0$, et en faisant $L_h \leftarrow L_h - \frac{{}^{h}[T]_{h+1}}{{}^{h+1}[T]_{h+1}} L_{h+1}$, on obtient une matrice T' avec ${}^{h}[T]_j = 0$, pour tout $j \leqslant h+1$.

Et on continue ainsi…

On trouve donc une matrice $\hat{T}$, triangulaire supérieure et inversible telle que $\hat{T} \times T$ possède la ligne h nulle.

Cette dernière matrice Z n'est pas inversible car $Z \times E_{h,h} = 0$.

C'est également le cas de T (puisque $\tilde{T}$ est non inversible).

□

Algorithme

Souvent, les démonstrations par récurrence, si elles sont constructives, permettent d'écrire un algorithme (récursif, en particulier). Comme toute matrice échelonnée est triangulaire supérieure, on peut **terminer** l'algorithme de Gauss :

Théorème - Transformation de Gauss-Jordan

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

A est inversible si et seulement s'il est possible de transformer A en une matrice triangulaire supérieure, sans 0 sur la diagonale, à l'aide uniquement d'opérations élémentaires portant sur les lignes.

Dans ce cas, on peut terminer la décomposition de A vers I_n par suite d'opérations élémentaires.

Si on applique alors à la matrice I_n les mêmes opérations élémentaires, dans le même ordre, on obtient A^{-1}.

Démonstration

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

Supposons que par une succession de k opérations élémentaires sur les lignes de A on obtienne une matrice triangulaire T, cela signifie

$$E_k E_{k-1} \dots E_1 A = T$$

En posant $Q = E_k E_{k-1} \dots E_1 \in \mathcal{M}_n(\mathbb{K})$, on obtient $QA = T$, donc $A = Q^{-1}T$.

Alors A est inversible si et seulement si T est inversible, c'est à dire T a des coefficients diagonaux tous non nuls.

Supposons que T soit inversible et que par une succession de $m-k$ nouvelles opérations élémentaires sur les lignes de A on obtienne la matrice I_n, cela signifie

$$E_m E_{m-1} \dots E_1 A = I_n$$

En posant $B = E_m E_{m-1} \dots E_1 \in \mathcal{M}_n(\mathbb{K})$, on obtient $BA = I_n$, A étant inversible, on a $BAA^{-1} = I_n A^{-1}$ d'où $B = A^{-1}$. Or $B = E_m E_{m-1} \dots E_1 = E_m E_{m-1} \dots E_1 I_n$ est la matrice déduite de I_n par la même succession des m opérations. □

Pour aller plus loin - Réussite de l'algorithme de Gauss - Conditionnement

Théoriquement, la question ne se pose pas : l'algorithme réussit toujours sa mission.

Mais dans la pratique, en particulier informatiquement, il peut y avoir des approximations numériques (par exemple à 2^{-52} près en Python).

Supposons donc la donnée de A avec une erreur à δA près.

On note (par exemple) $\|B\|_2 = \sqrt{(Tr(B^T \times B)}$, il s'agit d'une norme. Elle est de plus multiplicative : $\|AB\|_2 \leqslant \|A\|_2 \times \|B\|_2$.

On définit alors le conditionnement de A

$$cond(A) = \|A\|_2 \times \|A^{-1}\|_2$$

On a alors l'erreur relative à l'arrivée proportionnelle à l'erreur relative du départ par le conditionnement.

$$\frac{\|\delta A^{-1}\|_2}{\|A^{-1}\|_2} \leqslant cond(A) \frac{\|\delta A\|_2}{\|A\|_2}$$

On dit qu'une matrice est mal conditionnée si $cond(A)$ est important. Plus une matrice est mal conditionnée, plus l'impact d'une petite erreur au départ est important sur l'erreur finale.

Remarque - Et les colonnes

On peut également procéder à l'aide d'opérations élémentaires sur les colonnes puisque l'on aura alors $AF_1 \dots F_p = I_n$ d'où $A^{-1} = I_n F_1 \dots F_m$,

Attention - Surtout pas!

Mais en revanche il ne faut surtout **pas mélanger les deux types d'opérations** car l'on aboutit à $E_m E_{m-1} \dots E_1 A F_1 \dots F_p = I_n$ qui n'est pas de la forme $AB = I_n$ et ne permet pas de conclure à l'inversibilité de A.

Mais néanmoins, comme souvent, rien n'est perdu dans ce cas là : on montrera que A est équivalente à I_n, donc de même rang : n, donc elle est inversible…

Corollaire - Inversion à droite suffisante

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Supposons qu'il existe $B \in \mathcal{M}_n(\mathbb{K})$ tel que $AB = I_n$.

Alors A est inversible et $A^{-1} = B$.

(De même, B est inversible et $B^{-1} = A$)

Pour aller plus loin - Autres algorithmes

Il existe d'autre méthode (raffinement de Gauss) pour inverser une matrice. Elles ont une complexité algorithmique plus faible (on gagne sur la constante dans le O - ou mieux encore dans certains cas tout particulier de matrices). Il s'agit des méthodes LU, QR, Choleski. On peut aussi employer des méthodes itératives assez différentes dans leur philosophie comme les méthodes de Jacobi… On crée une suite de matrice (A_n), avec $A_0 = A$ et $\lim(A_n) = A^{-1}$. On s'arrête quand on est « assez proche » de A^{-1}.

Pour aller plus loin - Coût de l'algorithme de Gauss

Si l'on suit parfaitement la démarche de l'algorithme de Gauss, la complexité calculatoire est en $O(n^3)$ où n est l'ordre de la matrice considérée.

En effet, il faut mettre en place trois boucles imbriquées, indexée par n (pas tout à fait l'une est triangulaire).

Démonstration

On applique une série de transformations élémentaires à A pour l'échelonner.

$$\exists E_1, E_2, \dots E_k, T \text{ telles que } E_k E_{k-1} \cdots E_1 A = T$$

On a donc $TB = E_k E_{k-1} \cdots E_1$.

Puis en multipliant à droite par $E_1^{-1} \dots E_k^{-1}$, on a $T(B(E_k E_{k-1} \cdots E_1)^{-1}) = I_n$.

On a vu que si T avait un coefficient nul sur la diagonale, il est impossible d'obtenir I_n.

Donc T n'a aucun coefficient nul sur la diagonale, il est inversible.

Par produit de matrices inversibles : $A = (E_k E_{k-1} \cdots E_1)^{-1} T$ est inversible.

Et donc $B = A^{-1}AB = A^{-1}$. □

Savoir faire - Inversibilité et inverse d'une matrice par l'algorithme de Gauss

Calculer l'inverse de $A = \begin{pmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$.

On applique l'algorithme de Gauss-Jordan en considérant $(A|I_3)$:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & -1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 \end{array}\right) \quad \begin{cases} L_1 \leftarrow -L_3 \\ L_2 \leftarrow L_1 \\ L_3 \leftarrow L_2 \end{cases}$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 1 & 0 & 1 \\ 0 & -1 & 0 & 0 & 1 & 1 \end{array}\right) \quad \begin{cases} L_2 \leftarrow L_2 - L_1 \\ L_3 \leftarrow L_3 - L_1 \end{cases} \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & -1 & 0 & -1 \end{array}\right) \quad \begin{cases} L_2 \leftarrow \\ L_3 \leftarrow \end{cases}$$

Par suite d'opérations élémentaires, on a transformé A en I_3 donc A est inversible.

Par suite des mêmes opérations élémentaires, on a transformé I_3 en A^{-1},

donc $A^{-1} = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & -1 \\ -1 & 0 & -1 \end{pmatrix}$.

A retenir : **dans une opération élémentaire, il ne faut pas perdre l'information d'une ligne**. Autrement écrit, il faut toujours pouvoir revenir en arrière!!

Exercice

Calculer l'inverse de $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & -1 & -2 \\ 2 & 2 & 5 \end{pmatrix}$.

Correction

On applique l'algorithme de Gauss-Jordan en considérant $(A|I_3)$:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ -1 & -1 & -2 & 0 & 1 & 0 \\ 2 & 2 & 5 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & -2 & -1 & -2 & 0 & 1 \end{array}\right) \quad \begin{cases} L_2 \leftarrow L_1 + L_2 \\ L_3 \leftarrow L_3 - 2L_1 \end{cases}$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{array}\right) \quad \left\{ L_3 \leftarrow L_3 + 2L_2 \right. \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & -4 & -1 \\ 0 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{array}\right) \quad \left\{ \begin{array}{l} L_1 \leftarrow L_1 - 2L_2 - L_3 \\ L_2 \leftarrow L_2 - L_3 \end{array} \right.$$

Par suite d'opérations élémentaires, on a transformé A en I_3 donc A est inversible.
Par suite des mêmes opérations élémentaires, on a transformé I_3 en A^{-1}, donc $A^{-1} = \begin{pmatrix} -1 & -4 & -1 \\ 1 & -1 & -1 \\ 0 & 2 & 1 \end{pmatrix}$.

Remarque - Et si A n'est pas inversible?

Si A n'est pas inversible, alors l'algorithme conduit à une matrice échelonné (triangulaire supérieure) dont la diagonale possède (au moins) un zéro. Il est alors totalement impossible d'obtenir I_n.
Nous verrons plus loin que l'algorithme donne alors une nouvelle information à propos de la matrice A : son rang!

Exercice

Déterminer les inverses de

$$A = \begin{pmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ -2 & -3 & 5 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 10 & 9 & 1 \\ 9 & 10 & 5 \\ 1 & 5 & 9 \end{pmatrix}, D = \begin{pmatrix} 1 & 2 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 2 & 1 & 3 & -1 \\ 1 & 1 & 2 & 1 \end{pmatrix}$$

Correction

On applique l'algorithme de Gauss-Jordan en considérant $(A|I_3)$:

$$\left(\begin{array}{ccc|ccc} 2 & 1 & -2 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 & 1 & 0 \\ -2 & -3 & 5 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} 2 & 1 & -2 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 & 1 & 0 \\ 0 & -2 & 3 & 1 & 0 & 1 \end{array}\right) \quad \left\{ L_3 \leftarrow L_3 + L_1 \right.$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & \frac{1}{2} & -1 & \frac{1}{2} & 0 & 0 \\ 0 & 3 & 1 & 0 & 1 & 0 \\ 0 & 0 & \frac{11}{3} & 1 & \frac{2}{3} & 1 \end{array}\right) \quad \left\{ \begin{array}{l} L_1 \leftarrow \frac{1}{2}L_1 \\ L_3 \leftarrow L_3 + \frac{2}{3}L_2 \end{array} \right.$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & \frac{1}{2} & -1 & \frac{1}{2} & 0 & 0 \\ 0 & 1 & \frac{1}{3} & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 1 & \frac{3}{11} & \frac{2}{11} & \frac{3}{11} \end{array}\right) \quad \left\{ \begin{array}{l} L_2 \leftarrow \frac{1}{3}L_2 \\ L_3 \leftarrow -\frac{3}{11}L_3 \end{array} \right.$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & \frac{1}{2} & -1 & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 & \frac{-1}{11} & \frac{3}{11} & \frac{-1}{11} \\ 0 & 0 & 1 & \frac{3}{11} & \frac{2}{11} & \frac{3}{11} \end{array}\right) \quad \left\{ L_2 \leftarrow L_2 - \frac{1}{3}L_3 \right.$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{9}{11} & \frac{1}{22} & \frac{7}{22} \\ 0 & 1 & 0 & \frac{-1}{11} & \frac{3}{4} & \frac{-1}{11} \\ 0 & 0 & 1 & \frac{3}{11} & \frac{2}{11} & \frac{3}{11} \end{array}\right) \quad \left\{ L_1 \leftarrow L_1 - \frac{1}{2}L_2 + L_3 \right.$$

Par suite d'opérations élémentaires, on a transformé A en I_3 donc A est inversible.
Par suite des mêmes opérations élémentaires, on a transformé I_3 en A^{-1}, donc $A^{-1} = \frac{1}{22}\begin{pmatrix} 18 & 1 & 7 \\ -2 & 6 & -2 \\ 6 & 4 & 6 \end{pmatrix}$.

$C^{-1} = \begin{pmatrix} 65 & -76 & 35 \\ -76 & 89 & -41 \\ 35 & -41 & 19 \end{pmatrix}$ et $D^{-1} = \frac{1}{7}\begin{pmatrix} 8 & 9 & -3 & -4 \\ 3 & -1 & -2 & 2 \\ -6 & -5 & 4 & 3 \\ 1 & 2 & -3 & 3 \end{pmatrix}$

6. Bilan

Synthèse

⇝ Les problèmes à double entrées se codent dans des tableaux. Ces problèmes s'articulent lorsqu'ils ont une entrée commune ; cela se code par la multiplication des tableaux. Nous avons ainsi défini des opérations sur les tableaux (à taille fixée), donnant une structure d'anneau et d'espace vectoriel à cet ensemble (lorsque les dimensions correspondent bien). Attention c'est un anneau non commutatif, avec des diviseurs de zéros…

⇝ Un espace est particulièrement intéressant, celui des matrices de taille carrée, car dans cette situation, elles codifient les transformations d'un

espace sur lui-même. Cas très fréquent.
Pour ces matrices, on peut être amené à étudier leurs puissances A^n (cf. Sciences physiques). Mais ici on se concentre surtout sur l'étude de l'inversibilité de A et le calcul de A^{-1} si possible.

⇝ On met en place un algorithme pour répondre à ces questions. C'est un algorithme sur les matrices, mais qui se code aussi par du calcul matriciel. Ainsi on voit les matrices (ou plutôt des ensembles de matrices) agir sur les matrices (ou plutôt d'autres ensembles de matrices). Cela nous donne l'idée de considérer des actions de groupes $GL_n(\mathbb{K})$ (groupe des matrices carrées de taille n, inversibles) sur tout plein d'ensembles.
En exploitant cette idée, on dégage la notion de rang d'une matrice ; il est invariant par produit par matrices inversibles à droite et à gauche et on trouve une forme normalisée adaptée (pour la relation d'équivalence qui conserve le rang). Cette méthode est exploitée similairement dans plein d'autres parties des mathématiques (matrices congruentes, matrices semblables…)

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Notations
- Savoir-faire - Notation et multiplication matricielle
- Savoir-faire - Présentation des calculs
- Savoir-faire - Exploiter un polynôme annulateur pour trouver M^{-1}
- Savoir-faire - Exploiter un polynôme annulateur pour trouver M^n
- Savoir-faire - Montrer qu'une matrice est triangulaire supérieure
- Savoir-faire - Retenir les opérations matricielles codant les transformations élémentaires.
- Savoir-faire - Inversibilité et inverse d'une matrice par algorithme de Gauss

Notations

Notations	*Définitions*	*Propriétés*	*Remarq*
$\mathcal{M}_{n,k}(\mathbb{K})$	Ensemble (espace) des matrices avec n lignes et p colonnes à coefficients dans $\mathbb{K}$		On note
$\mathcal{S}_n(\mathbb{K})$, resp. $\mathcal{A}_n(\mathbb{K})$	Ensemble (espace) des matrices symétrique (nécessairement carrées), resp. antisymétrique	$A^T = A$, resp. $A^T = -A$	
$GL_n(\mathbb{K})$	Groupe (linéaire) des matrices carrées d'ordre n inversible		
${}^i[A]_j$ ou $[A]_{i,j}$ ou $\text{Coeff}_{i,j}(A)$	Coefficient en ligne i et colonne j de la matrice A	C'est une application linéaire	${}^i[AB]_j$:
${}^tA$ ou A^T	Transposée de la matrice A	${}^i[A^T]_j = {}^j[A]_i$	Applica
A^n, A^{-1}	Puissance n^e de A (par récurrence). Inverse de A (si inversible)		
$\text{Tr}(A)$	Trace de A (somme des coeff. sur la diagonale)	$\text{Tr}(A) = \sum_{i=1}^{n} {}^i[A]_i$	$\text{Tr}(AB)$:
$(E_{i,j})_{i,j}$	Base canonique de $\mathcal{M}_{n,p}(\mathbb{K})$	${}^h[E_{i,j}]_k = \delta_{i,h}\delta_{j,k}$	$E_{i,j} \times E$
$P_{i,j} = I_n + E_{i,j} + E_{j,i} - E_{i,i} - E_{j,j}$	Matrice de transposition	Inversion des lignes (resp. colonnes) i et j si multiplication par la gauche (resp. la droite)	$P_{i,j}^{-1} = P$
$T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$	Matrice de transvection	$L_i \leftarrow L_i + \lambda L_j$ à gauche (resp. $C_j \rightarrow C_j + \lambda C_i$ - à droite)	$T_{i,j}(\lambda)^-$
$D_i(\alpha) = I_n + (\alpha - 1)E_{i,i}$	Matrice de dilatation	$L_i \leftarrow \alpha L_i$ à gauche (resp. $C_i \rightarrow \alpha C_i$ - à droite)	$D_i(\alpha)^{-1}$
$J_r(n,p) = \begin{pmatrix} I_r & O_{r,p-r} \\ O_{n-r,r} & O_{n-r,p-r} \end{pmatrix}$	Matrice J_r	$\text{rg}(A) = r \iff \exists P,Q \in GL_n(\mathbb{K}) \times GL_p(\mathbb{K})$ tel que $A = P \times J_r \times Q$	

Retour sur les problèmes

42. Addition naturelle des éléments de mêmes caractéristiques (donc situés dans une même case)

43. L'interprétation en terme de graphes qui figure dans la marge donne des éléments de réponse à ce problème.
$[A]_{ij}$ est le coefficient de dépendance de la moyenne de l'élève i par rapport à la note j.
$[B]_{j,k}$ est le poids de la partie k dans la note j.
Alors $[AB]_{i,k}$ est le coefficient de dépendance de la moyenne de l'élève i par rapport aux parties k.

44. La matrice de la question n'admet aucune racine. On démontre qu'on devrait la chercher parmi les matrices triangulaires avec des zéros sur la diagonale : $a = \begin{pmatrix} 0 & \alpha & \beta \\ 0 & 0 & \gamma \\ 0 & 0 & 0 \end{pmatrix}$.
On a alors $a^2 = \begin{pmatrix} 0 & & \alpha\gamma \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Il n'y a pas de racine.
En revanche, le même calcul montre que pour tout $\alpha \in \mathbb{R}^*$ et $\beta \in \mathbb{R}$, $a = \begin{pmatrix} 0 & \alpha & \beta \\ 0 & 0 & \frac{1}{\alpha} \\ 0 & 0 & 0 \end{pmatrix}$ est une racine de $a = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, qui admet donc une double infinité de racines…

45. L'anneau des matrices n'est pas commutatif, les éléments ne sont pas tous inversibles ni régulier. Il y a des diviseurs de 0.
Les seules matrices qui commutent avec toutes les matrices sont les λI_n.
($AE_{i,j} = \sum_k [A]_{k,i} E_{k,j}$ et $E_{i,j} A = \sum_{\mathbb{K}} [A]_{j,k} E_{i,k} \Rightarrow [A]_{i,j} = 0$ si i $\neq j$ et $[A]_{i,i} = [A]_{j,j}$)
Essentiellement (à peu de choses près…) si B commute avec A, alors il existe $P \in \mathbb{K}[X]$ tel que $B = P(A)$…

46. Oui si A n'est pas inversibles, alors $\mathrm{Ker}(A) \neq \emptyset$. Il existe une colonne X tel que $AX = 0$.
Si $B = (X|X|\cdots|X)$ alors $AB = 0$.
Pour étudier l'inversibilité de A, on peut étudier son noyau. On peut aussi exploiter la méthode de Gauss-Jordan.

47. Voir cours.

Deuxième partie

Logique ensembliste

Chapitre 10

Structure logique

Résumé -

En mathématiques, on s'intéresse à des objets sur lesquelles on formule des assertions. Si, partant des axiomes ou des définitions on peut, en respectant des règles logiques, démontrer qu'une assertion est vraie, elle prend alors le nom de théoréme (avec un certain nombre de variantes sur ce nom : proposition (résultat considéré comme un peu moins important qu'un théorème), lemme *(résultat qui est avant tout une étape intermédiaire pour arriver au résultat final),* corollaire *(conséquence plus ou moins immédiate d'un résultat précédemment démontré).*
Le but de l'activité mathématique est de prouver de nouveaux résultats. Pour éviter les erreurs, il faut : du bon sens (i.e. de la logique), de la méthode, de la rigueur.
Quelques vidéos de youtubers :

— *Canal unisciel - Logique et raisonnement -*

Sommaire

1. Cours mathématiques 196
1.1. L'énigme mathématique 196
1.2. Structure de cours 196
2. Quantificateurs et notations ensemblistes 197
2.1. Appartenance, éléments 197
2.2. Différentes manières d'écrire un ensemble 198
2.3. Utilisation de quantificateurs 200
2.4. Parties d'un ensemble 201
2.5. Produit cartésien 202
2.6. Opérations sur les ensembles 202
3. Vocabulaire sur les assertions 203
3.1. Définitions 203
3.2. Négation 204
3.3. Implications et équivalence d'assertions 205
4. Principales méthodes de démonstration 206
4.1. Démonstration d'une implication 206
4.2. Démonstration d'une équivalence 209
4.3. Raisonnement par l'absurde 210
4.4. Conditions nécessaire, suffisante 211
4.5. Exploiter un contre-exemple dans une démonstration 212
4.6. Démonstration par récurrence 212
4.7. Démonstration par algorithme 214
5. Bilan 217

1. Cours mathématiques

1.1. L'énigme mathématique

Pas de réponse, que des questions. Extrait de « l'efficacité des mathématiques est-elle déraisonnable » de D. Lambert.

? Problème 47 - Déraisonnable efficacité des mathématiques

Le développement des sciences physiques contemporaines a clairement manifesté l'efficacité surprenante des mathématiques. Dans un article souvent cité, E. P. Wigner parle à ce propos d'une « efficacité déraisonnable », d'une sorte de « miracle » qui est comme un « don magnifique que nous ne comprenons ni ne méritons ». Einstein lui-même manifeste son étonnement à cet égard ? : « Comment est-il possible que la mathématique, qui est un produit de la pensée humaine et indépendante de toute expérience, puisse s'adapter d'une si admirable manière aux objets de la réalité ? La raison humaine serait-elle capable, sans avoir recours à l'expérience, de découvrir par la pensée seule les propriétés des objets réels » ? Aujourd'hui cet étonnement est encore renforcé par les confirmations expérimentales très précises apportées à la mécanique quantique, à l'électrodynamique quantique, à la théorie unifiée des interactions électro-faibles (qui a permis la découverte effective des bosons vectoriels intermédiaires) ou encore à la théorie cosmologique standard (grâce aux mesures effectuées par le satellite COBE par exemple). De plus, cette efficacité se manifeste également, quoique de manière plus discrète, dans d'autres domaines des sciences. En biologie, par exemple, les mathématiques apportent des résultats surprenants au niveau de la compréhension des dynamiques de populations en écologie. . .

? Problème 48 - Un simple langage ? Ou plus

Les mathématiques sont-elles un langage ? Est-ce un jeu ? Un aperçu sur la/une vérité ? Autre chose. . .

? Problème 49 - Inspiration. . .

Les deux sources d'inspiration pour les mathématiques jusqu'au XXème siècle sont la physique dans sa globalité (mécanique, électricité, chimie. . .) et l'arithmétique (le calcul avec des nombres entiers). La géométrie a été aussi d'une certaine façon une source d'inspiration.
Il est donc nécessaire en filière mathématique d'étudier la physique et l'arithmétique. . .
La biologie et l'informatique (quoi que pour cette dernière, il est parfois compliqué de démêler informatique et mathématiques) sont de nouvelles sources d'inspiration. . .

1.2. Structure de cours

Analyse - Formalisation

Le cours se construit d'une façon systématique. La chronologie est importante.

1. Quelques axiomes : des résultats de base admis, sans démonstration, sur un *bon sens* commun.
2. A partir de ces axiomes, on développe des idées, des mots, des images mentales et des heuristiques.
   Ces images permettent de bien comprendre mais pas ne permettent pas les

démonstrations.
Une heuristique, c'est l'art de trouver, de découvrir. En pédagogie : l'adjectif heuristique signifie : « Qui consiste à faire découvrir par l'élève ce qu'on veut lui enseigner ».

3. Il faut formaliser les idées pour pouvoir agir dessus : on donne donc des définitions précises avec un langage très précis, mais finalement assez restreint. Une définition, c'est une *légalisation* d'une idée.
4. La manipulation des définitions pour créer des théorèmes ou propositions (moins importantes qu'un théorème, ou étape intermédiaire), des corollaires (résultats immédiats), des lemmes (propositions pour des démonstrations).
5. Les démonstrations sont les étapes intermédiaires entre définitions et propositions ou entre propositions et théorèmes. C'est l'essentiel de notre cours !
6. Pour bien comprendre et apprendre à manipuler les mathématiques, nous aurons beaucoup d'exercices d'applications, de moments d'analyse, des devoirs (maisons ou surveillés) et des colles évidemment !

Exercice
Pour ces six étapes, donner un pourcentage du temps passé en cours de mathématiques pendant le lycée ?
Reprendre l'exercice en fin d'année pour évaluer le cours de CPGE.

Correction

2. Quantificateurs et notations ensemblistes

2.1. Appartenance, éléments

Définition - Ensemble
Un ensemble est une "collection" d'objets appelés *éléments*. On introduit une relation particulière entre un élément x et un ensemble E, la *relation d'appartenance* :

$x \in E$, ce qui se lit "x appartient à E" ou "x est un élément de E.

La négation de la relation d'appartenance s'écrit $x \notin E$, ce qui signifie que $x \in E$ est faux.

Pour aller plus loin - Propriété essentielle, sinon, c'est la faillite…
Trés vite dans la théorie des ensembles sont apparus quelques paradoxes, ce qui a demandé de faire une théorie plus fine. Ici, on reste au stade naïf, car cela demanderait beaucoup de temps et il serait assez peu productif de prendre ce temps.
La contradiction est de cette forme (en notant catalogue ou lieu d'ensemble) : « Peut-on faire un catalogue des catalogues qui ne se citent pas ? »

Proposition - Propriété essentielle
Un ensemble est défini dés que pour tout objet x, on **peut dire** si x est, ou n'est pas, un élément de cet ensemble.

Définition - Formalisation
On formalise les idées et objets pour signifier un certain type d'appartenance par :
$\forall x$, qui se lit « quel que soit x » ou pour « pour tout x »,
$\exists x$ se lit « il existe x »,
$\exists! x$ se lit « il existe un unique x »,

Attention - Pas d'abus
On n'abuse pas de ce formalisme dans un texte en français.
Seul un « $x \in E$ » peut être toléré.

Exemple - Applications
Par exemple,
$\forall x \in E$ se lit « quel que soit x appartenant à E », « quel que soit l'élément x de E » , ou encore « pour tout élément x de l'ensemble E »...
De plus si $P(x)$ désigne une propriété dépendant de x,
$\forall x \in E, P(x)$ se lit « pour tout x de E, la propriété P de x… »

et $\exists x \in E | P(x)$ (ou $\exists x \in E; P(x)$) se lit « il existe x dans E tel que la propriété P de x… »

Exemple - Ensembles classiques
Les plus connus : $\mathbb{N}$ (dont les éléments sont appelés "entiers naturels"), $\mathbb{Z}$ ("entiers relatifs"), $\mathbb{Q}$ ("nombres rationnels"), $\mathbb{R}$ ("nombres réels"), $\mathbb{C}$ ("nombres complexes"), mais également l'ensemble des élèves de la classe, l'ensemble des professeurs de la classe, l'ensemble des aliments contenus dans le frigo de la cuisine de vos parents...
Exercice
Que pensez-vous de l'affirmation suivante ?
On a donc

$$\forall x \in \mathbb{R}, x^2 \neq -1 \text{ mais } \exists x \in \mathbb{C} \mid x^2 = -1$$

Correction
Remarquez la négation du $\exists \ldots$

Histoire - Asse
Depuis la fin du
matique s'appui
Le premier a les
1918).



On commence
lant de cette th
mathématicien
nous exclure du

Remarque - Convention de notation
La lettre x peut être remplacée par n'importe quel autre symbole, bien que quelques conventions tacites existent en mathématiques (parfois différentes de la physique) : $n, m, p, i, j, k, \ell, \ldots$ pour des entiers, $x, y, z, s, t, \theta, \epsilon, \ldots$ pour des réels, z pour un complexe...

Proposition - Règle de la théorie des ensembles
Quelques régles régissent les ensembles (dont certaines sont des axiomes de la théorie des ensembles) :
— régle n°1 : Deux ensembles qui ont les mêmes éléments sont égaux.
— régle n°2 : Il existe un ensemble qui n'admet aucun élément, soit

$$\exists E | \forall x, x \notin E$$

D'après la règle n°1, cet ensemble est unique, on l'appelle *ensemble vide* et on le note $\emptyset$.

2.2. Différentes manières d'écrire un ensemble

Descriptions : en extension, en compréhension, par image

Définition - Singleton, paire
Soit a un objet mathématique. L'ensemble dont a est l'unique élément s'appelle un singleton, on le note $\{a\}$.
Soient a et b deux objets distincts. L'ensemble dont ce sont les deux seuls éléments s'appelle la paire formée de a et b. On le note $\{a, b\}$

D'aprés la régle n°1, $\{a, b\} = \{b, a\}$, qu'il ne faut pas confondre avec le couple (a, b).
Si $a = b$, $\{a, b\} = \{a\}$.

Définition - Définition en extension
On dit que l'on définit un ensemble en extension lorsque l'on énumère ses éléments :

$$\{a_1, a_2, \dots, a_n\}$$

Cette notation sous-entend que l'on sait interpréter les … intermédiaires.

Exemple - Ensemble défini en extension
$\{1,2,\dots,n\}$ représente l'ensemble des entiers compris entre 1 et n, on le note parfois aussi $[\![1,n]\!]$.
$\{0,2,\dots,2n\}$ est l'ensemble des entiers de la forme $2k$ où k varie de 0 à n.
Par abus courant, la même notation s'emploie pour énumérer des ensembles infinis, comme
$\mathbb{N} = \{0,1,2,\dots\}$ ou $2\mathbb{N} = \{0,2,4,\dots\}$.
Exercice
$\{1,2,3,\dots\} =$, $\{0,1,-1,2,-2,\dots\} =$

Correction
$\{1,2,3,\dots\} = \mathbb{N}$, $\{0,1,-1,2,-2,\dots\} = \mathbb{Z}$

Définition - Définition en compréhension
On peut définir un ensemble en compréhension, c'est à dire par l'intermédiaire d'une propriété qui le caractérise : soit E un ensemble et $P(x)$ une propriété dépendant d'un objet x de E, alors

$$\{x \in E \mid P(x)\}$$

est l'ensemble des x éléments de E tels que $P(x)$ (sous-entendu "tels que $P(x)$ soit vraie").

Pour aller plus loin - Définition par image
On peut définir un ensemble par image, c'est à dire par l'intermédiaire d'une application qui le caractérise : soit E un ensemble et $f : E \to F$ et enfin $A \subset E$.
Alors

$$f(A) = \{f(x), x \in A\}$$

est le sous-ensemble de F dont les éléments sont des images d'éléments de A par f.

Exercice
$\{x \in \mathbb{R} | x^2 + 1 = 0\} =$
$\{x \in \mathbb{N} | x + 1 = 0\} =$
$\{x \in \mathbb{C} | x^2 + 1 = 0\} =$
$\{x \in \mathbb{Z} | x + 1 = 0\} =$
$\{a^2 + 2 | a \in [\![1,5]\!]\} =$

Correction
$\{x \in \mathbb{R} | x^2 + 1 = 0\} = \emptyset$
$\{x \in \mathbb{N} | x + 1 = 0\} = \emptyset$
$\{x \in \mathbb{C} | x^2 + 1 = 0\} = \{-i, i\}$
$\{x \in \mathbb{Z} | x + 1 = 0\} = \{-1\}$
$\{a^2 + 2 | a \in [\![1,5]\!]\} = \{3,6,11,18,27\}$

Le dernier ensemble de cet exercice est un exemple d'ensemble défini comme image.

Intervalle de $\mathbb{R}$

Définition - Intervalles de $\mathbb{R}$
Pour $a, b \in \mathbb{R}$, $a < b$, on définit les *intervalles* de $\mathbb{R}$, ce sont les ensembles suivants :

$[a,b] = \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$ $]a,b] = \{x \in \mathbb{R} \mid a < x \leqslant b\}$ $[a,b[,]a,b[\dots$
$]-\infty,a] = \{x \in \mathbb{R} \mid x \leqslant a\}$ $]-\infty,a[= \{x \in \mathbb{R} \mid x < a\}$ $[b,+\infty[,]b,+\infty[\dots$

Les intervalles du type $[a,b],]-\infty,a], [b,+\infty[$ sont des *intervalles fermés*
Les intervalles du type $]a,b[,]-\infty,a[,]b,+\infty[$ sont des *intervalles ouverts*
Les intervalles du type $[a,b[$ ou $]a,b]$ sont dits *semi-ouverts (ou semi-fermés)*
$[a,b]$ s'appelle un *segment.*

Pour aller plus loin - Motivations
Il y a d'autres motivations.
Nous verrons plus loin l'articulation forte entre ces deux quantificateurs, en particulier pour la négation.
Nous verrons encore plus l'articulation très forte entre ces connecteurs et les opérations ensemblistes $\bigcap_{i\in I} A_i$ et $\bigcup_{i\in I} A_i$

Exemple - Autres exemples
$\emptyset =]0,0[$
$\mathbb{R}_- =]-\infty,0]$, $\mathbb{R}_-^* =]-\infty,0[$, $\mathbb{R}_+ = [0,+\infty[$, $\mathbb{R}_+^* =]0,+\infty[$ (on trouve aussi les notations $\mathbb{R}^+, \mathbb{R}^{+*}$...)

Savoir faire - Montrer que I est un intervalle de $\mathbb{R}$
Il suffit de montrer que pour tout $a, b \in I$, $[a,b] := \{t \in \mathbb{R} \mid a \leqslant t \leqslant b\} \subset I$.
C'est-à-dire :
« Soient $a, b \in I$ (quelconques puis fixés).
Soit $t \in [a,b]$ (i.e. $a \leqslant t \leqslant b$) alors…… et donc $t \in I$. »

Exercice
Montrer que $J = \{x \in \mathbb{R} \mid 1 \leqslant x + e^x \leqslant 10\}$ est un intervalle.

Correction
Soient $a, b \in J$. Soit $t \in [a,b]$.
Notons $\varphi : x \mapsto x + e^x$, croissante comme addition de deux fonctions croissantes.
Alors $a \leqslant t \leqslant b \Rightarrow \underbrace{1 \leqslant \varphi(a)}_{a\in J} \leqslant t + e^t \leqslant \underbrace{\varphi(b) \leqslant 10}_{b\in J}$

2.3. Utilisation de quantificateurs

Heuristique - Quantificateurs nécessaires
En mathématiques classiques, deux quantificateurs sont essentiels :
— $\forall$, lu « pour tout » ou « quel que soit », pour désigner qu'une propriété a un certain degré d'universalité :
$\forall\, x, \mathscr{P}(x)$. La propriété $\mathscr{P}$ est donc toujours vraie, puisque vraie pour tout point.
$\forall\, x \in E, x \in F$. Tous les éléments de E sont dans F. Dans sa totalité : $E \subset F$.
— $\exists$ lu « il existe » est la négation du précédent.

Remarque - Existence ET unicité
Il arrive qu'on ait besoin d'ajouter l'unicité à l'existence (cas des antécédents pour une fonction bijective…).
On écrit alors : $\exists\,!x$, pour dire « il existe un unique x qui… »

Analyse - Non commutativité des connecteurs
Les deux assertions suivantes ne sont pas identiques :

$$\forall\, x, \exists\, y \dots \qquad \exists\, y, \forall\, x \dots$$

L'une est plus forte que l'autre : la seconde. Pour la seconde assertion, il s'agit du même y pour tous les x. Dans la première assertion, chaque y dépend de chaque x.

Exemple - Suite majorée, ou rien
$\forall\, n \in \mathbb{N}, \exists\, M \in \mathbb{R}$ tel que $u_n \leqslant M$ est toujours vraie. Comme M peut dépendre de n, on peut prendre $M_n = x_n + 1$
$\exists\, M \in \mathbb{R}$ tel que $\forall\, n \in \mathbb{N}, u_n \leqslant M$ signifie qu'une suite est majorée. Ce n'est pas toujours vraie (ex : $(u_n) = (n)$).
Exercice
On considère la suite de FIBONACCI : $F_{n+2} = F_{n+1} + F_n$ et $F_0 = F_1 = 1$.
Que pensez-vous des deux assertions suivantes :
— $\forall\, n \in \mathbb{N}, \exists\, A, B \in \mathbb{R}$ tels que $F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$
— $\exists\, A, B \in \mathbb{R}$ tels que $\forall\, n \in \mathbb{N}, F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$

Correction
Le première est sans intérêt cela est toujours vrai. Il suffit de prendre $B_n = 0$ et $A_n = \frac{F_n}{\left(\frac{1+\sqrt{5}}{2}\right)^n}$.
La seconde est tout à fait intéressante, voire incroyable !

Savoir faire - Noter les dépendances

Si l'on écrit $\forall\ a, \exists\ b\ldots$, le nombre b en second dépend grandement de a. On devrait noter $b(a)$ ou b_a.
En revanche, si on écrit $\exists\ b$ tel que $\forall\ a\ldots$, le nombre a ne dépend pas (plus particulièrement que les autres) de b. La notation a_b ou $a(b)$ n'aurait pas d'intérêt. Rappelons que cette formulation est la plus forte.
De nombreux problèmes rencontrés en mathématiques en MPSI par les élèves reposent sur la non compréhension de cette (in)dépendance.

Une autre stratégie est de faire comme en Python, des indentations dans la démonstration.
A chaque paramètre introduit, on fait apparaître un petit retrait dans l'écriture de la démonstration qui permet de voir comme ces paramètres dépendent mutuellement les uns des autres…

2.4. Parties d'un ensemble

Définition - Partie d'un ensemble (sous ensemble)

On dit qu'un ensemble F est inclus dans un ensemble E, ce que l'on note $F \subset E$, si tous les éléments de F sont éléments de E.
On dit aussi que F est une partie ou un sous-ensemble de E.

Savoir faire - Montrer que $F \subset E$

Pour montrer que $F \subset E$, on démontre :
$$F \subset E \Leftrightarrow (\forall x, x \in F \Rightarrow x \in E).$$

Proposition - Relation d'ordre

Quelques propriétés :
- $\emptyset \subset E$ pour tout ensemble E
- $E \subset E$ (l'inclusion est une relation réflexive)
- Si on a $E \subset F$ et $F \subset G$ alors on a aussi $E \subset G$ (l'inclusion est une relation transitive)
- Si on a $E \subset F$ et $F \subset E$ alors $E = F$ (l'inclusion est une relation antisymétrique)

Savoir faire - Prouver l'égalité de deux ensembles

La dernière propriété sert souvent à prouver l'égalité de deux ensembles.

Exercice

A quelle condition a-t-on : $\{a\} \subset E$? $\{a,b\} \subset E$? $\{a\} \subset \{b\}$?

Correction

$\{a\} \subset E$ ssi $a \in E$ $\quad$ $\{a,b\} \subset E$ ssi $a, b \in E$ $\quad$ $\{a\} \subset \{b\}$ ssi $a = b$ ssi $\{a\} = \{b\}$

Définition - Ensemble des partes de E

$\mathscr{P}(E)$ est l'ensemble des parties de E : $X \in \mathscr{P}(E)$ signifie donc à $X \subset E$.

Exemple - Singleton…

$\mathscr{P}(\{a\}) = \{\emptyset, \{a\}\}$
$\mathscr{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$
$\mathscr{P}(\emptyset) = \{\emptyset\}$
$\mathscr{P}(\mathscr{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

2.5. Produit cartésien

Définition - Produit cartésien de deux ensembles

Soient E et F deux ensembles. On appelle produit cartésien de E et F, et on note $E \times F$, l'ensemble dont les éléments sont les couples formés d'un élément de E et d'un élément de F (dans cet ordre) :
$$E \times F = \{x | \exists a \in E, \exists b \in F;\ x = (a,b)\} = \{(a,b) | a \in E \text{ et } b \in F\}.$$

Remarque - Rôle de la ponctuation

Le " ;" dans la définition en compréhension peut être remplacé par " :", "tels que".
Plus généralement,

Définition - Produit cartésien de n ensembles

Soit $n \in \mathbb{N}$, si $E_1, \ldots, E_n$ sont n ensembles, on définit le produit cartésien $E_1 \times \cdots \times E_n$ comme l'ensemble des n-uplets $(a_1, \ldots, a_n)$ formés d'éléments $a_1 \in E_1, \ldots, a_n \in E_n$.
Si les E_i désignent un même ensemble E, on note $E_1 \times \cdots \times E_n = E^n$ ($\mathbb{R}^2, \mathbb{R}^3$…)

Remarque - Associativité du produit cartésien

A priori $E \times (F \times G) \neq (E \times F) \times G$, mais on les identifie fréquemment à $E \times F \times G$.

2.6. Opérations sur les ensembles

Définition - Réunion, intersection, différence d'ensembles

Pour E et F deux ensembles on définit :
- la réunion (ou union) de E et F : $E \cup F = \{x | x \in E \text{ ou } x \in F\}$ (le "ou" est inclusif : on peut avoir les deux simultanément)
- l'intersection de E et F : $E \cap F = \{x | x \in E \text{ et } x \in F\}$
- la différence de E et de F : $E \setminus F = \{x | x \in E \text{ et } x \notin F\}$

Remarque - Interprétation avec une table de vérité

En d'autres termes on a :

$x \in E$	$x \in F$	$x \in E \cup F$	$x \in E \cap F$	$x \in E \setminus F$
V	V	V	V	F
V	F	V	F	V
F	V	V	F	F
F	F	F	F	F

Définition - Complémentaire d'un ensemble (dans un ensemble plus gros)

Lorsque $F \subset E$, l'ensemble $E \setminus F$ est appelé *complémentaire* de F dans E et noté $\complement_E F$.
On ne peut parler de complémentaire de l'ensemble F que relativement à un ensemble "contenant" ce dernier. Toutefois, en l'absence d'ambiguïté sur E, on peut noter $\complement F$ ou F^c ou $\overline{F}$ (cette dernière notation ayant cependant différents sens suivant le domaine des mathématiques…)

Attention - Le verbe contenir

Attention également à l'ambiguïté du verbe "contenir", parfois utilisé pour dire que x est élément de E, parfois pour dire que F est une partie de E.

Exercice
Soit $A = \{x \in \mathbb{N} \mid x/2 \in \mathbb{N} \text{ et } x \geqslant 10\}$. Que représente A ? Ecrire cet ensemble différemment.
Ecrire en extension $\complement_{2\mathbb{N}} A$ puis déterminer $\complement_{\mathbb{N}} A$.
Déterminer les sous-ensembles X de $\mathbb{N}$ tels que $A \cup X = \mathbb{N}$.

Correction
A est l'ensemble des nombres paires plus grand que 10. $\complement_{2\mathbb{N}} A = \{0,2,4,6,8\}$.
$\complement_{\mathbb{N}} A = \{0,2,4,6,8\} \cup \{2k+1, k \in \mathbb{N}\}$. On doit prendre des ensembles qui contiennent au moins $\complement_{\mathbb{N}} A$

Exercice
Soit E un ensemble. Que peut-on dire de deux parties A et B de E vérifiant $A \cap B = A \cup B$?

Correction
$A = B$. En effet, nécessairement : $A \cup B \subset A \cap B \ldots$

Exercice
On définit la différence symétrique de deux ensembles E et F par

$$E \Delta F = (E \setminus F) \cup (F \setminus E).$$

Ecrire $E \Delta F$ à l'aide de $E \cup F$ et $E \cap F$.

Correction
$E \Delta F = (E \cup F) \setminus (E \cap F)$

Pour aller plus loin - Probabilité
Nous reprenons ces notions lors du cours de probabilité. Il y aura quelques modifications de vocabulaire

Proposition - Quelques règles de calcul
E, F et G désignent trois ensembles quelconques.

$E \cup F = F \cup E$	(commutativité de la réunion)
$E \cup (F \cup G) = (E \cup F) \cup G$	(associativité de la réunion)
$\emptyset \cup E = E \cup \emptyset = E$	(l'ensemble vide est neutre pour la réunion)
$E \cap F = F \cap E$	(commutativité de l'intersection)
$E \cap (F \cap G) = (E \cap F) \cap G$	(associativité de l'intersection)
$\emptyset \cap E = E \cap \emptyset = \emptyset$	(l'ensemble vide est absorbant pour l'intersection)
$E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$	(distributivité de l'intersection par rapport à la réunion)
$E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$	(distributivité de la réunion par rapport à l'intersection)

Pour A et B deux parties de E :

$$A \cap E = A$$
$$A \cup E = E$$
$$\complement_E(\complement_E A) = A$$
$$\complement_E(A \cup B) = (\complement_E A) \cap (\complement_E B)$$
$$\complement_E(A \cap B) = (\complement_E A) \cup (\complement_E B)$$

Les deux dernières formules sont connues sous le nom de *lois de Morgan*.

Pour la démonstration, on lie ces résultats aux affirmations correspondantes.
On peut aussi faire une table exhaustive de vérité

Démonstration
$x \in \complement(A \cap B) \iff x \notin A \cap B \iff \text{Non}(x \in A \cap B)$
$\iff \text{Non}(x \in A \text{ et } x \in B) \iff \text{Non}(x \in A)$ ou $\text{Non} x \in B$
$\iff x \notin A$ ou $x \notin B \iff x \in \complement(A)$ ou $x \in \complement(B) \iff x \in \complement(A) \cup \complement(B)$ □

3. Vocabulaire sur les assertions

3.1. Définitions

Pour aller plus loin - Logique floue (1)
Formalisée en 1965, la logique floue élargie ce point de vue : on associe un nombre entre 0 et 1 pour mesurer la véracité de chaque proposition. Une proposition de valeur 0 est fausse. Une proposition de valeur $\frac{1}{2}$ est à moitié fausse. L'arithmétique qui en découle est comparable à celle des probabilités d'événements.
Cela s'appuie sur les ensembles floues avec des degré d'appartenance entre le $\in$ et le $\notin$.
On l'utilise en automatique ou en médecine…

Définition - Assertion (proposition) et prédicat
Dans ce paragraphe une *proposition*, ou *assertion* est un énoncé qui peut prendre deux valeurs logiques : V (vrai) ou F (faux).
Si cette assertion dépend d'une variable x on parle alors de *prédicat*.

Exemple - Propositions
« tout entier est pair » est une assertion de valeur logique F ;
« tout réel est un complexe » est une assertion de valeur logique V ;
« 4 est pair » est une assertion de valeur logique V ;
« x est un multiple de 4' » est un prédicat dont la valeur logique dépend de la valeur de x.
Comme on peut le voir dans les parties suivantes, à partir de deux assertions A et B, on en définit d'autres dont la valeur logique est donnée par une *table de vérité*.

Exercice
Que pensez-vous de $\mathscr{P}_n$ dans l'énoncé formel suivant ?

Notons, $\forall\, n \in \mathbb{N}, \mathscr{P}_n$: « $\exists\, k \in E$ tel que $a_n = k$ »

Correction
Il s'agit d'une famille (suite) de prédicats, il y a donc $\mathscr{P}_0, \mathscr{P}_1 \ldots \mathscr{P}_{1224} \ldots$.
Peut-être que certains sont vraies et d'autres sont faux…

3.2. Négation

Définition - Négation d'une assertion
Considérons une assertion A.
On appelle négation de A l'assertion qui dit le contraire de A, c'est à dire qui est vraie exactement lorsque A est fausse, on la note "non$A$" (ou $\neg A$ en logique).
La *table de vérité* de non$A$:

A	non A
V	F
F	V

Exercice
La négation de « L'hiver dernier il a plu tous les jours à Toulouse » est :
La négation de « Chaque hiver, il neige au moins un jour en Aveyron » est :

Soit I un intervalle de $\mathbb{R}$.
La négation de « $0 \in I$ » est
La négation de « $\forall x \in I,\, x > 0$ » est
La négation de « $\exists x \in I \mid x \geqslant 0$ » est

Correction
La négation de « L'hiver dernier il a plu tous les jours à Toulouse » est « il n'a pas plu (au moins) un jour de l'hiver dernier à Toulouse » :
La négation de « Chaque hiver, il neige au moins un jour en Aveyron » est « il y a (eu) des hivers sans neige en Aveyron ».
Soit I un intervalle de $\mathbb{R}$.
La négation de « $0 \in I$ » est : « $0 \notin I$ »
La négation de « $\forall x \in I,\, x > 0$ » est « $\exists\, x \in I,\, x \leqslant 0$ »
La négation de « $\exists x \in I \mid x \geqslant 0$ » est « $\forall\, x \in I, x < 0$ »

D'une manière plus générale il faut savoir nier une proposition écrite avec des quantificateurs :
Exercice
P désignant une propriété dépendant de x ou de x, y suivant les cas, écrire la négation des assertions suivantes :

1. $\forall x \in E, P(x)$;
2. $\exists x \in E | P(x)$;
3. $\forall x \in E, \exists y \in E | P(x, y)$;
4. $\exists x \in E | \forall y \in E, P(x, y)$;
5. $\exists r \in \mathbb{R}, \exists s \in \mathbb{R} | \forall x \in \mathbb{R}, x \leqslant r$ et $s \leqslant r$.

Correction

1. $\exists\, x \in E, \neg P(x)$;
2. $\forall\, x \in E | \neg P(x)$;
3. $\exists\, x \in E, \forall\, y \in E | \neg P(x, y)$;
4. $\forall\, x \in E | \exists\, y \in E, \neg P(x, y)$;
5. $\forall\, r \in \mathbb{R}, \forall\, s \in \mathbb{R} | \exists\, x \in \mathbb{R}, x > r$ ou $s > r$.

L'exercice suivant permet de revoir également la table de vérité d'une conjonction (« et ») ou disjonction (« ou ») d'assertions.

Exercice

Compléter le tableau suivant :

A	B	A et B	A ou B	non (A et B)	non (A ou B)	non A	non B	
V	V	V	V					
V	F	F	V					
F	V	F	V					
F	F	F	F					

On a laissé une colonne pour des « tests ». Quelle relation remarquez-vous ?

Correction

A	B	A et B	A ou B	non (A et B)	non (A ou B)	non A	non B	non A et non B	non A ou non B
V	V	V	V	F	F	F	F	F	F
V	F	F	V	V	F	F	V	F	V
F	V	F	V	V	F	V	F	F	V
F	F	F	F	V	V	V	V	V	V

On démontre les lois de Morgan :

— non(A et B)$\Leftrightarrow$ (non A) ou (non B)

— non(A ou B)$\Leftrightarrow$ (non A) et (non B)

3.3. Implications et équivalence d'assertions

Définition - Implication d'assertions

Considérons deux assertions A et B.

Si, lorsque l'assertion A est vraie, alors, nécessairement, l'assertion B l'est également, on dit que A implique B et l'on écrit $A \Rightarrow B$

(ce qui se lit donc "A implique B" ou "si A alors B").

Plus précisément, la table de vérité de $A \Rightarrow B$ est donnée par :

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Remarque - Et si A est fausse

On remarquera qu'en logique, dés que A est fausse, $A \Rightarrow B$ est évaluée vraie, en bref, vous pouvez construire sans problème une démonstration juste avec une hypothèse fausse, mais finalement c'est sans intérêt parce que vous n'avez aucun résultat à énoncer à la fin...c'est la raison pour laquelle usuellement "prouver $A \Rightarrow B$" sous entend "prouver A vraie $\Rightarrow$ B vraie ".

Et donc si $E = \emptyset$, tout énoncé "$\forall x \in E, P(x)$" (ou "$x \in E \Rightarrow P(x)$") a la valeur logique V

…

Exercice

Pour aller plus loin - Logique floue (2)

A la place de V et F, on peut respectivement écrire 1 *et* 0.

Dans ce cas si p_i est une proposition et $v(p_i)$ sa valeur ($v(p_i) = 0$, si p_i est fausse…).

On a donc $v(p_1 \cap p_2) = v(p_1) \times v(p_2)$, $v(non(p_1)) = 1 - v(p_1)$ et $v(p_1 \cup p_2) = v(p_1) + v(p_2) - v(p_1)v(p_2)$.

Cet arithmétique se transpose aisément en logique floue.

Quelle est l'assertion qui a même table de vérité que « non$(A \Rightarrow B)$' » ?

Correction

Il s'agit de « A et non(B) » (il suffit de faire une table de vérité)

Avec deux implications, on a exactement une équivalence :

Définition - Equivalence d'assertions

Considérons deux assertions A et B.

On dit que A et B sont équivalentes si elles signifient la même chose, mais dite différemment, c'est à dire si, simultanément, A implique B et B implique A;

on note alors $A \Leftrightarrow B$.

Plus précisément, la table de vérité de $A \Leftrightarrow B$ est donnée par :

A	B	$A \Leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

Exemple - Deux assertions équivalentes

On a par exemple pour x réel : $(x > 0) \Leftrightarrow (-x < 0)$.

Exercice

Comparer la table d'équivalence de $A \Leftrightarrow B$ avec celle de $[(A \Rightarrow B)$ et $(B \Rightarrow A)]$

Correction

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$[A \Rightarrow B$ et $B \Rightarrow A]$
V	V	V	V	V	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

Attention - A démontrer?

Certaines équivalences correspondent en fait à la définition d'un objet mathématique, d'autres en revanche nécessitent une démonstration.

Attention - Ne pas abuser de $A \Longleftrightarrow B$

Les étudiants écrivent TROP souvent $A \Longleftrightarrow B$, en faisant un calcul dans leur tête (ou une démonstration) qui permet de passer de A à B, SANS vérifier si l'on passe aussi de B à A.

Il est important de ne pas faire cette erreur, surtout si l'on demande qu'une implication…. Il ne faut pas en faire trop, si c'est faux!

4. Principales méthodes de démonstration

4.1. Démonstration d'une implication

Démonstration directe

Considérons deux assertions A et B. On veut démontrer que $A \Rightarrow B$.

Savoir faire - $A \Rightarrow B$. Raisonnement direct

On suppose A vraie, par une succession d'implications connues (calculs, résultats de théorèmes...), on prouve qu'alors B est vraie.

Attention - Abus

Il existe un abus courant de la notation $\Rightarrow$ chez les étudiants (mais aussi les professeurs).
Comme réflexe de protection face à ces abus, il est conseillé de lire $A \Rightarrow B$ à voix haute en disant *« si A est vraie alors B est vraie »* plutôt que *« A implique B »*. Cela permet d'insister sur la prémisse.

Exercice

Montrer que si (x,y) est élément de $]0,2[\times]-2,0[$ alors $\frac{1}{x}-\frac{1}{y}>1$

Correction

$$\left.\begin{array}{r} x\in]0,2[\Longrightarrow \frac{1}{x}>\frac{1}{2} \\ y\in]-2,0[\Longrightarrow \frac{1}{y}<\frac{-1}{2} \end{array}\right\} \Longrightarrow \frac{1}{x}-\frac{1}{y}>\frac{1}{2}-\frac{-1}{2}=1$$

Exercice

Soit f la fonction définie sur $\mathbb{R}$ par $f(x)=|x+\frac{3}{2}|-\frac{1}{2}$. Montrer que

$$x\geqslant -1 \Rightarrow f(x)\geqslant 0$$

Correction

Si $x\geqslant -1$, alors $x+\frac{3}{2}\geqslant \frac{1}{2}\geqslant 0$, donc $f(x)=|x+\frac{3}{2}|-\frac{1}{2}=x+\frac{3}{2}f(x)-\frac{1}{2}\geqslant 0$

On peut-être amené à faire une disjonction de cas :

Exercice

Compléter l'énoncé suivant pour que la démonstration nécessite l'étude de deux cas séparés.
Soit f la fonction définie par ...
Montrer que $x\geqslant -1 \Rightarrow f(x)\geqslant 0$.

Correction

On peut par exemple prendre $f(x)=|x+\frac{3}{2}|+|x-1|-\frac{1}{2}$.
Dans ce cas,

- si $x\in[-1,1]$, $x-1<0$ et $x+\frac{3}{2}>0$, donc $f(x)=(x+\frac{3}{2})+(1-x)-\frac{1}{2}=2\geqslant 0$
- si $x\geqslant 1$, $x-1>0$ et $x+\frac{3}{2}>0$, donc $f(x)=(x+\frac{3}{2})+(x-1)-\frac{1}{2}=2x\geqslant 0$, car $x>0$

Le chemin de la démonstration

Heuristique - Démontrer que ...

Lorsqu'on cherche à démontrer un résultat, il y a fondamentalement deux attentes :

1. Trouver la (une) démonstration,
   satisfaisante i.e. qui donne la certitude du fait
2. Ecrire la démonstration,
   de sorte que toute personne qui lise la démonstration soit également persuadé du fait

Avec le temps du passage de 1 à 2, il faut donc trois temps dans la recherche d'une démonstration.

Attention - Premier piège

Le temps 1 est le temps de l'analyse.
Le temps 2 est le temps de la synthèse.
Ce sont deux choses très différentes. Lorsque vous lisez une démonstration d'un théorème faite par un professeur, un corrigé dans un livre... vous ne voyez que le second temps, celui de la synthèse. Après la lecture, vous pouvez vous dire : « et oui, je vois que c'est vrai », mais vous n'avez pas appris *comment on trouve* la démonstration!!!
La seule solution est de chercher, chercher, chercher... et de ne pas se précipiter sur la (une) solution.
De même, si pour vous écrire une démonstration de cours lors d'une colle est uniquement un exercice de mémoire, alors c'est que vous n'avez pas compris le premier point, ni le point 1 $\rightarrow$ 2 de la démonstration du fait considéré. *Pouvez-vous donner un exemple d'une telle situation rencontrée?*

Analyse - La métaphore du petit poucet

Faire une démonstration, c'est partir d'un point A (les hypothèses) pour arriver à un point B (la conclusion).
Il s'agit donc de **trouver un chemin**, sans se perdre en route...

- On peut avancer discrètement, les yeux fermés
  ou bien laisser des traces afin de pouvoir revenir (classique trace du petit poucet)
- On peut tourner autour du point de départ (on parle de mouvement brownien)
  ou bien fixer son cap et se diriger en direction du point B (même s'il peut y avoir quelques obstacles en chemin)
  (mettre un phare, prendre une boussole qui indique une direction)
  voire placer quelqu'un d'autre en B, le laisser venir vers nous et nous vers lui et chercher à faire la jonction (s'appeler, mettre un phare)
- On peut se précipiter sur son GPS
  ou bien chercher à reconnaître là où l'on se trouve, voir si on ne voit pas une route déjà connue (courage, familiarité avec le chemin) le monstre
- Prendre du recul, de la hauteur... prendre le temps de voir de plus haut (bottes de 7 lieux)

Pour aller plus loin* - f *surjective, injective

On verra plus loin les définitions. A ce stade, il suffit de savoir que par définition f est surjective de E sur F si $\forall\, y\in F, \exists\, x\in E$ tel que $y=f(x)$.
Et par définition f est injective de E (sur F) si $\forall\, x_1,x_2\in E, f(x_1)=f(x_2)\Leftrightarrow x_1=x_2$.

Exemple - Exercice « de base »

On suppose que $f:E\rightarrow E$ est surjective, montrer que $f^2(=f\circ f)$ est surjective.
Si l'on n'écrit pas ce que l'on veut obtenir i.e. le point B : « f^2 est surjective », on ne peut s'en sortir uniquement en dérivant du point A : « f est surjective ».
Pour préparer la démonstration, il faut donc laisser des espaces et compléter au fur et à mesure.
Le temps joue un rôle important, or il n'y parait plus lorsque la démonstration est écrite. Pour le voir à l'oeuvre, nous allons présenter la démonstration comme succession de photos prises de son écriture.

1er — 2eme — 3eme — 4eme — 5eme — 6eme — 7eme

3eme : Soit $y\in E$

4eme : f est surjective donc $\forall\, b\in E, \exists\, a\in E$ tel que $b=f(a)$

5eme : ainsi $\exists\, x_1$ tel que $y=f(x_1)$

6eme : et $\exists\, x_2$ tel que $x_1=f(x_2)$

7eme : donc $\exists\, x(=x_2)$ tel que $f^2(x)=f(x_1)=y$

2eme : $\forall\, y\in E, \exists\, x\in E$ tel que $y=f^2(x)$

1er : donc f^2 est surjective

Cela s'écrit ensuite :
Soit $y\in E$
f est surjective donc $\forall\, b\in E, \exists\, a\in E$ tel que $b=f(a)$.
ainsi $\exists\, x_1$ tel que $y=f(x_1)$
et $\exists\, x_2$ tel que $x_1=f(x_2)$
donc $\exists\, x(=x_2)$ tel que $f^2(x)=f(x_1)=y$
Donc : $\forall\, y\in E, \exists\, x\in E$ tel que $y=f^2(x)$ et finalement : f^2 est surjective

Exercice

Soit E un ensemble et $f:E\rightarrow E$, une application sur E.
On suppose que $f^3=f$. Montrer que si f est injective alors f est surjective. Et réciproquement.

Correction

1er — 2eme — 3eme — 4eme — 5eme

3eme : Soit $y\in E$

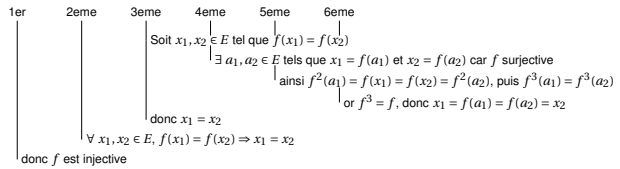
5eme : Soit $x=f(y)$. Alors $f^2(x)=f^3(y)$ et puisque $f^3=f$

4eme : $f^2(x)=f(y)$ et $f(x)=y$ car f injective

2eme : $\forall\, y\in E, \exists\, x\in E$ tel que $y=f(x)$

1er : donc f^2 est surjective

Ce qui s'écrit :
Soit $y\in E$.
Prenons $x=f(y)$, alors $f^2(x)=f^3(y)=f(y)$ car $f^3=f$.
Puis comme f est injective : $f(x)=y$.
Donc il existe $x\in E$ tel que $y=f(x)$.
Par conséquent : $\forall\, y\in E, \exists\, x\in E$ tel que $y=f(x)$, donc f surjective.
De même, réciproquement



Ce qui s'écrit :
Soient $x_1, x_2 \in E$ tels que $f(x_1) = f(x_2)$.
Comme f est surjective, il existe $a_1, a_2 \in E$ tels que $x_1 = f(a_1)$ et $x_2 = f(a_2)$.
Et donc en composant par f : $f^2(a_1) = f(x_1) = f(x_2) = f^2(a_2)$, puis $f^3(a_1) = f^3(a_2)$
Mais comme $f^3 = f$, alors $f(a_1) = f(a_2)$, soit $x_1 = x_2$.
On a donc démontré : $\forall\, x_1, x_2 \in E$ tels que $f(x_1) = f(x_2)$, alors $x_1 = x_2$.
Donc f est injective.

Contraposée

Proposition - Contraposée
$(\text{non } B \Rightarrow \text{non } A)$ s'appelle la contraposée de $(A \Rightarrow B)$.
Il est équivalent de prouver l'une ou l'autre de ces deux implications

Démonstration
On complète la table de vérité :

A	B	non A	non B	$A \Rightarrow B$	non $B \Rightarrow$ non A
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

□

Savoir faire - $A \Rightarrow B$. Raisonnement par contraposée
On suppose donc B fausse et on prouve qu'alors A est fausse, comme précédemment

Le résultat de l'exercice suivant sera fréquemment exploité en analyse :
Exercice
On considère un nombre réel $x \geqslant 0$. Montrer que

$$(\forall \epsilon > 0,\ 0 \leqslant x \leqslant \epsilon) \Rightarrow x = 0.$$

Correction
On fait donc un raisonnement par contraposée (c'est presqu'un raisonnement par l'absurde ici).
Si $x > 0$, alors avec $\epsilon = \frac{x}{2}$, on a la preuve de : $\exists\, \epsilon > 0$ tel que $x > \epsilon$.
Donc l'assertion négative de notre hypothèse A est alors vérifiée.
Ainsi non$(B) \Rightarrow$ non(A) et par contraposée : $A \Rightarrow B$.

4.2. Démonstration d'une équivalence

Deux possibilités pour prouver l'équivalence $A \Leftrightarrow B$:

Savoir faire - $A \Leftrightarrow B$. On procède en deux temps
1. On montre $A \Rightarrow B$
2. On montre $B \Rightarrow A$

Exercice
On considère une fonction f définie sur $\mathbb{R}$ à valeurs dans $\mathbb{R}$. Montrer que

$$(f \text{ est une fonction paire et impaire }) \Leftrightarrow (f \text{ est la fonction nulle }).$$

Correction
En deux temps.
— Supposons que f est nulle.
Alors pour tout $x \in \mathbb{R}$, $f(-x) = 0 = f(x)$ donc f est paire et $f(-x) = 0 = -f(x)$ donc f est impaire. Bilan : f est nulle $\Longrightarrow$ f est une fonction paire et impaire.
— Réciproquement, si f est une fonction paire et impaire,
Alors pour tout $x \in \mathbb{R}$, $f(x) = f(-x)$ et $f(x) = -f(-x)$, donc $f(x) = -f(x)$ donc $2f(x) = 0$ donc $f(x) = 0$.
Ceci est vrai pour tout $x \in \mathbb{R}$, donc $f = 0$ (f est identiquement la fonction nulle).
Bilan : f est une fonction paire et impaire $\Longrightarrow$ f est nulle.
Par double implication : f est nulle $\Longleftrightarrow$ f est une fonction paire et impaire.

Savoir faire - $A \Leftrightarrow B$. On procède par équivalences connues successives.
Cette méthode est surtout utilisée pour des résolutions calculatoires.
Attention de ne pas en abuser : *il faut à chaque étape être sûr que l'on peut « remonter » les équivalences.*

Exercice
Montrer que

$$\begin{cases} 2x + y = 2 \\ 3x + 4y = 3 \end{cases} \Longleftrightarrow (x, y) = (1, 0)$$

Correction
Les règles d'équivalence sur les systèmes sont strictes, il faut bien les respecter ! En particulier la substitution mal employée ne conserve pas les équivalences de système. Nous reverrons cela plus tard dans l'année.

$$\begin{cases} 2x + y = 2 \\ 3x + 4y = 3 \end{cases} \Leftrightarrow \left\{ \begin{array}{rcrcl} 2x & + y & = & 2 & \\ -5x & & = & -5 & \left| \begin{array}{l} \\ L_2 \leftarrow L_2 - 4L_1 \end{array} \right. \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} y & = & 0 \\ x & = & 1 \end{array} \left| \begin{array}{l} L_1 \leftarrow L_1 + \frac{2}{5} L_2 \\ \end{array} \right. \right.$$

Insistons :

Truc & Astuce pour le calcul - Ne pas abuser de $\Leftrightarrow$
Il faut éviter le plus possible d'écrire $\Leftrightarrow$ comme un tic de langage.
1. Si il n'est pas utile, on ne le note pas !
2. Si on choisit de le noter, on vérifie bien à chaque étape le sens $\Leftarrow$ tout particulièrement.

4.3. Raisonnement par l'absurde

Savoir faire - Raisonnement par l'absurde
Pour démontrer un certain énoncé, on fait l'hypothèse qu'il est faux et on aboutit à une contradiction.

Exercice
Montrer que le réel $\sqrt{2}$ est irrationnel (i.e. n'est pas rationnel)

Correction
Si $\sqrt{2} = \frac{p}{q}$, fraction irréductible, alors $2q^2 = p^2$, donc 2 divise p^2, puis p qui est donc pair.
Puis $p = 2p'$ et donc $2q^2 = 4p'^2$, donc $q^2 = 2p'^2$, puis 2 divise q^2, puis q qui est donc pair.
Et ainsi la fraction $\frac{p}{q}$ n'est pas irréductible...

Remarque - Différence avec la contraposée
Pour la contraposée, on suppose non$B$ et on aboutit à non$A$.
Pour l'absurde, on suppose non$B$ et A ensemble et on montre qu'il y a une contradiction. Dans ce second cas, on exploite plus d'hypothèses !

Pour aller plus loin - Raisonnement par l'absurde, à accepter ?
Certaine axiomatique de mathématique refuse le raisonnement par l'absurde, en effet la notion d'existence qui en découle est quelque peut frustrante.
On sait que $\sqrt{2}$ n'est pas un nombre rationnel, c'est un nombre algébrique de degré 2 (quadratique).
Notons $a = \sqrt{2}^{\sqrt{2}}$. Alors il existe un nombre transcendant à la puissance $\sqrt{2}$ (transcendant) qui est algébrique (contraire de transcendant).
En effet, si a est algébrique, alors $\sqrt{2}$, à la puissance $\sqrt{2}$ est algébrique.
Si tel n'est pas le cas alors a est transcendant et $a^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2$. Donc, c'est a qui résout le problème.
Et pourtant...
On ne sait toujours pas aujourd'hui lequel des deux nombres $\sqrt{2}$ ou $\sqrt{2}^{\sqrt{2}}$ répond à la question !

4.4. Conditions nécessaire, suffisante

Il s'agit simplement *d'un peu de bon sens* sur la signification des mots « nécessaire » et « suffisant ».

Exemple - A : « x est le carré d'un entier » et B : « $x \geqslant 0$ »
Considérons un réel x et posons

A : x est le carré d'un entier
B : $x \geqslant 0$

Qu'est-ce qui est nécessaire, qu'est-ce qui est suffisant (ou ne l'est pas) ?

Définition - Condition nécessaire. Condition suffisante
Plus généralement $A \Rightarrow B$ peut se dire :
- B est une condition nécessaire (**CN**) pour avoir A (puisque si on A, nécessairement on a B)
- A est une condition suffisante (**CS**) pour avoir B (puisqu'il suffit d'avoir A pour avoir B

Rechercher une condition nécessaire et suffisante (**CNS**) pour avoir A revient donc à chercher B tel que $A \Leftrightarrow B$.

Savoir faire - Analyse-Synthèse
Certaines démonstrations, difficiles à gérer par équivalences, ou lorsque le résultat n'est pas donné, se font en deux phases :

1. phase d' "analyse" : on obtient une condition nécessaire (par implications successives par exemple) pour qu'une première hypothèse soit vérifiée
2. phase de "synthèse", ou phase de vérification : la condition précédemment obtenue est-elle suffisante?

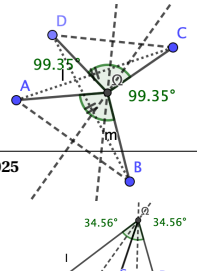
Exercice
Montrer que toute fonction définie sur $\mathbb{R}$ à valeurs dans $\mathbb{R}$ s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire.
On procédera de la manière suivante :
Première étape (analyse) : supposons qu'il existe deux fonctions f et g telles que ..., alors $f =$, $g =$
Deuxième étape (synthèse) : on vérifie que les solutions trouvées à la première étape conviennent

Correction
ANALYSE : Si $h = f + g$ avec f paire et g impaire,
alors $\forall\, x \in \mathbb{R}$, $h(-x) = f(-x) + g(-x) = f(x) - g(x)$ et $h(x) = f(x) + g(x)$.
En additionnant et retranchant : $f(x) = \frac{1}{2}\big(h(x) + h(-x)\big)$ et $g(x) = \frac{1}{2}\big(h(x) - h(-x)\big)$.
L'analyse a abouti à une unique décomposition (sous reserve d'existence...).
SYNTHESE : Soit h une fonction de $\mathbb{R}$ et associons lui :
$f : x \mapsto \frac{1}{2}\big(h(x) + h(-x)\big)$ et $g : x \mapsto \frac{1}{2}\big(h(x) - h(-x)\big)$
alors par construction $h = f + g$,
mais aussi $f(-x) = \frac{1}{2}\big(h(-x) + h(x)\big) = \frac{1}{2}\big(h(x) + h(-x)\big) = f(x)$, donc f est paire
également $g(-x) = \frac{1}{2}\big(h(-x) - h(x)\big) = -\frac{1}{2}\big(h(x) - h(-x)\big) = g(x)$, donc g est impaire

Exercice
Soit A, B, C et D quatre points du plan tel que $AC = BD$ et (AB) non parallèle à (CD).
Alors il existe une unique rotation du plan r tel que $r(A) = B$ et $r(C) = D$.
Donner ses caractérisations

Correction
Nous allons raisonner par analyse-synthèse.
ANALYSE. Supposons que $r(A) = B$ et $r(C) = D$.
Notons Ω le centre de r et θ son angle de rotation.
Comme $r(A) = B$, on a donc $|\Omega A| = |\Omega B|$ et $(\overrightarrow{\Omega A}, \overrightarrow{\Omega B}) = \theta$.
Ainsi, Ω est sur la médiatrice de $[AB]$. De même Ω est sur la médiatrice de $[CD]$.

Représentation - Deux configurations de l'exercice



Ces deux médiatrices se coupent en un seul point, ssi elles ne sont pas parallèles.
Si ces médiatrices sont parallèles, alors (AB) et (CD) sont parallèles,
la contraposée donne donc :
si (AB) et (CD) ne sont pas parallèles, alors les deux médiatrices se coupent en un seul point.
Ainsi Ω est obtenu de manière unique et $\theta := (\overrightarrow{\Omega A}, \overrightarrow{\Omega B})$, bien défini.
SYNTHESE. Considérons la rotation, centrée Ω concours des médiatrices et d'angle $\theta := (\overrightarrow{\Omega A}, \overrightarrow{\Omega B})$.
On a par définition $r(A) = B$.
Comme $\Omega C = \Omega D$, $\Omega A = \Omega B$ et $AC = BD$, les triangles ΩAC et ΩBD sont semblables.
Donc $(\overrightarrow{\Omega A}, \overrightarrow{\Omega C}) = (\overrightarrow{\Omega B}, \overrightarrow{\Omega D})$.
Ainsi, avec la relation de Chasles (des angles) :

$$\theta = (\overrightarrow{\Omega A}, \overrightarrow{\Omega B}) = (\overrightarrow{\Omega A}, \overrightarrow{\Omega C}) + (\overrightarrow{\Omega C}, \overrightarrow{\Omega B}) = (\overrightarrow{\Omega B}, \overrightarrow{\Omega D}) + (\overrightarrow{\Omega C}, \overrightarrow{\Omega B}) = (\overrightarrow{\Omega C}, \overrightarrow{\Omega D})$$

Donc $r(C) = D$. BILAN : Il existe une unique rotation tel que $r(A) = B$ et $r(C) = D$, c'est la rotation dont le centre est Ω, le point de concours des médiatrices de $[AB]$ et de $[CD]$ et d'angle $\theta = (\overrightarrow{\Omega A}, \overrightarrow{\Omega B})$.
On appliquera ce résultat dans le cours sur les nombres complexes.

4.5. Exploiter un contre-exemple dans une démonstration

Savoir faire - Utilisation d'un contre-exemple
Lorsque l'on veut prouver qu'une implication est fausse, on cherche un exemple vérifiant l'hypothèse mais pas la conclusion, ce que l'on appelle un *contre-exemple*.

Exercice
Soit f la fonction définie sur $\mathbb{R}$ par $f(x) = |x + \frac{3}{2}| - \frac{1}{2}$. Montrer que $(x \geqslant -1)$ et $(f(x) \geqslant 0)$ ne sont pas équivalents.

Correction
$-10 \leqslant -1$ et $f(-10) = \frac{7}{2} - \frac{1}{2} = 3 \geqslant 0$

4.6. Démonstration par récurrence

Proposition - Principe admis (axiome)
Soit $P(n)$ (parfois notée $\mathscr{P}_n$) une propriété portant sur l'entier n.
Si on a

$$\begin{cases} P(0) \text{ vraie} \\ \forall n \in \mathbb{N}, (P(n) \text{ vraie } \Rightarrow P(n+1) \text{ vraie}) \end{cases}$$

alors $P(n)$ est vraie pour tout entier n.

Savoir faire - Rédaction d'un raisonnement par récurrence
• Pour $n = 0$, $P(0)$ est vérifiée, avec vérification effective! (souvent deux simples calculs)
• Supposons la propriété vérifiée pour **un certain** $n \geqslant 0$ (et surtout pas "pour tout", parce que là, ce n'est plus la peine de faire une démonstration!).
⇒ Montrons que $P(n+1)$ est vraie.
Conclusion : $\forall n \in \mathbb{N}$, $P(n)$ est vraie.

Remarque - Démarrer à un autre nombre
On peut aussi démarrer à une valeur de n autre que 0.
Exercice
Montrer que $\forall n \in \mathbb{N}$, $n < 2^n$.

Correction
Remarquons d'abord que pour tout entier n, $2^n \geqslant 1$ Notons pour tout entier $n \in \mathbb{N}$, $\mathscr{P}_n$: « $n < 2^n$ ».
— $0 < 1 = 2^0$, donc $\mathscr{P}_0$ est vraie.
— Soit $n \in \mathbb{N}$, supposons que $\mathscr{P}_n$ est vérifiée.
Donc $n < 2^n$ et donc $n + 1 < 2^n + 1 \leqslant 2^n + 2^n = 2^{n+1}$
Donc $\mathscr{P}_{n+1}$ est alors vraie.

Histoire - Citation de Henri Poincaré, La science et l'hypothèse, 1902
« Le caractère du raisonnement par récurrence est qu'il contient, condensés, pour ainsi dire en une formule unique, une infinité de syllogismes.
Pour qu'on s'en puisse mieux rendre compte, je vais énoncer les uns après les autres ces syllogismes qui sont, si l'on veut me passer l'expression, disposés en cascade.
Ce sont bien entendu des syllogismes hypothétiques.
Le théorème est vrai du nombre 1.
Or si il est vrai de 1, il est vrai de 2.
Donc il est vrai de 2.
Or si il est vrai de 2, il est vrai de 3.

Le résultat est donc bien démontré par récurrence et on peut affirmer : $\forall\, n\in\mathbb{N},\ n<2^n$.

Exercice

Y a-t-il des erreurs dans les raisonnements suivants ? Où sont-elles ?

1. On a : $10^{n+1}+1 = 10\times 10^n+1 = (9+1)\times 10^n+1 = 9\times 10^n+10^n+1$
   Donc, si 10^n+1 est divisible par 9, il en est de même de $10^{n+1}+1$, ce qui prouve que pour tout entier naturel n, 10^n+1 est divisible par 9.
2. Prouvons que tout ensemble fini a tous ses éléments égaux :
   Si dans tout ensemble E_n à n éléments, tous les éléments sont égaux, alors, soit E_{n+1} un ensemble à $n+1$ éléments :
   $$E_{n+1} = \{x_1, x_2, \dots, x_n, x_{n+1}\}.$$
   Avec l'ensemble de n éléments $\{x_1, x_2, \dots, x_n\}$, on a, par hypothèse de récurrence : $x_1 = x_2 = \cdots = x_n$.
   Avec l'ensemble de n éléments $\{x_2, x_3, \dots, x_{n+1}\}$, on a, par hypothèse de récurrence : $x_2 = x_3 = \cdots = x_{n+1}$.
   Donc $x_1 = x_2 = \cdots = x_{n+1}$.
   Comme la propriété est vraie pour $n=1$ (cas d'un singleton), il en résulte que tout ensemble de n éléments a tous ses éléments égaux.

Correction

Dans le premier raisonnement, on montre bien le moteur de la récurrence : $\mathscr{P}(n)\Rightarrow\mathscr{P}(n+1)$.
Mais l'initialisation n'est pas démontrée ; et pour cause : elle est fausse.
Le résultat (pour tout $n\in\mathbb{N}$) n'est donc pas démontré (et d'ailleurs il est toujours faux).
Dans le second raisonnement, c'est plus subtile. Dans le passage $\mathscr{P}(n)\Rightarrow\mathscr{P}(n+1)$,
il faut nécessairement que E_{n+1} possède au moins 3 éléments, et donc $n\geqslant 2$.
Ainsi, l'initiation ne sert à rien ici, il faut commencer par démontrer $\mathscr{P}(2)$.

Savoir faire - Récurrence à plusieurs pas (ou plusieurs termes)

Suivant la façon dont est énoncée la propriété de récurrence $P(n)$ il peut être nécessaire
- d'initialiser la récurrence avec plusieurs (k) valeurs de n
- de supposer $P(n),\dots,P(n+k-1)$ (il y en a aussi k) vraies pour un certain $n\geqslant 0$
- de prouver que ces k propriétés exactes entraînent $P(n+k)$ vraie

Savoir faire - Récurrence forte

- Pour $n=0$, $P(0)$ est vérifiée (avec vérification effective !)
- Supposons la propriété vérifiée **jusqu'à** un certain $n\geqslant 0$ (i.e $P(0),P(1),\dots,P(n)$ vraies)
- Montrons que $P(n+1)$ est vraie.

On parle parfois alors de « récurrence à plusieurs pas » ou de « récurrence forte », par opposition à la récurrence du théorème dite « récurrence simple (ou faible) »).

Exercice

Soit (u_n) la suite définie par $u_0=\dfrac{2}{5}, u_1=1$ et pour tout entier naturel n,
$$u_{n+2} = 5u_{n+1}-6u_n.$$
Démontrer que pour tout $n\in\mathbb{N}$, $u_n=\dfrac{2^n+3^n}{5}$.

Correction

Nous verrons par la suite d'autre méthode que la récurrence.
En attendant, nous devons employer ici une récurrence à deux pas.
Notons pour tout entier $n\in\mathbb{N}$, $\mathscr{P}_n$: « $u_n=\dfrac{2^n+3^n}{5}$ ».
- $\dfrac{2^0+3^0}{5}=\dfrac{2}{5}=u_0$, donc $\mathscr{P}_0$ est vraie.
- $\dfrac{2^1+3^1}{5}=\dfrac{5}{5}=u_1$, donc $\mathscr{P}_1$ est vraie.

- Soit $n\in\mathbb{N}$, supposons que $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ sont vérifiées.
  Donc $u_{n+2}=5\dfrac{2^{n+1}+3^{n+1}}{5}-6\dfrac{2^n+3^n}{5}=\dfrac{2^n(10-6)+3^n(15-6)}{5}=\dfrac{2^{n+2}+3^{n+2}}{5}$ Donc $\mathscr{P}_{n+2}$ est alors vraie.

Le résultat est donc bien démontré par récurrence et on peut affirmer : $\forall\, n\in\mathbb{N}$, $u_n=\dfrac{2^n+3^n}{5}$.

Exercice

Montrer que tout entier $n\geqslant 2$ se décompose en produit de nombres premiers.

Correction

On fait une récurrence forte.
Notons pour tout entier $n\geqslant 2$, $\mathscr{P}_n$: « n se décompose en produit de nombres premiers ».
- 2 est un nombre premier donc $\mathscr{P}_2$ est vraie.
- Soit $n\in\mathbb{N}$, $n\geqslant 2$ supposons que pour tout entier $k\leqslant n$, $\mathscr{P}_k$ est vérifiée.
  Si $n+1$ est un nombre premier, alors il est le produit de nombres premiers.
  Si $n+1$ n'est pas premiers, il existe $a,b\geqslant n$ tel que $n+1=ab$.
  Or $\mathscr{P}_a$ et $\mathscr{P}_b$ sont vraies, donc on peut décomposer ces deux nombres,
  et par produit $n+1$ est également le produit de nombres premiers.
  Donc $\mathscr{P}_{n+1}$ est alors vraie.

Le résultat est donc bien démontré par récurrence (forte) et on peut affirmer que tout entier $n\geqslant 2$ se décompose en produit de nombres premiers.

Exercice

Montrer qu'un changement d'hypothèse de récurrence ramène une récurrence à plusieurs pas ou une récurrence forte à une récurrence faible.

Correction

Dans le cas d'une récurrence à h pas, on peut considérer $\mathscr{Q}_n$: « $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ et … $\mathscr{P}_{n+h}$ ».
Dans le cas d'une récurrence forte, on peut considérer $\mathscr{Q}_n$: « $\forall\, k\geqslant n\ \mathscr{P}_k$ ».

Exercice

Montrer par récurrence forte que toute suite décroissante d'entiers est stationnaire (i.e. constante à partir d'un certain rang).

Correction

On note, pour tout entier $k\in\mathbb{N}$, $\mathscr{P}_k$: « si $(u_n)\in\mathbb{N}^{\mathbb{N}}$ avec $u_0=k$ et (u_n) décroissante, alors (u_n) est stationnaire. »
- Si $u_0=0$, alors nécessairement, il s'agit de la suite stationnaire égal à 0, car $0=u_0\geqslant \underbrace{u_n}_{\in\mathbb{N}}\geqslant 0$.
  Donc $\mathscr{P}_0$ est vraie.
- Soit $k\in\mathbb{N}$. Supposons que pour tout $h\geqslant k$, $\mathscr{P}_h$ est vraie.
  Soit (u_n) suite d'entiers, décroissante telle que $u_0=k+1$.
  • Ou bien pour tout $n\in\mathbb{N}$, $u_n=k+1$ et donc (u_n) est stationnaire.
  • Ou bien il existe $n_0\in N$ tel que $u_{n_0}\neq k+1$, par décroissance, $u_{n_0}<k+1$.
  Considérons la suite (extraite) (v_n) telle que $v_n=u_{n+n_0}$.
  Alors (v_n) est une suite d'entiers, décroissante de premier terme $u_{n_0}\leqslant k$.
  On applique $\mathscr{P}_{u_{n_0}}$ à (v_n), qui est donc stationnaire à partir du rang N.
  Alors (u_n) est stationnaire à partir du rang $N+n_0$. Donc $\mathscr{P}_{k+1}$ est vraie.

4.7. Démonstration par algorithme

Algorithme

Heuristique - Exploitation d'un algorithme

Un algorithme peut permettre de démontrer, constructivement, l'existence d'un certain objet (ou d'une certaine fonction).
La difficulté est plutôt de démontrer que l'algorithme :
- se termine bien
- réalise bien ce que l'on désire

Définition - Algorithme

Un algorithme est une suite finie de règles à appliquer dans un ordre déterminé à un nombre fini de données pour arriver avec certitude (c'est-à-dire sans indétermination ou sans ambiguïté), en un nombre fini d'étapes, à un certain résultat et cela indépendamment des données.

Terminaison de l'algorithme

Pour démontrer que l'algorithme termine (que le nombre d'étapes est fini), on exploite un variant de boucle, en règle général, en suite d'entiers décroissante. Pour des boucles `for`, la terminaison de boucle est en règle générale immédiate.

Savoir faire - Démontrer qu'une boucle se termine

On identifie une expression (variable) qui :
- est entière
- décroît strictement à chaque étape de la boucle

Alors, nécessairement, la boucle se termine.

Exemple - Division euclidienne

On considère le bout de programme suivant :

```
q=0
r=n
while r>=d :
        q=q+1
        r=r-d
```

Ce programme calcul le quotient `q` et le reste `r` de la division euclidienne de `n` par `d`. (A démontrer)
Mais est-ce qu'il termine bien? Oui
On constate que la suite des valeurs prises par la variable `r` est **strictement décroissante** de `n` à un nombre compris entier positif plus petit que `d`.
Si la boucle ne s'arrêtait pas, alors cette suite de valeur serait infini, ce qui est impossible.

Exercice

On considère le bout de programme suivant :

```
c=0
while p>0 :
        if c==0 :
                p=p-2
                c=1
        else :
                p=p+1
                c=0
```

1. Que fait ce programme ?
2. Les variables `p` et `c` sont-elles décroissantes, strictement ?
3. Montrer que la variable `t=2p+3c` est entière, strictement décroissante.
   En déduire la terminaison de l'algorithme.

Correction

1. On commence par faire le tableau pour comprendre, avec les premiers étapes ce qui peut se passer :

temps	p	c
0	p	0
1	p-2	1
2	p-2+1=p-1	0
3	p-3	1
4	p-2	0
5	p-4	1

   Le programme donne donc pour finir `p=0` (condition d'arrêt) et `c=0`, si `p` est pair initialement, et `c=1` sinon.
2. Les variables `p` et `c` ne sont pas décroissantes.
3. Il y a deux évolutions possibles pour `t=2p+3c`, selon la valeur de `c`.
   - si `c=0`, alors `t=2p+3c→2(p-2)+3(c+1)=2p+3c-1`
   - si `c=1`, alors `t=2p+3c→2(p+1)+3(c-1)=2p+3c-1`

   Donc la variable `t=2p+3c` est entière, strictement décroissante.
   L'algorithme se termine donc bien.

Correction de l'algorithme

Il faut aussi savoir **démontrer** que le programme (avec de nombreuses répétitions de la boucle) réalise se que l'on souhaite.
On utilise alors pour cela des *invariant de boucles*.
Comme son nom l'indique il s'agit d'identifier (créer) une expression-variable qui ne change pas de valeur tout au long du programme.
Puis lorsque le programme se termine, en exploitant cette expression, nous pourrons démontrer que l'on obtient bien le résultat attendu.

Savoir faire - Utilisation d'un invariant de boucle pour démontrer le résultat attendu

Pour démontrer qu'une boucle réalise bien le résultat attendu,

1. on cherche une expression qui reste constante tout au long des calculs de la boucle ;
2. on calcule sa valeur initiale (avant le début de la boucle) ;
3. on en déduit sa valeur finale ;
4. enfin connaissant les valeurs finales des variables du système (testées pour la sortie de boucle), on en déduit la valeur de la variable retournée par le programme.

Exemple - Retour sur la division euclidienne

Reprenons l'algorithme de la division euclidienne par soustraction successive :

```
q=0
r=n
while r>=d :
        q=q+1
        r=r-d
```

- La valeur qui n'évolue pas est `t=dq+r`.
  En effet, on passe à chaque boucle de `t=dq+r→d(q+1)+(r-d)=dq+d+r-d=dq+r`
- De plus initialement, `t=d×0+n=n`
- Et pour finir `r` appartient à l'intervalle $[0, d[$.

On a donc trouver le couple `(q,r)` tel que `n=dq+r` avec `r`$\in [0, d[$.
C'est la définition de la division euclidienne. Et le résultat obtenu est bien celui attendu.

Exercice

Montrer que le programme

```
def somme2(n) :
    S=0
    for i in range(1,n+1):
        S=S+i**2
    return(S)
```

calcule bien $\sum_{i=1}^{100} i^2$

Correction

Notons `T=S-`$\sum_{k=1}^{i-1} k^2$.

Alors à chaque étape, on a `T=S-`$\sum_{k=1}^{i-1} k^2$ `⟶S+i²-`$\sum_{k=1}^{i} k^2$`=S-`$\sum_{k=1}^{i-1} k^2$ Nous avons trouvé notre invariant : `T`.

Initialement, `T=0`, à la fin aussi et donc `S=`$\sum_{k=1}^{n} k^2$

Exercice

On cherche à écrire un programme qui calcul $n!$.

1. Ecrire un programme avec une boucle `while`.
2. **Démontrer** que le programme se termine bien.

3. **Démontrer** que le programme effectue bien ce que l'on souhaite.

Correction

1.

```
def factorielle2(n):
    """Calcul de la factorielle de n"""
    f=1
    k=1
    while k<n :
        f,k=f*(k+1),k+1
    return(f)
```

2. Il s'agit de trouver une variable entière qui décroit strictement.
   Ici, c'est clair, il faut prendre `k`.
   Elle commence à `n`, et décroit strictement à chaque étape. Donc à partir d'un certain moment (ici `n` étapes, puisqu'elle diminue de 1 à chaque étape), elle est nulle ; et la boucle s'arrête bien.
3. Notons $I = f*(k!)$.
   A l'instant initial, $k = n$, $f = 1$ et il a pour valeur $I = 1 \times n! = n!$.
   A chaque instant, on a $I = f*(k!) \rightarrow (f*k)((k-1)!) = I$. Donc I est invariant.
   Enfin, en fin de course, pour la dernière boucle, $k = 1$, et donc $I = f*1! = n!$. Ce qui implique que $f = n!$.
   Le programme renvoie la valeur de f, donc c'est bien la valeur de $n!$.

Proposition - Plus petit élément d'un ensemble fini
Considérons E un ensemble muni d'une relation d'ordre totale.
Un ensemble A de n éléments de E admet un plus petit élément.

Nous allons faire la démonstration par algorithme

Démonstration
Soit A un ensemble fini, on peut supposer que $A = \{x_1, x_2, \dots x_n\}$.
Considérons l'algorithme :

```
a=A[1]
   for k in range(n):
      if A[k]<a :
         a=A[k]
   return(a)
```

L'algorithme termine car il s'agit d'une boucle `for`
Il faut montrer la correction en trouvant un invariant de boucle. On va considérer pour le tour `k` la proposition $\mathscr{P}_k$:« $\forall\ i \leqslant k$, $a \leqslant x_i$, $a \in A$ ». Au premier tour, comme $A[1] = x_1 = a$, $\mathscr{P}_1$ est vraie.
Si $\mathscr{P}_k$ est vraie, il en est de même de $\mathscr{P}_{k+1}$, selon que $x_{k+1} < a$ ou $x_{k+1} \geqslant a$.
En bout de course, on a donc $a \leqslant x_i$, pour tout $i \leqslant n$ et $a \in A$.
□

5. Bilan

Synthèse

⇝ En mathématiques, les raisonnements se fondent sur une vision ensembliste des objets ou des propositions. Nous faisons un premier passage, *de bon sens*, sur ce qu'est un ensemble et ce que signifie appartenir à un ensemble ou en être une partie ; ce qu'est un intervalle ou un produit cartésien d'ensembles.

⇝ Naturellement, apparait fréquemment dans les affirmations mathématiques ensemblistes deux notions : une notion d'universalité *pour tout* et une notion d'exception *il existe*. La formalisation qui est le langage écrit des mathématiques, réserve donc deux symboles pour ces notions : $\forall$ et $\exists$. On les retrouve tout le temps.

⇝ Les mathématiques donnent des relations (de vérité ?) entre les assertions. Nous voyons différentes méthodes exploitées dans *l'artisanat de la démonstration* : table de vérité (cas par cas), implication ou équivalence, analyse-synthèse, contraposée, raisonnement par l'absurde, contre-exemple ou récurrences…

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Montrer que I est un intervalle de $\mathbb{R}$
— Savoir-faire - Noter les dépendances
— Savoir-faire - Montrer que $F \subset E$
— Savoir-faire - Prouver l'égalité de deux ensembles
— Savoir-faire - $A \Rightarrow B$. Raisonnement direct.
— Savoir-faire - $A \Rightarrow B$. Raisonnement par contraposée.
— Savoir-faire - $A \Leftrightarrow B$. On procède en deux temps.
— Savoir-faire - $A \Leftrightarrow B$. On procède par équivalences connues successives.
— Truc & Astuce pour le calcul - Ne pas abuser de $\Leftrightarrow$
— Savoir-faire - Raisonnement par l'absurde
— Savoir-faire - Analyse-Synthèse
— Savoir-faire - Utilisation d'un contre-exemple
— Savoir-faire - Rédaction d'un raisonnement par récurrence
— Savoir-faire - Récurrence à plusieurs pas (ou plusieurs termes)
— Savoir-faire - Récurrence forte
— Savoir-faire - Démontrer qu'une boucle termine
— Savoir-faire - Utilisation d'un invariant de boucle pour démontrer le résultat attendu

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\forall$ - $\exists$	Pour tout (ou quel que soit) - Il existe	Les affirmations mathématiques exploitent très souvent uniquement ces deux symboles	Attention, on $\forall\ a \exists\ b \Leftrightarrow \exists\ b'$
$A \Longrightarrow B \equiv B \Longleftarrow A$	Implication de A vers B	A est suffisante pour B et B est nécessaire à A	Ex : $\exists\ b \forall\ a \Rightarrow$
$A \Longleftrightarrow B$	A et B sont équivalentes	Identique à $A \Rightarrow B \& B \Rightarrow A$	Ne pas en ab

Retour sur les problèmes

47. Quoi dire…
48. Ce n'est probablement pas qu'un langage, mais…
49. Ce n'est pas un problème

Chapitre 11

Applications (entre ensembles)

Résumé -

Nous complétons quelques notions essentielles du fondement des mathématiques (formalisé non sans mal à la fin du XIX-ième siècle). Ces fondements se basent sur les ensembles et sur les applications entre ces ensembles!
Quelles sont les applications qui ne transforment pas trop les ensembles?
Les ensembles images ou réciproques (retour) permet de décrire (par des ensembles) les qualités de l'application.
Une application classique est l'application qui compte les éléments. On précisera ici les notions intuitives de cardinaux des ensembles ici.
Nous terminerons pas étudier les familles Quelques vidéos :

- *Khan Academy - Intersection et union d'ensembles - https ://www.youtube.com/watch ?v=vcwMTpgNlQA*
- *Canal unisciel (P. Dehornoy) - La théorie des ensembles 50 ans après Cohen - https ://www.canal-u.tv/video/institut_fourier/patrick_dehornoy _la_theorie_des_ensembles_cinquante_ans_apres_cohen.41917*

Sommaire

1. Problèmes 220
2. Applications de E dans F 220
2.1. Vocabulaire lié aux applications 220
2.2. Bijections (injections et surjections) 222
3. Image directe et image réciproque d'un ensemble 226
3.1. Image directe 226
3.2. Image réciproque d'un ensemble 228
4. Fonction indicatrice 229
4.1. Définition 229
4.2. Propriétés ensemblistes et calcul avec fonctions indicatrices 229
5. Cardinal d'ensemble fini 230
5.1. Principe des tiroirs 230
5.2. Classe des ensembles de même cardinal 231
5.3. Cardinal, fonction indicatrice et somme (finie) . . . 232
6. Familles 233
6.1. Familles quelconques 233
6.2. Famille indexée sur $\mathbb{N}$. Suites 234
7. Bilan 237

1. Problèmes

Problème 50 - Qualités des fonctions

Résoudre une équation, c'est trouver x (tous les x) tel que $f(x) = b$, où b et f sont connus.
Il est intéressant de savoir si :

- l'équation a (au moins) une solution.
- l'équation a exactement une solution.
- l'équation a (au plus) une solution.

Evidemment, la réponse dépend de b et de f, on peut la noter $f^{-1}(\{b\})$, c'est un ensemble de solution (qui peut être vide)!.
Si on reprend ces trois options, qu'on généralise à tout b, on trouve 3 qualités précises de f. Comment peut-on qualifier ces trois propriétés?

Problème 51 - Description d'ensemble simple

Peut-on comparer deux ensembles facilement. Pour être un tant soit peu identique, ils doivent au moins avoir le même nombre d'éléments.
Comment fait-on pour savoir cela? Quelle est la nature du lien qui unit l'un à l'autre? Existe-t-il des ensembles de référence à k éléments?
Comment calculer formellement le nombre d'éléments d'un sous-ensemble?

Problème 52 - Cardinal fini. Cardinal infini

Deux ensembles sont de taille identique s'il existe une application bijective de l'un sur l'autre.
Même l'existence d'une application bijective d'un ensemble à un autre peut très bien se produire même si les ensembles ne sont pas de taille fini.
Existe-t-il des ensembles infinis de même taille? Des ensembles infinis de tailles différentes? Existe-t-il une relation d'ordre (totale?) entre les ensembles de taille infini?

Problème 53 - Famille $(O_i)_{i\in I}$

Lorsqu'une application dépend d'un nombre réel, on note $f : x \mapsto \dots$ cette application.
Lorsqu'elle dépend d'un nombre entier naturel, on la note $(u_n)_{n\in\mathbb{N}}$.
Existe-t-il une notation officielle pour une application qui dépend d'un ensemble I de points. Et comment on appelle cette application : fonction, suite, autre chose?

2. Applications de E dans F

Il s'agit ici de donner une théorie plus précise sur les fonctions.

2.1. Vocabulaire lié aux applications

Heuristique - Application (définition non formelle)

Une application d'un ensemble E dans un ensemble F est un "procédé" qui associe à chaque élément $x \in E$ un élément $f(x) \in F$. Une telle application est notée

$$\begin{array}{rcl} f: & E & \to F \\ & x & \mapsto f(x) \end{array}$$

$f(x)$ est appelé image de x par f ;
l'ensemble E est appelé ensemble de départ de l'application f ;
l'ensemble F est appelé ensemble d'arrivée de f.
On a donc une application de E dans F dès qu'à tout élément $x \in E$ on peut associer sans ambiguïté un élément $f(x) \in F$ (c'est-à-dire s'il y en a un et un seul possible).

Une application est donc déterminée par la donnée des couples $(x, f(x))$ où x parcourt E, d'où la définition plus formelle :

Définition - Application

Soient E et F deux ensembles et $\mathscr{G} \subset E \times F$ vérifiant

$$\forall x \in E, \exists! y \in F, |\, (x,y) \in \mathscr{G}.$$

La donnée d'un tel triplet $(E,F,\mathscr{G})$ s'appelle une application de E dans F.
On note

$$\begin{array}{rcl} f: & E & \to F \\ & x & \mapsto y = f(x) \end{array}$$

où y est l'unique élément de F vérifiant $(x,y) \in \mathscr{G}$.
$\mathscr{G}$ s'appelle le graphe de l'application. On le note souvent Γ_f.
On a donc $\Gamma_f = \{(x,y) \in E \times F \,|\, y = f(x)\} = \{(x, f(x)) \,|\, x \in E\}$.

Remarque - Fonctions ou applications ?

D'après la définition, une fonction définie sur E, à valeurs dans F, est une application de E dans F.
De cette définition découle le résultat suivant :

Savoir faire - Montrer une égalité de deux fonctions

Soient $f : E \to F$ et $g : E' \to F'$ deux applications. f et g sont égales si et seulement si :
- $E = E'$ (même ensemble de départ),
- $F = F'$ (même ensemble d'arrivée),
- $\forall x \in E,\ f(x) = g(x)$.

Définition - Ensemble de fonctions

On notera $\mathscr{F}(E,F)$ (on trouve aussi les notations $\mathscr{A}(E,F)$ ou F^E) l'ensemble des applications (ou fonctions) de E dans F.

Exemple - Classiques

- Pour tout ensemble E, l'application $x \mapsto x$ de E dans lui-même est appelée application identité de E et notée Id_E, son graphe est la diagonale de E^2.
- Soient E et $F \neq \emptyset$ deux ensembles, et $a \in F$. L'application $x \mapsto a$ de E dans F s'appelle une application constante, son graphe est $E \times \{a\}$.
- Soient $E_1, \dots, E_n$ des ensembles. Pour chaque $i \in \{1, \dots, n\}$ l'application

$$\begin{array}{rcl} p_i: & E_1 \times \cdots \times E_n & \to E_i \\ & (x_1, \cdots, x_n) & \mapsto x_i \end{array}$$

s'appelle la i-ième projection ou la i-ième application coordonnée.

Définition - Restriction et prolongement

Soit $f : E \to F$ une application.
- Soit $A \subset E$. **La** restriction de f à A, notée $f_{|A}$, est l'application

$$\begin{array}{rcl} f_{|A}: & A & \to F \\ & x & \mapsto f(x) \end{array}$$

- Si $E \subset B$, une application $\tilde{f} : B \to F$ est **un** prolongement à B de l'application f si $\tilde{f}_{|E} = f$, c'est-à-dire si $\forall x \in E, \tilde{f}(x) = f(x)$.

Définition - Composée

Soient deux applications $f : E \to F, g : F \to G$. On définit l'application composée, notée $h = g \circ f$, de E dans G par

$$\forall x \in E, h(x) = g(f(x))$$

Exemple - Identité

Si on a une application $f : E \to F$, alors $Id_F \circ f = f$ et $f \circ Id_E = f$.

Remarque - Répresentation

Il est parfois utile de représenter les applications par un graphe.

Attention - Non commutativité

En général, même lorsque les deux applications $g \circ f$ et $f \circ g$ ont un sens, elles sont différentes.

Proposition - Associativité de $\circ$

Pour trois applications $E \xrightarrow{f} F \xrightarrow{g} G \xrightarrow{h} H$ on a

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

On peut donc noter $h \circ g \circ f$.

Démonstration

$h \circ (g \circ f) = (h \circ g) \circ f$ sont toutes deux des applications de F dans H.
Soit $x \in F$,

$$[h \circ (g \circ f)](x) = h\big(g(f(x)\big) = (h \circ g)(f(x)) = [(h \circ g) \circ f](x)$$

□

2.2. Bijections (injections et surjections)

Applications injectives ou surjectives

Heuristique - Résoudre une équation

Une fonction est de la forme : $E \xrightarrow{f} F$. A tout x de E, f donne une valeur de F.
Résoudre une équation est toujours le problème inverse :

Sont données : $E \xrightarrow{f} F$ et $b \in F$. Il s'agit de trouver $x \in E$ tel que $f(x) = b$.
Les questions naturelles sont les suivantes :
- Cette équation admet-elle (au moins) une solution ?
- Cette équation admet-elle au plus une solution ?
- Cette équation admet-elle exactement une solution ? Ce qui évite les quiproquos…

Pour aller plus loin - Exemples

Donner E, F, f et b pour les équations :
- $y' + y = x$
- $x^2 + 3x - 4 = 2$
- $\begin{cases} 2x + y = 1 \\ x - y = 2 \end{cases}$

Définition - Injection et surjection
Soit $f : E \to F$ une application. On dit que
- f est injective (est une injection) si $\forall (x,x') \in E^2, f(x) = f(x') \Rightarrow x = x'$;
- f est surjective (est une surjection) si $\forall y \in F, \exists x \in E \,|\, y = f(x)$.

Remarque - Notation
On pourra noter $f : E \hookrightarrow F$ pour exprimer que f est une application injective de E sur F.
On pourra noter $f : E \twoheadrightarrow F$ pour exprimer que f est une application surjective de E sur F.
Comment écrire une flèche de bijection? $E \hookrightarrow\!\!\!\!\rightarrow F$ Exercice
Montrer que f est injective ssi $\forall\, b \in F$, $f(x) = b$ admet au plus une solution.
Montrer que f est surjective ssi $\forall\, b \in F$, $f(x) = b$ admet toujours (au moins) une solution.

Correction
Supposons f injective.
Si $f(x) = b$ admet deux solutions x_1 et x_2, alors $f(x_1) = f(x_2)$, impossible si f injective.
Si $\forall\, b \in F$, $f(x) = b$ admet au plus une solution, alors $f(x) = f(x')(= b)$ donc $x = x^{pr\,ime}$
La deuxième équivalence correspond exactement à la définition de la surjection.

Savoir faire - Autres formulations équivalentes (injectivité, surjectivité)
Il y a différentes façons équivalentes de formuler ces propriétés :
- Dire que f est injective revient à dire (par contraposée) que :
$$\forall (x,x') \in E^2, x \neq x' \Rightarrow f(x) \neq f(x')$$
c'est-à-dire que deux éléments distincts de l'ensemble de départ ont des images distinctes.
- Dire que f est surjective revient à dire que tout élément de l'ensemble d'arrivée possède au moins un antécédent.

Exemple - $x \mapsto x^2$, $x \mapsto x^3$, $x \mapsto \sin x$
Les applications de $\mathbb{R}$ dans $\mathbb{R}$ suivantes sont-elles injectives? surjectives?
$$f_1 : x \mapsto x^2, \quad f_2 : x \mapsto x^3, \quad f_3 : x \mapsto \sin x$$
f_1 n'est ni injective ni surjective de $\mathbb{R}$ sur $\mathbb{R}$, elle est surjective de $\mathbb{R}$ sur $\mathbb{R}_+$, puis même injective de $\mathbb{R}_+$ sur $\mathbb{R}_+$ ou de $\mathbb{R}_-$ sur $\mathbb{R}_+$.
f_2 est injective et surjective de $\mathbb{R}$ sur $\mathbb{R}$.
f_3 est ni injective ni surjective de $\mathbb{R}$ sur $\mathbb{R}$, elle est surjective de $\mathbb{R}$ sur $[-1,1]$, puis même injective de $[\frac{\pi}{2} + k\pi, \frac{\pi}{2} + (k+1)\pi]$ sur $[-1,1]$.
Exercice
L'application
$$\begin{array}{rccc} f : & \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (x,y) & \mapsto & (x-y, 2x+y) \end{array}$$
est-elle injective ? surjective ?
Mêmes questions avec
$$\begin{array}{rccc} f : & \mathbb{R}^2 & \to & \mathbb{R}^3 \\ & (x,y) & \mapsto & (x-y, 2x+y, x-3y) \end{array}$$

Correction
$(x-y, 2x+y) = (a,b) \iff (x,y) = (\frac{a+b}{3}, \frac{b-2a}{3})$.
Donc f est injective et surjective.
$(x-y, 2x+y, x-3y) = (a,b,c) \iff (x,y) = (\frac{a+b}{3}, \frac{b-2a}{3})$ avec $c = \frac{7a-2b}{3}$.
Donc f est injective mais pas surjective (si $c \neq \frac{7a-2b}{3}$, pas de solution...).

Nous ferons plus tard une étude plus complète de l'étude des systèmes linéaires.
Exercice
$$\begin{array}{rccc} f : & \mathbb{C} & \to & \mathbb{C}^* \\ & z & \mapsto & \exp z \end{array}$$

est-elle injective ? surjective ?

Correction
Elle n'est pas injective : $1 = e^0 = e^{2i\pi}$.
En revanche, exp est bien surjective de $\mathbb{C}$ sur $\mathbb{C}^*$. En effet, si $z = \rho e^{i\theta} \neq 0$,
$\exp\left(\ln(\rho) + i\theta\right) = \exp^{\ln\rho} e^{i\theta} = z$.

Remarque - Les ensembles qui sont importants!
On remarquera que :
- c'est l'ensemble de départ joue un rôle important pour l'injectivité,
- c'est l'ensemble d'arrivée joue un rôle important dans la surjectivité.

Heuristique - Stratégies
Soit $f : E \to F$. Il est pratique que f soit bijective, mais cela ne nous appartient pas en règle générale.
Toutefois, il est possible de rendre :
- f surjective en restreignant « simplement » l'ensemble d'arrivée à $f(E)$.
- f injective en restreignant l'ensemble de départ, ou plus fréquemment en considérant non plus $f : E \text{ø} F$, mais $\hat{f} : \frac{E}{\mathcal{R}_f} \to F, \overline{x} \mapsto f(x)$.

Exercice
Montrer que pour cette dernière stratégie, la fonction $\hat{f}$ est bien définie et qu'elle est injective

Correction
Si $\overline{x} = \overline{y}$, alors $f(x) = f(y)$ et donc il n'y a pas de problème pour écrire $\hat{f}(\overline{x})$.
Elle est injective, car si $f(\overline{x}) = f(\overline{x'})$, alors $f(x) = f(x')$ et donc $x \mathcal{R}_f x'$ et donc $\overline{x} = \overline{x'}$.

Théorème - Propriétés des composées
Soient $f : E \to F$ et $g : F \to G$ deux applications.
Si f et g sont injectives (respectivement surjectives), alors $g \circ f$ est injective (resp. surjective).

Démonstration
Supposons que f et g sont injectives.
Soient $x, x' \in G$ tel que $g \circ f(x) = g \circ f(x')$.
Par injectivité de g : $f(x) = f(x')$
Par injectivité de f : $x = x'$
Donc $g \circ f$ est injective.
Supposons que f et g sont surjectives.
Soit $y \in G$,
par surjectivité de g, il existe $u \in F$ tel que $g(u) = y$.
par surjectivité de f, il existe $x \in E$ tel que $f(x) = u$.
Donc $g \circ f(x) = g(f(x)) = g(u) = y$
Donc $g \circ f$ est surjective.
□

Exercice
Soient $f : E \to F$ et $g : F \to G$ deux applications. Montrer que :
- si $g \circ f$ est injective, alors f est injective ;
- si $g \circ f$ est surjective, alors g est surjective.

Correction
Supposons que $g \circ f$ est injective.
Soient $x, x' \in E$ tel que $f(x) = f(x')$.
alors $g(f(x)) = g(f(x'))$, donc $x = x'$ car $g \circ f$ injective.
Par conséquent f est injective.
Supposons que $g \circ f$ est surjective.
Soit $y \in G$. Alors il existe $x \in E$ tel que $g \circ f(x) = y$.
donc avec $X = f(x)$, on a $g(X) = y$.
Par conséquent f est surjective.

Applications bijectives

Pour que l'equation $f(x) = b$ admette une unique solution, quel que soit $b \in F$, il faut (et il suffit) que f soit bijective :

Définition - Application bijective
Soit $f : E \to F$ une application. On dit que f est bijective (ou est une bijection) de E sur F si si f est injective et surjective.
Dire que f est bijective revient à dire que :

$$\forall\, y \in F, \exists\, !x \in E \quad \text{tel que} \quad y = f(x)$$

c'est-à-dire que tout élément de l'ensemble d'arrivée possède un et un seul antécédent.

Définition - Application réciproque
Soit f une bijection de E sur F, on définit une application g par

$$\begin{array}{rccl} g: & F & \to & E \\ & y & \mapsto & x \quad | \, y = f(x) \text{ (unique antécédent de } y \text{ par } f) \end{array}$$

Cette application g est elle-même bijective et appelée bijection réciproque de f, et notée f^{-1}.

Démonstration
Il faut montrer que g ainsi définie est bien bijective.
Soit $x \in E$, alors prenons $y = f(x)$, on a donc $g(y) = x$. Donc g est surjective.
Si $g(y) = g(y') = x$, alors cela signifie que $y = f(x) = y'$. Donc g est injective. □

Savoir faire - Critère pour montrer la bijectivité
Soient $f : E \to F$ et $g : F \to E$ deux applications telles que $g \circ f = Id_E$ et $f \circ g = Id_F$.
Alors f et g sont bijectives et $g = f^{-1}$

Exercice
Soit

$$f: \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & n+1 \end{array} \quad \text{et} \quad g: \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \begin{cases} 0 \text{ si } n = 0 \\ n-1 \text{ si } n \neq 0 \end{cases} \end{array}$$

Etudier l'injectivité et la surjectivité des applications f et g.
Déterminer les applications $g \circ f$ et $f \circ g$. Conclusion ?

Correction
$g(0) = g(1) = 0$, donc g n'est pas injective (donc pas bijective).
0 n'a pas d'antécédent par f, donc f n'est pas surjective (ni bijective).
Pour tout $n \in \mathbb{N}$, $g \circ f(n) = n$ en revanche $f \circ g(n) = n$ pour $n \neq 0$, mis $f \circ g(0) = f(0) = 1$.
Conclusion : il faut bien les deux conditions $f \circ g = Id_F$ ET $g \circ f = Id_E$ pour affirmer la bijectivité.

Proposition - Relation entre f et f^{-1}
Si f est une bijection de E sur F, on a

$$\begin{array}{ll} \forall x \in E, (f^{-1} \circ f)(x) = x & \text{soit } f^{-1} \circ f = Id_E; \\ \forall y \in F, (f \circ f^{-1})(y) = y & \text{soit } f \circ f^{-1} = Id_F; \\ y = f(x) \iff x = f^{-1}(y); & \\ (f^{-1})^{-1} = f. & \end{array}$$

Démonstration
Soit $x \in E$, avec $y = f(x)$, on $f^{-1}(f(x)) = f^{-1}(y) = x$ car $y = f(x)$. Donc $f^{-1} \circ f = Id_E$.
Soit $y \in F$, notons $x = f^{-1}(y)$, donc $y = f(x)$ et ainsi : $f(f^{-1}(y) = f(x) = y$. Donc $f \circ f^{-1} = Id_F$.
L'équivalence proposée découle de la définition.
$(f^{-1})^{-1} : E \to F, z \mapsto y$ tel que $f^{-1}(y) = z$, i.e. $y = f(z)$. Ainsi $\forall\, z \in E, (f^{-1})^{-1}(z) = f(z)$. □

Pour aller plus loin - Homographie de $\mathbb{C}$
Comme le montre l'exercice, il y a une certaine stabilité pour les fonction homographique $z \mapsto \dfrac{az+b}{cz+d}$ (réciproque de la même forme).
Il s'agit d'une famille de transformation de $\mathbb{C}$ des étudiée : en particulier elle conserve le birapport!
Notons que dans ce cas, il vaut mieux se placer sur $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$...

Exercice
Soit

$$f: \begin{array}{ccc} \mathbb{C} \setminus \{i\} & \to & \mathbb{C} \\ z & \mapsto & \dfrac{z+2i}{z-i} \end{array}$$

Montrer que l'on peut trouver $F \subset \mathbb{C}$ tel que l'application $\hat{f}$ de $\mathbb{C} \setminus \{i\}$ dans F définie par $\hat{f}(z) = f(z)$ soit une bijection. Déterminer sa bijection réciproque.

Correction
$f(z) = Z \iff \dfrac{z+2i}{z-i} = Z \iff z+2i = Z(z-i) \iff z(1-Z) = -2i - Zi \iff z = \dfrac{(Z+2)i}{Z-1}$.
Donc si $Z \neq 1$, $f(z) = Z \Longrightarrow h(Z) = z$, avec $h : Z \mapsto \frac{(Z+2)i}{Z-1}$.
Ainsi $\hat{f} : \mathbb{C} \setminus \{i\} \to \mathbb{C} \setminus \{1\}, z \mapsto f(z)$ est bijective et admet une application réciproque : $\hat{h}$.
Il est possible de donner une interprétation géométrique à ce calcul.

Théorème - Bijection réciproque d'une composée
Si $f : E \to F$ et $g : F \to G$ sont deux bijections, alors $g \circ f$ est une bijection et

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Démonstration
$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ f = Id_E$.
$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ f \circ f^{-1} \circ g^{-1} = g \circ g^{-1} = Id_F$.
On a ainsi et la bijectivité de $g \circ f$ et la valeur de $(g \circ f)^{-1}$. □

3. Image directe et image réciproque d'un ensemble

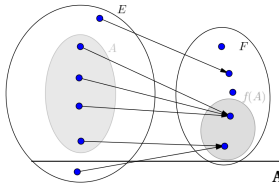
Heuristique - Si les applications ne sont pas bijectives
Si $f : E \to F$ n'est pas bijective, peut-on néanmoins trouver « comme » une application réciproque.
On a vu que tout n'est pas perdu, à condition de limiter l'ensemble de départ (pour tenter de gagner l'injectivité) et de réduire l'ensemble d'arrivée (pour gagner la surjectivité).
Dans le premier cas, on s'intéressera à l'ensemble réciproque de F par f, c'est un sous-ensemble de E.
Dans le second cas, on s'intéressera à l'ensemble image de E par f, c'est un sous-ensemble de F.

3.1. Image directe

Définition - Ensemble image
Soit $f : E \to F$ une application.
L'ensemble des éléments de F qui admettent un antécédent par f est une partie de F appelée ensemble image ou image de f et notée $\operatorname{Im} f$:

$$\operatorname{Im} f = \{y \in F \,|\, \exists x \in E; y = f(x)\}.$$

Représentation - Image directe
Avec un graphe :



Remarque - Autre écriture
On peut écrire $\operatorname{Im} f = \{f(x) \,|\, x \in E\}$

Savoir faire - Critère de surjectivité.
On a donc

$$f \text{ surjective} \Leftrightarrow \operatorname{Im} f = F$$

Et toute application $f : E \to F$ définit une surjection en restreignant l'ensemble d'arrivée, c'est à dire en considérant l'application de E dans $\operatorname{Im} f$ qui a x associe $f(x)$ (que l'on continue usuellement à noter f, on

, dit alors que f est surjective de E sur Im f).

Définition - Image directe
Soient $f : E \to F$ une application et $A \subset E$. On appelle image (directe) de A par f la partie de F, notée $f(A)$, définie par

$$f(A) = \{y \in F \mid \exists x \in A; y = f(x)\} = \{f(x) \mid x \in A\} = \{f(x); x \in A\}.$$

Remarque - Autres notations en exploitant Im f
On constate que l'on a également Im $f = f(E)$.
Donc f est surjective si et seulement si $f(E) = F$.
Et $f(A) = \text{Im } f_{|A}$.

Savoir faire - Montrer que $y \in f(A)$
Pour montrer que $y \in f(A)$ il faut trouver $x \in A$ tel que $f(x) = y$.

Proposition - Stabilité et image
Soit $f : E \to F$ une application et $A_1, A_2 \subset E$. Alors

$$A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2);$$
$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2);$$
$$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

Démonstration
Supposons que $A_1 \subset A_2$,
Soit $y \in f(A_1)$, alors il existe $x \in A_1$ tel que $y = f(x)$.
Mais $x \in A_2$ également, donc $y = f(x) \in f(A_2)$.
Donc $f(A_1) \subset f(A_2)$.
Soit $y \in f(A_1 \cup A_2)$ donc il existe $x \in A_1 \cup A_2$ tel que $y = f(x)$.
donc il existe $x \in A_1$ tel que $y = f(x)$ ou $x \in A_2$ tel que $y = f(x)$
donc $y \in f(A_1)$ ou $y \in f(A_2)$ i.e. $y \in f(A_1) \cup f(A_2)$.
Réciproquement, soit $y \in f(A_1) \cup f(A_2)$.
donc $y \in f(A_1)$ ou $y \in f(A_2)$
donc il existe $x_1 \in A_1$ tel que $y = f(x_1)$ ou $x_2 \in A_2$ tel que $y = f(x_2)$
donc il existe $x_1 \in A_1 \cup A_2$ tel que $y = f(x_1)$ ou $x_2 \in A_2 \cup A_1$ tel que $y = f(x_2)$
dans tous les cas $y \in f(A_1 \cup A_2)$.
Soit $y \in f(A_1 \cap A_2)$ donc il existe $x \in A_1 \cap A_2$ tel que $y = f(x)$.
donc il existe $x \in A_1$ tel que $y = f(x)$ et $x \in A_2$ tel que $y = f(x)$
donc $y \in f(A_1)$ et $y \in f(A_2)$ i.e. $y \in f(A_1) \cap f(A_2)$. □

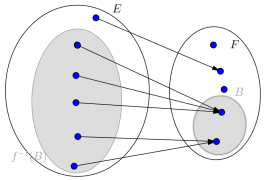
Attention - Une seule inclusion pour l'intersection!
On fera bien attention qu'il n'y a pas l'égalité : $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$
Pour se convaincre on peut penser au cas où $A_1 \cap A_2 = \emptyset$.
Par exemple, avec $f : x \mapsto x^2$, $A_1 = [-2,-1]$ et $A_2 = [1,2]$,
alors $f(A_1 \cap A_2) = f(\emptyset) = \emptyset$, et $f(A_1) \cap f(A_2) = [1,4] \cap [1,4] = [1,4]$

Définition - Partie stable et application induite
Soit $f : E \to E$ une application. On dit qu'une partie A de E est stable par f si $f(A) \subset A$.
On appelle application induite par f sur A l'application

$$A \to A$$
$$x \mapsto f(x)$$

Pour aller plus loin - Suite de la forme $u_{n+1} = f(u_n)$
Pour les suites définies par récurrence par une fonction f itérée, ces notions de partie stable (souvent intervalle) ou de points fixes sont très importants. Nous reviendrons sur ces notions

Représentation - Image réciproque
Avec un graphe :



Exemple - Point fixe
Par exemple pour $x \in E$, le singleton $\{x\}$ est stable si et seulement si $f(x) = x$, c'est-à-dire si x est un *point fixe* de f.

3.2. Image réciproque d'un ensemble

Définition - Image réciproque
Soient $f : E \to F$ une application et $B \subset F$. On appelle image réciproque de B par f la partie de E, notée $f^{-1}(B)$ (ou $[f \in B]$ en probabilité), définie par

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}.$$

C'est donc l'ensemble formé des antécédents par f des éléments de B.

Exemple - Pour $x \mapsto x^2$ et $x \mapsto \exp x$
Par exemple pour

$$f : \begin{array}{l} \mathbb{R} \to \mathbb{R} \\ x \mapsto x^2 \end{array}$$

on a $f^{-1}([0,4]) = [-2,0,2]$, $f^{-1}(\{4\}) = \{-2,2\}$, $f^{-1}([-1,4[) = [-2,2]$ et pour

$$g : \begin{array}{l} \mathbb{C} \to \mathbb{C} \\ z \mapsto \exp z \end{array}$$

on a $g^{-1}(\{0\}) = \emptyset$, $g^{-1}(\{1\}) = \{2ik\pi \mid k \in \mathbb{Z}\}$, $g^{-1}(\mathbb{R}) = \{L + 2ik\pi \mid L \in \mathbb{R}, k \in \mathbb{Z}\}$

Attention - Ne pas confondre la fonction f^{-1} et l'ensemble $f^{-1}(B)$
Il s'agit d'une notation qui ne demande pas que f soit bijective. (voir l'exemple précédent)

Savoir faire - Montrer que $x \in f^{-1}(B)$
Pour montrer que $x \in f^{-1}(B)$ il faut montrer que $f(x) \in B$.

Exemple - Fonction sin
Soit

$$f : \begin{array}{l} \mathbb{R} \to \mathbb{R} \\ x \mapsto \sin x \end{array}$$

Déterminer, si cela a un sens : $f(0)$; $f(\{0\})$; $f([0,\pi[)$; $f(\mathbb{R})$; $f^{-1}(0)$; $f^{-1}(\{0\})$; $f^{-1}([0,+\infty[)$.
$f(0) = 0$; $f(\{0\}) = \{0\}$; $f([0,\pi[) = [0,1]$; $f(\mathbb{R}) = [-1,1]$; $f^{-1}(0)$ pas de sens;
$f^{-1}(\{0\}) = \pi\mathbb{Z}$; $f^{-1}([0,+\infty[) = \bigcup_{k\in\mathbb{Z}} [2k\pi, (2k+1)\pi]$.

Remarque - Et si f est bijective
Soit $f : E \to F$ un bijection. Pour $B \subset F$ la notation $f^{-1}(B)$ n'est pas ambigüe.
En effet, ici f^{-1} existe, et $f^{-1}(B)$ est l'image de B par f^{-1}. Donc

$$f^{-1}(B) = \text{Im } f^{-1}_{|B} = \{f^{-1}(y), y \in B\} = \{x \in E \mid \exists\, y \in B, x = f^{-1}(y)\}$$
$$= \{x \in E \mid f(x)(= y) \in B\} = f^{-1}(B)$$

Proposition - Stabilité et image réciproque
Soit $f : E \to F$ une application et $B_1, B_2 \subset F$. Alors

$$B_1 \subset B_2 \Rightarrow f^{-1}(B_1) \subset f^{-1}(B_2);$$
$$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2);$$
$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2).$$

xcte et réci-

Démonstration
Supposons que $B_1 \subset B_2$,
Soit $x \in f^{-1}(B_1)$, alors $f(x) \in B_1 \subset B_2$ Donc $x \in f^{-1}(B_2)$
Donc $f^{-1}(B_1) \subset f^{-1}(B_2)$.
On peut reconduire le même genre de démonstration que plus haut. Ou autre :

$$f^{-1}(B_1 \cap B_2) = \{x \in E \mid f(x) \in B_1 \cap B_2\} = \{x \in E \mid f(x) \in B_1 \text{ et } f(x) \in B_2\}$$
$$= \{x \in E \mid x \in f^{-1}(B_1) \text{ et } x \in f^{-1}(B_2)\} = f^{-1}(B_1) \cap f^{-1}(B_2)$$

(On a directement l'égalité sans faire la double inclusion).
De même :

$$f^{-1}(B_1 \cup B_2) = \{x \in E \mid f(x) \in B_1 \cup B_2\} = \{x \in E \mid f(x) \in B_1 \text{ ou } f(x) \in B_2\}$$
$$= \{x \in E \mid x \in f^{-1}(B_1) \text{ ou } x \in f^{-1}(B_2)\} = f^{-1}(B_1) \cup f^{-1}(B_2)$$

□

Attention - Attention $f^{-1}(f(A)) \neq A$ et $f(f^{-1})(B) \neq B$
Le schéma montre sur un exemple qu'on a pas l'égalité…
On a au mieux : $A \subset f^{-1}(f(A))$ et $f(f^{-1}(B)) \subset B$

Exercice
Démontrer ces inclusions. Donner des contre-exemple de l'inclusion réciproque

Correction
Soit $x \in A$, alors $f(x) \in f(A)$ et donc $x \in f^{-1}(f(A))$.
De même si $y \in f(f^{-1}(B))$, alors il existe $x \in f^{-1}(B)$ tel que $y = f(x)$.
Mais comme $x \in f^{-1}(B)$, cela signifie que $f(x) \in B$, donc $y = f(x) \in B$.
Prenons $f : x \mapsto x^2$, $A = [0,2]$, $f(A) = [0,4]$ et $f^{-1}(f(A)) = [-2,2] \supset A$.
C'est un problème d'injectivité De même avec $B = [-1,2]$, $f^{-1}(B) = [-\sqrt{2},\sqrt{2}]$, $f(f^{-1}(B)) = [0,2] \subset B$ *C'est un problème de surjectivité*

4. Fonction indicatrice

4.1. Définition

Définition - Fonction indicatrice
Soit E un ensemble. Pour $A \subset E$, on appelle fonction indicatrice de A l'application de E dans $\mathbb{R}$, notée $\mathbb{1}_A$ ou χ_A, définie par

$$\forall x \in E, \mathbb{1}_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$$

Remarque - Pourquoi et comment exploiter une telle fonction ?
Cela permet de représenter certaines fonctions définies par morceaux par une seule expression (très utile en probabilités) sur $\mathbb{R}$, par exemple la loi uniforme sur $[a,b]$ a pour densité $\frac{1}{b-a}\mathbb{1}_{[a,b]}$ et la loi exponentielle de paramètre λ a pour densité la fonction définie sur $\mathbb{R}$ par $t \mapsto \lambda e^{-\lambda t}\mathbb{1}_{[0,+\infty[}(t)$.
Cela permet également de ramener certaines égalités d'ensemble à des calculs sur les fonctions.

4.2. Propriétés ensemblistes et calcul avec fonctions indicatrices

Proposition - Propriété essentielle de la fonction indicatrice
Soient A et B deux parties de E. Alors

$\mathbb{1}_A \leqslant \mathbb{1}_B \Leftrightarrow A \subset B$ $\mathbb{1}_A = \mathbb{1}_B \Leftrightarrow A = B$ (d'où le nom de fonction caractéristique);
$\mathbb{1}_{\complement_E A} = 1 - \mathbb{1}_A$;
$\mathbb{1}_{A\cap B} = \mathbb{1}_A \times \mathbb{1}_B$;
$\mathbb{1}_{A\cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \times \mathbb{1}_B$.

Exercice
Soit E un ensemble. Pour deux parties A et B de E, on appelle différence symétrique de ces deux parties la partie de E définie par

$$A\triangle B = (A \cup B) \setminus (A \cap B).$$

Comment exprimer la fonction indicatrice de $A\triangle B$ à l'aide des fonctions indicatrices de A et B ?
En déduire que pour trois parties A, B, C de E, on a $(A\triangle B)\triangle C = A\triangle(B\triangle C)$.

Correction
$\mathbb{1}_{A\triangle B} = \mathbb{1}_{A\cup B} - \mathbb{1}_{A\cap B} = \mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B$ On a donc $A\triangle B = B\triangle A$ (ce qui est assez évident).
On a également :

$$\begin{aligned}\mathbb{1}_{(A\triangle B)\triangle C} &= \mathbb{1}_{A\triangle B} + \mathbb{1}_C - 2\mathbb{1}_{A\triangle B}\mathbb{1}_C \\ &= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2[\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_A\mathbb{1}_C\mathbb{1}_B\mathbb{1}_C] \\ &\quad + 4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C\end{aligned}$$

Ce résultat est symétrique en A, b et C, donc : $(A\triangle B)\triangle C = (B\triangle C)\triangle A = A\triangle(B\triangle C)$.

Démonstration
Si $A \leqslant B$. Soit $x \in E$ Supposons que $\mathbb{1}_A(x) = 1$, alors $x \in A$ donc $x \in B$ donc $\mathbb{1}_B(x) = 1$.
Donc, comme les indicatrices sont à valeurs dans $\{0,1\}$, on a $\mathbb{1}_A \leqslant \mathbb{1}_B$.
Réciproquement, si $\mathbb{1}_A \leqslant \mathbb{1}_B$. Soit $x \in A$, alors $\mathbb{1}_B(x) \geqslant \mathbb{1}_A(x) = 1$, donc $x \in B$.
La double inclusion signifie la double inégalité. Donc $A = B$ ssi $\mathbb{1}_A = \mathbb{1}_B$.
$x \in \complement_E(A) \leftrightarrow x \notin A \leftrightarrow \mathbb{1}_A(x) = 0 \leftrightarrow 1 - \mathbb{1}_A(x) = 1$.
Quatrième proposition :

$$\mathbb{1}_{A\cap B}(x) = 1 \Longleftrightarrow x \in A \cap B \Longleftrightarrow x \in A \text{ et } x \in B$$
$$\Longleftrightarrow \mathbb{1}_A(x) = 1 \text{ et } \mathbb{1}_B(x) = 1 \Longleftrightarrow 1 = \mathbb{1}_A(x) \times \mathbb{1}_B(x) = \left(\mathbb{1}_A \times \mathbb{1}_B\right)(x)$$

car pour $a, b \in \{0,1\}$, $a \times b = 1$ si et seulement si $a = b = 1$ Comme il n'y a que deux valeurs, on peut affirmer $\mathbb{1}_{A\cap B} = \mathbb{1}_A \times \mathbb{1}_B$.
Cinquième proposition :
On peut aussi faire un autre type de démonstration, avec comme une table de vérité

$x \in ?$	$\mathbb{1}_{A\cup B}(x)$	$\mathbb{1}_A(x)$	$\mathbb{1}_B(x)$	$\mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \times \mathbb{1}_B](x)$
$x \in A, x \in B$	1	1	1	$1+1-1=1$
$x \in A, x \notin B$	1	1	0	$1+0-0=1$
$x \notin A, x \in B$	1	0	1	$0+1-0=1$
$x \notin A, x \notin B$	0	0	0	$0+0-0=0$

□

On retrouve évidemment des résultats comparables à ceux vus en logique…

5. Cardinal d'ensemble fini

5.1. Principe des tiroirs

Nous considérons ici que l'ensemble $\mathbb{N}$ est bien connu. Nous expliquerons au chapitre suivant sa construction, en attendant, il nous faut savoir que c'est l'ensemble d'appui du raisonnement par récurrence….
On rappelle que l'on note $\mathbb{N}_k = \{1,2,3,\dots k-1,k\}$, l'ensemble des k premiers entiers naturels non nuls.
On commence par deux lemmes.

Lemme - Injection de $\mathbb{N}_n$ sur $\mathbb{N}_p$. Principe des tiroirs (DIRICHLET)
Soient $n, p \in \mathbb{N}^*$.
S'il existe une fonction $\varphi : \mathbb{N}_n \to \mathbb{N}_p$ injective, alors $n \leqslant p$.
Sous sa forme contraposée : si $\varphi : \mathbb{N}_n \to \mathbb{N}_p$ avec $n > p$,
Alors il existe $x \neq x\prime \in \mathbb{N}_n$ tel que $\varphi(x) = \varphi(x')$ (φ non injective).

Démonstration
On peut le démontrer par récurrence sur n.
Posons, pour tout entier $n \geqslant 1$, $\mathscr{P}_n$: « $\forall\ p \geqslant 1$, ($\exists\ \varphi : \mathbb{N}_n \to \mathbb{N}_p$ injective)$\Rightarrow n \leqslant p$ ».
— Le cas $n = 1$ est simple, car nécessairement $p \geqslant 1$.
Donc $\mathscr{P}_1$ est vraie.
— Soit $n \in \mathbb{N}^*$. On suppose que $\mathscr{P}_n$ est vraie.
Soit $p \in \mathbb{N}^*$. On suppose qu'il existe $\varphi : \mathbb{N}_{n+1} \to \mathbb{N}_p$ injective.
On note $r = \varphi(n+1) \in \mathbb{N}_p$.
On considère $\psi : \mathbb{N}_p \to \mathbb{N}_p$, $k \mapsto \begin{cases} p & \text{si } k = r \\ r & \text{si } k = p \\ k & \text{sinon} \end{cases}$.
En fait, ψ intervertit p et r. ψ est une bijection de $\mathbb{N}_p$ sur $\mathbb{N}_p$.
Donc, par composition, $\psi \circ \varphi : \mathbb{N}_{n+1} \to \mathbb{N}_p$, injective et $(\psi \circ \varphi)(n+1) = \psi(r) = p$.
Notons $\Psi = (\psi \circ \varphi)_{|\mathbb{N}_n}$, alors Ψ est également une injection.
Et $\Psi : \mathbb{N}_n \to \mathbb{N}_{p+1}$.
On peut appliquer $\mathscr{P}_n$ avec Ψ. Et donc $n \leqslant p - 1$.
Donc $\mathscr{P}_{n+1}$ est vérifiée.
□

5.2. Classe des ensembles de même cardinal

Lemme - $\mathscr{R}$ comme relation d'équivalence
On note $\mathscr{R}$, la relation entre ensembles définies par :
$$E \mathscr{R} F \iff \exists\ \varphi : E \to F, \text{bijective}$$
$\mathscr{R}$ est une relation d'équivalence.

Démonstration
On vérifie les trois qualités d'une relation d'équivalence :
— Pour tout ensemble E, l'application $\varphi : E \to E, x \mapsto x$ est bijective de E sur E.
Donc pour tout E, $\quad E \mathscr{R} E$ i.e. $\mathscr{R}$ est reflexive.
— Soient deux ensembles E et F tels que $E \mathscr{R} F$.
Alors il existe $\varphi : E \to F$ bijective de E sur F.
Elle admet une réciproque $\varphi^{-1} : F \to E$ bijective.
Donc pour tout E, F, $\quad E \mathscr{R} F \Rightarrow F \mathscr{R} E$ i.e. $\mathscr{R}$ est symétrique.
— Soient trois ensembles E, F et G tels que $E \mathscr{R} F$ et $F \mathscr{R} G$.
Alors il existe $\varphi_1 : E \to F$ et $\varphi_2 : F \to G$ bijectives.
$\phi = \varphi_2 \circ \varphi_1$ est une bijection de E sur G.
Donc pour tout E, F, G, $\quad E \mathscr{R} F$ et $F \mathscr{R} G \Rightarrow E \mathscr{R} G$ i.e. $\mathscr{R}$ est transitive.
□

Définition - Ensemble de cardinal n. Ensemble fini.
Soit $n \in \mathbb{N}$.
On dit qu'un ensemble E est fini de cardinal $n (\in \mathbb{N})$, si $E \mathscr{R} \mathbb{N}_n$. On note $\text{Card}(E) = n$
On dit qu'un ensemble E est fini, si il existe $n \in \mathbb{N}$ tel que E est fini de cardinal n.

Exemple - Cardinal de $E = \{1, 2, \dots k\}$
L'identité est bijective de E sur $\mathbb{N}_k$, donc $\text{card}(E) = k$.
Exercice
Montrer que si $n, p \in \mathbb{N}$ et $n < p$, alors on n'a pas $\mathbb{N}_n \mathscr{R} \mathbb{N}_p$.

Correction
On démontre le résultat contraposé.
Soient $n, p \in \mathbb{N}$. On suppose que $\mathbb{N}_n \mathscr{R} \mathbb{N}_p$.

Alors il existe $\varphi : \mathbb{N}_n \to \mathbb{N}_p$, bijective donc injective.
Et d'après le résultat admis : $n \leqslant p$.
Et par symétrie de la relation $\mathscr{R}$, on a de même : $p \leqslant n$.
Ainsi $n = p$. Donc par contraposée :
$$n < p \Longrightarrow n \neq p \Longrightarrow \text{NON } [\mathbb{N}_n \mathscr{R} \mathbb{N}_p]$$

Proposition - Classe d'équivalence pour $\mathscr{R}$
Sur l'ensemble des ensembles $E, F, \dots$ de cardinaux finis, on a l'équivalence : $E \mathscr{R} F \iff \text{Card}(E) = \text{Card}(F)$.
Les classes d'équivalence pour $\mathscr{R}$ sont formé des ensembles de même cardinaux.
On peut les *paramétrer* par leur cardinaux

***Pour aller plus loin - Construction de* $\mathbb{N}$**
Un mode de construction de $\mathbb{N}$ *qui a fait grand bruit au début du XX*^{e} *siècle consistait à dire que l'ensemble des nombres entiers était en fait l'ensemble des cardinaux possibles pour les ensembles finis.*
Qu'est-ce que 3*, un représentant de tous les ensembles à 3 éléments. Si on veut…*

5.3. Cardinal, fonction indicatrice et somme (finie)

Proposition - Calcul avec l'indicatrice
Soit E, un ensemble fini et A un sous-ensemble de E.
Alors le calcul $\sum_{x \in E} \mathbb{1}_A(x)$ a un sens et il vaut $\text{Card}(A)$.

Démonstration
Comme E est un ensemble fini, il existe $k \in \mathbb{N}$ et $\varphi : E \to \mathbb{N}_k$ bijective.
On peut donc écrire que $E = \{\varphi^{-1}(1), \varphi^{-1}(2) \dots \varphi^{-1}(k)\}$ que l'on préfère noter $\{x_1, x_2, \dots x_k\}$.
On a alors la somme $\sum_{x \in E} \mathbb{1}_A(x)$ qui se calcule de la façon suivante : $\sum_{i=1}^{k} \mathbb{1}_A(x_i)$.
On note alors $\varphi : A \to \mathbb{N}$, $x_h (\in A \subset E) \mapsto \sum_{i=1}^{h} \mathbf{1}_A(x_i)$. Alors
— φ est injective :
si $x_h \neq x_\ell$, alors on peut supposer $h < \ell$ (SPDG) et donc $\varphi(x_\ell) = \varphi(x_h) + \sum_{i=h+1}^{\ell} \mathbf{1}_A(x_i) \geqslant \varphi(x_h) + \mathbf{1}_A(x_\ell) \geqslant \varphi(x_h) + 1$, donc $\varphi(x_h) \neq \varphi(x_\ell)$.
— Par ailleurs, par construction $\varphi(A)$ est de la forme $\mathbb{N}_s$ avec $s = \sum_{i=1}^{k} \mathbf{1}_A(k)$:
$\varphi(x_{m+1}) - \varphi(x_m) = \mathbf{1}_A(x_{m+1}) \in \{1, 0\}$. Il ne peut y avoir de trou.
La fonction φ établit donc une bijection de A sur $\mathbb{N}_s$. Nécessairement $s = \text{Card}(A) = \sum_{i=1}^{k} \mathbf{1}_A(k)$.
□

Corollaire - Inclusion et cardinaux
Si $A \subset B (\in E)$ avec E un ensemble fini, alors $\text{Card}\, A \leqslant \text{Card}\, B$.

Démonstration
On a vu $A \subset B$ implique $\mathbb{1}_A \subset \mathbb{1}_B$.
On somme en tout x de E. □

Exercice
Soient E, un ensemble fini de cardinal n et F, un ensemble fini de cardinal m.
1. On suppose que $f : E \to F$ est une application injective.
(a) Montrer que $f(E)$ est un ensemble fini de cardinal n.
(b) Montrer que $n \leqslant m$.
2. Que se passe-t-il si f est surjective ?
3. Démontrer le théorème de Cantor-Bernstein pour des ensembles E et F finis.
$$\exists\ i : E \to F, j : F \to E \text{ injectives} \Longrightarrow \exists\ b : E \to F \text{ bijective}$$

Correction

1. (a) $E \mathscr{R} \mathbb{N}_n$. Et on note $\hat{f} : E \to f(E), x \mapsto f(x)$.
   Par définition de $f(E)$: pour tout $y \in f(E)$, il existe $x \in E$ tel que $y = f(x) = \hat{f}(x)$.
   Donc $\hat{f}$ est surjective de E sur $f(E)$.
   Et si $\hat{f}(x) = \hat{f}(x')$, alors $f(x) = f(x')$ et donc $x = x'$, car f injective.
   Donc $\hat{f}$ est injective.
   Par conséquent $\hat{f}$ est bijective de E sur $f(E)$ et donc $E \mathscr{R} f(E)$.
   Par transitivité, $f(E) \mathscr{R} \mathbb{N}_n$, $f(E)$ est un ensemble fini de cardinal n.
   (b) On note $\varphi : E \to \mathbb{N}_n$, bijective (elle existe bien car $E \mathscr{R} \mathbb{N}_n$).
   Alors φ^{-1} est injective. Il en est de même de $f \circ \varphi^{-1}$ (f est injective).
   Puis on note $\psi : F \to \mathbb{N}_m$ bijective (elle existe bien car $F \mathscr{R} \mathbb{N}_m$).
   ψ est injective et par composition :
   $$\psi \circ f \circ \varphi^{-1} : \mathbb{N}_n \to \mathbb{N}_m$$
   est également injective. Donc $n \leqslant m$.
2. Si f est surjective : $f(E) = F$, et donc $\mathrm{Card} F = \mathrm{Card} f(E)$.
   Or $\mathrm{Card}(f(E)) \leqslant \mathrm{Card} E$, donc $\mathrm{Card} F \leqslant \mathrm{Card} E$.
3. Soient E et F deux ensembles finis.
   On suppose qu'il existe $i : E \to F$ injective. Donc d'après 2., $\mathrm{Card}(E) \leqslant \mathrm{Card}(F)$.
   On suppose qu'il existe $j : F \to E$ injective. Donc d'après 2., $\mathrm{Card}(F) \leqslant \mathrm{Card}(E)$.
   Donc, par double inégalité : $\mathrm{Card}(E) = \mathrm{Card}(F)$.
   D'après la question 1.(c), cela signifie que $E \mathscr{R} F$. Et par définition, cela signifie qu'il existe une bijection de E sur F.
   $\exists\, i : E \to F, j : F \to E$ injectives $\Longrightarrow \exists\, b : E \to F$ bijective

L'exercice donne le résultat suivant (dans le cas injectif)

Proposition - Cardinaux, injectivité et surjectivité
Si E et F sont des ensembles finis.
S'il existe une fonction $f : E \to F$ injective, alors $\mathrm{card} E \leqslant \mathrm{card}(F)$ (la réciproque est vraie).
S'il existe une fonction $f : E \to F$ surjective, alors $\mathrm{card} F \leqslant \mathrm{card}(E)$ (la réciproque est vraie).

Démonstration
On a toujours $\mathrm{card} f(E) \leqslant \mathrm{card}(E)$, avec égalité ssi f injective.
On a toujours $\mathrm{card} f(E) \leqslant \mathrm{card}(F)$, avec égalité ssi f surjective. □

6. Familles

6.1. Familles quelconques

On peut définir de manière formelle la notion de famille d'éléments ou de famille d'ensemble.

Définition - Familles
Soient I et E deux ensembles. On appelle famille d'éléments de E indexée par I toute "liste" (finie ou non, avec répétitions éventuelles), notée $(a_i)_{i \in I}$, telle qu'à tout élément de I (appelé indice) soit associé un unique élément a_i de E (appelé terme d'indice i de la famille).
Cette famille peut donc être considérée comme l'application

$$\begin{array}{rcl} a : & I & \to E \\ & i & \mapsto a_i = a(i) \end{array}$$

Pour aller plus loin - Cardinal d'un ensemble
Si $A \subset E$, sont des ensembles finis.
Alors $\mathrm{Card}(A) = \sum_{x \in E} \mathbb{1}_A(x)$.
En déduire $\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$.
Que vaut $\mathrm{Card}(A \cup B \cup C) = ?$

Définition - Sous famille
Soit $(a_i)_{i \in I}$ une famille d'éléments d'un ensemble E.
Si $J \subset I$, on dit que $(a_i)_{i \in J}$ est une sous-famille de $(a_i)_{i \in I}$.
on dit également que $(a_i)_{i \in I}$ est une sur-famille de $(a_i)_{i \in J}$.

Exemple - $E = \mathbb{R}$ et $I = \mathbb{N}$
Par exemple, si $E = \mathbb{R}$ et $I = \mathbb{N}$, on définit ainsi une *suite* de réels.

Définition - Intersection et réunion d'une famille de parties
Soient un ensemble I (les indices) et un ensemble E.
On considère une famille de parties de E (c'est-à-dire une famille d'éléments de $\mathscr{P}(E)$) $(A_i)_{i \in I}$.
On note
$$\bigcap_{i \in I} A_i = \{x \in E \,|\, \forall i \in I, x \in A_i\} \text{ et } \bigcup_{i \in I} A_i = \{x \in E \,|\, \exists i \in I, x \in A_i\}.$$

Exemple - $E = \mathbb{R}$
Par exemple, si $E = \mathbb{R}$, on a

$$\bigcap_{k \in \mathbb{N}} [-k, k] = \qquad , \bigcup_{k \in \mathbb{N}} [-k, k] = \qquad , \bigcap_{k \in \mathbb{N}^*} \left]-\frac{1}{k}, \frac{1}{k}\right[= \qquad .$$

Exercice
On dit que la suite numérique (u_n) converge vers ℓ si :
$$\forall\, \epsilon > 0, \exists\, N \in \mathbb{N} \mid \forall\, n \geqslant N, \quad |u_n - \ell| < \epsilon$$

1. Montrer que $|u_n - \ell| < \epsilon \Longleftrightarrow \ell \in]u_n - \epsilon, u_n + \epsilon[$.
2. En déduire que l'ensemble des limites possibles pour la suite (u_n) est l'intersection d'une réunion d'intersection d'ensembles

Correction

1. $|u_n - \ell| < \epsilon \Longleftrightarrow -\epsilon < \ell - u_n < \epsilon \Longleftrightarrow u_n - \epsilon < \ell < u_n + \epsilon \Longleftrightarrow \ell \in]u_n - \epsilon, u_n + \epsilon[$
2. On a donc :
   $$\forall\, \epsilon > 0, \forall\, N \in \mathbb{N}, \quad \{\ell \mid \forall\, n \geqslant N, \quad |u_n - \ell| < \epsilon\} = \bigcap_{n \geqslant N}]u_n - \epsilon, u_n + \epsilon[$$
   Puis
   $$\forall\, \epsilon > 0, \quad \{\ell \mid \exists\, N \in \mathbb{N} \mid \forall\, n \geqslant N, \quad |u_n - \ell| < \epsilon\} = \bigcup_{N \in \mathbb{N}} \left(\bigcap_{n \geqslant N}]u_n - \epsilon, u_n + \epsilon[\right)$$
   Et
   $$\{\ell \mid \forall\, \epsilon > 0, \exists\, N \in \mathbb{N} \mid \forall\, n \geqslant N, \quad |u_n - \ell| < \epsilon\} = \bigcap_{\epsilon > 0} \left[\bigcup_{N \in \mathbb{N}} \left(\bigcap_{n \geqslant N}]u_n - \epsilon, u_n + \epsilon[\right) \right]$$

6.2. Famille indexée sur $\mathbb{N}$. Suites

Vocabulaire de base sur les suites (infinies)

L'ensemble E n'est pas précisé pour le moment. Cela peut être $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou autre chose ($\mathscr{M}_p(\mathbb{R})$...).
Par la suite nous pourrons avoir besoin que l'ensemble E soit ordonné.

Définition - Suite et ensemble de suites
Soit E un ensemble.
Une suite est une application $u : \mathbb{N} \to E$ (on dira aussi qu'une application de $\{n \in \mathbb{N} | n \geqslant n_0\}$ dans E où $n_0 \in \mathbb{N}$ est une suite). On note cette application sous forme indicielle :
$$(u_n)_{n \in \mathbb{N}} \quad \text{(éventuellement } (u_n)_{n \geqslant n_0} \text{) ou } (u_n)$$

On note $E^{\mathbb{N}}$ l'ensemble des suites à valeurs dans E.

Attention - Avec ou sans parenthèses
(u_n) désigne une suite alors que u_n désigne un nombre de E (le n ou $n+1$-ième terme de la suite).

Exemple - Suite (ou famille) de fonctions
Il arrivera, de plus en plus souvent durant ces années de CPGE que vous rencontriez des suites de fonctions.
On les note en générale (f_n), avec pour tout $n \in \mathbb{N}$, $f_n : I \to \mathbb{R}$.
On peut, par exemple, avoir à étudier $M_n = \sup_{x\in I} f_n(x)$, puis le comportement de la suite (M_n).

$\mathbb{N}$ est ordonnée

Heuristique - Particularité des suites aux familles
L'ensemble d'indexation des suites $\mathbb{N}$ a une particularité très importante que n'a pas I.
Il est ordonné naturellement. Ainsi, une notion importante des suites qui n'existe pas pour les familles est la notion de suite croissante que l'on verra un peu plus bas ou encore les propriétés vraies à partir d'un certain rang.
Autre propriété : si $A \subset \mathbb{N}$, alors A est borné si et seulement si A est fini.

Définition - Propriété vraie à partir d'un certain rang...
On dit qu'une propriété $p(n)$ est vérifiée à partir d'un certain rang s'il existe $n_0 \in \mathbb{N}$ tel que la propriété $p(n)$ soit vraie pour $n \geqslant n_0$.

Exercice
Quelle est le contraire, *formalisée*, d'une propriété vraie à partir d'un certain rang ?
Que penser également de $A = \{n \in \mathbb{N} \mid p(n) \text{ vraie}\}$

Correction
La formalisation positive est : $\exists\, n_0 \in \mathbb{N}$ tel que $\forall\, n \geqslant n$, $p(n)$ est vraie. La négation donne : $\forall\, n \in \mathbb{N}$, $\exists\, n' \geqslant n$ tel que $p(n)$ fausse.
Dans le premier cas A est bornée (par n_0) et dans le second cas A est infini.

Analyse - Suites extraites (sous-suite)
Si on enlève des termes d'une suite, on obtient une suite extraite.
Soit E une partie infinie de $\mathbb{N}$. On dit $(u_n)_{n\in\mathbb{E}}$ est une suite extraite de $(u_n)_{n\in\mathbb{N}}$.
Le problème est que l'indexation sur E n'est pas très aisée à exploiter.
Par ailleurs, la particularité de la croissance doit être conservé. Il faut garder l'ordre.
On aimerait que si $\varphi : \mathbb{N} \to E(\subset \mathbb{N})$ est une bijection, elle conserve l'ordre :

$$k \leqslant h \Longleftrightarrow \varphi(k) \leqslant \varphi(h) (\in E)$$

On a donc la définition suivante :

Définition - Suites extraites
On dit que $(v_n)_{n\in\mathbb{N}}$ est une suite extraite de $(u_n)_{n\in\mathbb{N}}$ si il existe $\varphi : \mathbb{N} \to \mathbb{N}$, strictement croissante telle que

$$\forall\, n \in \mathbb{N}, \qquad v_n = u_{\varphi(n)}$$

. On note parfois : pour tout $k \in \mathbb{N}$, $v_k = u_{n_k}$.

Exemple - Suites extraites paires et impaires
La suite extraite des termes d'indice pair de (u_n) est la suite $(u_{2n})_{n\in\mathbb{N}}$.
La fonction φ est ici $n \mapsto 2n\ldots$
Exercice
Montrer que si $p(n)$ est vraie à partir d'un certain rang alors elle est vraie pour tous les termes d'une suite extraite de $\mathbb{N}$ à préciser

Correction
Il s'agit simplement de la suite obtenue avec $\varphi : k \mapsto n_0 + k$

Proposition - Suite extraite et ensemble infini
Considérons une famille de propriété indexée par $\mathbb{N}$, notée $(P_n)_{n\in\mathbb{N}}$.
On note $A = \{n \in \mathbb{N} \mid P_n \text{ vraie.}\}$. Alors
A est infinie si et seulement si $\exists\, \varphi : \mathbb{N} \to \mathbb{N}$, strictement croissante telle que $\forall\, n \in \mathbb{N}$, $P_{\varphi(n)}$ est vraie.

Démonstration
Si il existe une suite extraite de (P_n) toujours vraie,
i.e. si il existe $\varphi : \mathbb{N} \to \mathbb{N}$, strictement croissante telle que $\forall\, n \in \mathbb{N}$, $P_{\varphi(n)}$ est vraie.
Notons $A' = \varphi(\mathbb{N}) = \{\varphi(0), \varphi(1), \ldots \varphi(n), \ldots\} = \{\varphi(k), k \in \mathbb{N}\}$, c'est un ensemble infini car φ est injectif.
Enfin $A' \subset A$. Donc A est infinie
Réciproquement, supposons que A est infini.
Il faut construire φ.
$A \subset \mathbb{N}$, donc A possède un plus petit élément $n_0 = \varphi(0)$.
Construisons φ par récurrence, i.e. pour tout $k \in \mathbb{N}$, on donne une valeur à $\varphi(k)$ bien déterminée, selon les valeurs de $\{\varphi(0), \ldots \varphi(k-1)\}$.
Ainsi fixons $k \in \mathbb{N}^*$ et supposons que $\varphi(0) < \cdots < \varphi(k-1)$ sont bien définis.
L'ensemble $A_k = \{\varphi(0), \ldots \varphi(k-1)\}$ est fini, donc $B_k = A \setminus [\![0, \varphi(k-1)]\!]$ est infini, inclus dans $\mathbb{N}$.
Il possède un plus petit élément noté $n_k = \varphi(k)$ et $\varphi(k) > \varphi(k-1)$ et $P_{\varphi(k)}$ est vraie. □

Suites bornées

On considère $E, \preceq$ un ensemble ordonnée.

Définition - Suite majorée, minorée, bornée
On dit qu'une suite (u_n) d'éléments de E est
— majorée s'il existe $M \in E$ tel que $\forall\, n \in \mathbb{N}$, $u_n \preceq M$.
— minorée s'il existe $m \in E$ tel que $\forall\, n \in \mathbb{N}$, $m \preceq u_n$.
— bornée si elle est majorée et minorée.

Remarque - Familles bornées, majorées...
Cette définition est également adaptable au cas des familles simples.
Exercice
Montrer qu'une suite majorée à partir d'un certain rang est une suite majorée.

Correction
Si (x_n) est majorée à partir du rang n_0,
Alors il existe M tel que pour tout $n \geqslant n_0$, $x_n \leqslant M$.
Notons $M' = \max(M, x_0, x_1, \ldots x_{n_0-1})$ (ensemble fini), alors : $\forall\, n \in \mathbb{N}$, $x_n \leqslant M'$

Suites monotones

Définition - Suite croissante, décroissante
On dit qu'une suite (u_n) d'éléments de E est
— croissante
si $\forall\, n \in \mathbb{N}$, $u_n \preceq u_{n+1}$.
— décroissante
si $\forall\, n \in \mathbb{N}$, $u_{n+1} \preceq u_n$.
— monotone si elle est croissante ou décroissante.
— stationnaire si elle est constante à partir d'un certain rang.

Exemple - Deux suites monotones :

— La suite (u_n) où $u_n = \binom{2n}{n}$ est monotone.
$u_{n+1} - u_n = \binom{2n}{n}\left(\frac{(2(2n+1)}{n+1} - 1\right) = \binom{2n}{n}\frac{3n+1}{n+1} > 0$

— Soit (u_n) une suite de nombres positifs et $m_p = \inf_{n \geqslant p} u_n$. Alors (m_p) est une suite croissante.
En effet : $m_p = \min(m_{p+1}, u_p)$, donc $m_p \leqslant m_{p+1}$

Nous élargirons ces notions, lorsque nous nous concentrerons sur les suites numériques, une fois que $\mathbb{R}$ sera construit…

7. Bilan

Synthèse

⇝ Depuis la fin du XIX, on travaille en mathématiques à partir d'ensembles. On peut aussi passer d'un ensemble à un autre par des applications. Les applications injectives ne mélangent pas les éléments de l'ensemble du départ, les applications surjectives sont complètes (vu de l'arrivée).

⇝ Très souvent en mathématiques (probabilité, construction de l'intégrale), on s'intéresse plutôt aux ensembles réciproques (ie des antécédents) $f^{-1}(B)$ qu'aux ensembles images directes $f(A)$.

⇝ La fonction indicatrice d'un ensemble A dans E est une projection naturelle de E sur A. Elle est d'une utilité essentielle en mathématique, par exemple pour calculer le cardinal (ou en probabilité).

⇝ On termine par décrire les propriétés pour des familles indexées sur un ensemble I fini ou dénombrable.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Montrer une égalité entre deux fonctions.
— Savoir-faire - Autre formulations équivalentes (injectivité, surjectivité)
— Savoir-faire - Critère pour montrer la bijectivité
— Savoir-faire - Critère de surjectivité.
— Savoir-faire - Montrer que $y \in f(A)$
— Savoir-faire - Montrer que $x \in f^{-1}(B)$

Notations

	Propriétés	*Remarques*
définition (du terme de gauche)		autre notation : $\overset{\text{def.}}{s} =$
pplication de E sur F, injective		Cette notation donne deux informations
pplication de E sur F, surjective		Cette notation donne deux informations
de f à l'ensemble de départ A nent d'arrivée B)	$f_{\|A} : A \to F$, $x \mapsto f(x)$ et $f^{\|B} : E \to B$, $x \mapsto f(x)$	Pour la restriction d'arrivée, il faut vérifier que cela a du sens…
te de A par f	$\{f(x), x \in A\}$. $y \in f(A) \Leftrightarrow \exists\, x \in A \mid y = f(x)$	autre notation : $[\mathrm{Im}(f_{\|A}$
lmage) réciproque de B par f	$\{x \in E \mid f(x) \in B\}$. $x \in f^{-1}(B) \Leftrightarrow f(x) \in B$	autre notation (probabilité) : $[f \in B]$
nion disjointe des ensembles A_i	$x \in C$ ssi $\exists\, !i \in \mathbb{N}_n$ tel que $x \in A_i$	Deux informations : C est la réunion des A_i & les A_i sont disjoints deux à deux.
$\Rightarrow x \in A$	Codage numérique d'une propriété caractéristique	$\mathbb{1}_{A\cap B} = \mathbb{1}_A \times \mathbb{1}_B$, $\mathrm{Card} A = \sum_{x\in E} \mathbb{1}_A(x)$

Retour sur les problèmes

50. Voir cours

51. Une bijection montre que deux ensembles sont équivalents (si ce n'est égaux).

52. Là on sort du cours.
$\mathbb{Z}$ et $\mathbb{N}$ ont la même puissance ($\approx$ cardinal) car on peut les mettre en bijection l'un par l'autre.
Avec par exemple $\varphi : \mathbb{Z} \to \mathbb{N}$, $m \mapsto 2|m| + \mathbb{1}_{\mathbb{Z}_-}(m)$.
De même (c'est plus subtile) $\mathbb{Z} \times \mathbb{N}$ est en bijection avec $\mathbb{N}$ (vous pouvez trouver une bijection ?), donc $\mathbb{Q}$ est également en bijection avec $\mathbb{N}$.
On dit que $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ ont la puissance du dénombrable (le même cardinal infini).
En revanche, il n'existe aucune bijection entre $\mathbb{R}$ et $\mathbb{N}$. $\mathbb{R}$ a un cardinal plus grand, on parle du cardinal du continue.

53. Cours.

Chapitre 12

Relations binaires sur un ensemble

Résumé -

Nous complétons quelques notions essentielles du fondement des mathématiques (formalisé non sans mal à la fin du XIX-ième siècle). Ces fondements se basent sur les ensembles!
Mais il faut agir sur ces ensemble. Nous commençons donc d'abord par voir deux notions dont l'emploi en mathématiques est fréquent (en particulier lorsqu'il s'agit de construire de nouvelles notions). Il s'agit des relations binaires : relation d'ordre et relation d équivalence.
Dans ce chapitre, il y a beaucoup de définitions. A apprendre!! Quelques vidéos :
- *Science4all - Les mathématiques modernes - https ://www.youtube.com/watch ?v=7fbn99V1f9U*
- *Maths Adultes - Relations binaires - https ://www.youtube.com/watch ?v=W7cH06qOImM*

Sommaire

1. Problèmes 240
2. Graphe 241
2.1. Formalisation 241
2.2. Vocabulaire 241
2.3. Applications 241
3. Relations binaires 242
3.1. Construction et représentation 242
3.2. Caractérisations 242
4. Relation d'ordre 242
4.1. Définitions 242
4.2. Ensemble avec ordre total 243
4.3. Ensemble avec ordre partiel 244
4.4. Eléments particuliers 244
4.5. Ordre strict 247
5. Relation d'équivalence 247
5.1. Propriétés caractéristiques 247
5.2. Classes d'équivalence 248
5.3. Partition de E 249
6. Bilan 250

1. Problèmes

Problème 54 - Graphe

En option « maths expertes », les élèves étudient les graphes : sommets, arrêtes. . ..
C'est une famille essentielle d'objets en mathématiques et en informatique (nous les y retrouverons en fin d'année). Comment formaliser proprement les graphes? Comment passer de l'idée bien comprise (de sommets et d'arêtes/flèches) à une représentation mathématique/informatique acceptable?

Problème 55 - Forcer l'égalité. Qu'est-ce qu'une égalité ?

Pour résoudre un exercice, on exploite souvent des équivalences ($\Leftrightarrow$). La bijection de f permet d'écrire : $f(x) = y \Longleftrightarrow x = f^{-1}(y)$ en prenant x et y dans les bons ensembles.
Si f n'est pas surjective, il suffit de changer l'ensemble de définition de y et la résolution du problème se conserve.
Mais si f n'est pas injective, qu'il y a plusieurs solutions $x_1, x_2, \dots x_n$ à l'équation $f(x) = y$. Que faire?
Une idée : forcer l'égalité et affirmer que $x_1 = x_2 = \dots x_n$, comme pour l'équation $\tan x = \sqrt{3}$ qui permet d'affirmer $x = \frac{\pi}{3}$ ou $x = \frac{4\pi}{3}$. . ..
C'est choquant! Comment rendre cela propre : en redonnant un sens nouveau à l'égalité $x_1 = x_2 = \dots x_n$. Qu'est-ce qu'une égalité?

Problème 56 - Relation d'ordre ?

Pour résoudre le problème précédent, nous créons la notion de relation d'équivalence.
Mais plus souvent, lorsque nous prenons deux objets nous ne pouvons pas affirmer qu'ils sont pareils. Souvent l'un est PLUS quelque chose que l'autre.
Comment formaliser cette idée? Qu'est-ce qu'une relation d'ordre? Et comment l'exploiter?

Problème 57 - Plus grand élément

Existe-t-il nécessairement un, un seul, plus grand élément à un ensemble ordonné?
Par exemple : quel est le plus grand élément de $[0, 1[$?

Problème 58 - Codage de graphe (ou relation) à partir d'applications. Et réciproquement. . .

Après avoir défini les ensembles, on peut ou bien définir les applications et à partir de là les relations (ou graphes), ou bien définir les relations et à partir de là les applications.
Comment faire naturellement ces deux implications? (Evidemment, pas en même temps. . .)

2. Graphe

2.1. Formalisation

Heuristique - Images mentales des graphes!
Pour l'heuristique et les images mentales (à ne pas oublier et vraiment à garder en mémoire!!), il faut revoir le cours de mathématiques de terminale.

Définition - Graphe non orienté
On considère un ensemble S (de sommets), fini en règle générale. Puis un ensemble $A \subset \binom{S}{2}$ de paires d'arêtes.
On appelle graphe non orienté le couple (S, A).

Définition - Graphe orienté
On considère un ensemble S (de sommets), fini en règle générale. Puis un ensemble $A \subset S \times S$ de couples d'arêtes.
On appelle graphe orienté le couple (S, A).

Exercice
Donner la définition formalisée d'un graphe complet.

Correction
Un graphe complet est, heuristiquement, dont chaque sommet est relié à tous les autres.
Formellement : $A = S \times S$ (cas orienté) ou $A = \binom{S}{2}$ (cas non orienté).

2.2. Vocabulaire

Définition - Sommets reliés
On dit que deux sommets $s_1, s_2 \in S$ sont reliés si $(s_1, s_2) \in A$ (cas orienté) ou $\{s_1, s_2\} \in A$ (cas non orienté)

Définition - Degré d'un sommet
Soit $s \in S$ un sommet d'un graphe non orienté (S, A) a pour degré $d(s) = \text{card}(A_s)$ où $A_s = \{a \in A \mid s \in a\}$.
Soit $s \in S$ un sommet d'un graphe orienté (S, A) a pour degré sortant $d_+(s) = \text{card}(A_s)$ où $A_s = A \cap (\{s\} \times S)$ et pour degré entrant $d_-(s) = \text{card}(A'_s)$ où $A'_s = A \cap (S \times \{s\})$.

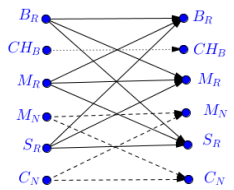
Exercice
Comment définir chemin d'un sommet à un autre ?
Et graphe connexe ?

Correction
On dit que le graphe (S, A) admet un chemin de s à s' $(\in S)$ s'il existe un entier n et une suite $(s_0, s_1, s_2, \dots s_n)$ d'éléments de S tels que $s_0 = s$, $s_n = s'$ et $\forall\, i \in \mathbb{N}_n$, $(s_{i-1}, s_i) \in A$ (cas orienté) ou $\{s_{i-1}, s_i\} \in A$ (cas non orienté).
Un graphe est connexe si pour tout sommets s, $s' \in S$, il existe un chemin de s à s'.

2.3. Applications

On retrouvera très vite les graphes dans le cours sur les relations binaires, plus loin en probabilité et algèbre linéaire (chaine de Markov), ou en informatique… A l'occasion, nous verrons en informatique, un façon supplémentaire et pratique de coder/définir un graphe à l'aide de matrice…

Représentation - Graphe



C'est le graphe de l'exercice du Stade Toulousain.

3. Relations binaires

3.1. Construction et représentation

Définition - Relation
Soit E un ensemble.
Une relation binaire sur E est un sous-ensemble G de $E \times E$. Si $(x, y) \in E^2$ on écrit $x \mathscr{R} y$ lorsque $(x, y) \in G$.

On peut représenter une relation par un graphe (diagramme sagittal) : une représentation de $E \times E$ et avec des flèches on indique que x (du premier E) est en relation à y (du second E).

Exemple - Stade Toulousain
Par exemple dans l'ensemble E=Boutique du Stade Toulousain où :

$$E = \{\text{beret rouge, chaussette blanche, maillot rouge, maillot noir, short rouge, cuissart noir}\} = \{B_R, CH_B, M_R, M_N, S_R, C_N\},$$

on définit la relation $\mathscr{R}_1$ par "est de la même couleur que" c'est-à-dire que l'on a

$$G_1 = \{(B_R, M_R), (M_R, B_R), (M_R, S_R), (S_R, M_R), (B_R, S_R), (S_R, B_R), (B_R, B_R), (M_R, M_R), (S_R, S_R), (CH_B, CH_B), (M_N, C_N), (C_N, M_N), (M_N, M_N), (C_N, C_N)\}$$

ou encore $B_R \mathscr{R}_1 M_R$, $M_R \mathscr{R}_1 B_R$, $M_R \mathscr{R}_1 S_R$…

Exercice
On peut définir dans l'ensemble $\{0, 1, 2, 3, 4, 5, 6\}$ les relations $\mathscr{R}_1$ "est un multiple de" ou $\mathscr{R}_2$ "est le double de".
Expliciter G_1, G_2 et les diagrammes sagittaux de ces deux relations.

Correction
$G_1 = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (0,6), (1,1), (2,1), (2,2), (3,1), (3,3), (4,1), (4,2), (4,4), (5,1), (5,5), (6,1), (6,2), (6,3), (6,6)\}$ et $G_2 = \{(0,0), (2,1), (4,2), (6,3)\}$

3.2. Caractérisations

Définition - Propriétés des relations
Soit $\mathscr{R}$ une relation sur un ensemble E. On dit que $\mathscr{R}$ est :
- réflexive si $\forall x \in E$, $x \mathscr{R} x$;
- symétrique si $\forall (x, y) \in E^2$, $x \mathscr{R} y \Rightarrow y \mathscr{R} x$;
- antisymétrique si $\forall (x, y) \in E^2$, $x \mathscr{R} y$ et $y \mathscr{R} x \Rightarrow x = y$;
- transitive si $\forall (x, y, z) \in E^3$, $x \mathscr{R} y$ et $y \mathscr{R} z \Rightarrow x \mathscr{R} z$.

Exemple - Stade Toulousain
Dans l'exemple précédent, la relation est réflexive, symétrique et transitive.
Exercice
Comment se représentent pour un graphe les propriétés précédentes ?

Correction
En terme de graphe, cela signifie que :
- pour la réflexivité : chacun est relié à lui-même, donc le diagramme présente des lignes droites.
  (Dans le cas d'une représentation matricielle : que des 1 sur la diagonale)
- pour la symétrie : un flèche dans un sens, donne une flèche dans l'autre sens (on pourrait faire des doubles flèches).
  On parle alors de graphe non orienté.
  (Dans le cas d'une représentation matricielle : la matrice est symétrique)
- pour l'antisymétrie : il ne peut y avoir de double flèche, excepté sur eux-mêmes.
  (Dans le cas d'une représentation matricielle : la matrice est presque antisymétrique)
- pour la transitivité : il y a des blocs de points regroupés entre eux.

4. Relation d'ordre

4.1. Définitions

Définition - Relation d'ordre
Soit $\mathscr{R}$ une relation sur un ensemble E. On dit que c'est une relation d'ordre si elle est réflexive, antisymétrique et transitive.

Définition - Plus petit
Une relation d'ordre permet de *comparer* deux éléments. Lorsque $x\mathscr{R}y$ on dit que x est "plus petit" que y et on note usuellement $x \preceq y$.

Savoir faire - Montrer que $\mathscr{R}$ est une relation d'ordre.
Il s'agit de montrer, tour à tour, que la relation est réflexive, antisymétrique et transitive.

4.2. Ensemble avec ordre total

Définition - Ordre total
Soit $\preceq$ une relation d'ordre sur un ensemble E. On dit que c'est une relation d'ordre total si
$$\forall (x,y) \in E^2,\ x \preceq y \text{ ou } y \preceq x$$
(c'est-à-dire si deux éléments quelconques de E sont comparables).

Pour aller plus loin - Treillis (de Galois)
Pour les relations d'ordre, au lieu du grpahe, on préfère une représentation graphique sous forme de treillis (de Galois).
Si $x \preceq y$, alors on représente x « sous » y, et l'on trace un lien entre les deux.
Si l'ordre est total, il n'y a qu'un élément à chaque hauteur.
Cette représentation n'a d'intérêt que pour E de cardinal fini (et petit), même si elle peut aussi donner de bonnes idées complémentaires.

Remarque - Concernant le treillis (ou graphe)
Le fait que l'ordre soit total signifie que le treillis/graphe est connexe (en un seul morceau).

Exemple - Sur $\mathbb{R}$
Par exemple, dans $\mathbb{R}$ la relation $\leqslant$ est une relation d'ordre total, en revanche $<$ n'est pas une relation d'ordre.
En effet, $<$ n'est pas reflexive.

Exercice
Sur $E = \mathbb{R}^2$ on définit les deux relations suivantes :
- l'ordre produit :
$$(x,y) \preceq_1 (x',y') \Leftrightarrow x \leqslant x' \text{ et } y \leqslant y'$$
- l'ordre lexicographique :
$$(x,y) \preceq_2 (x',y') \Leftrightarrow (x < x') \text{ ou } (x = x' \text{ et } y \leqslant y')$$

Vérifier qu'il s'agit de relations d'ordre. S'agit-il d'ordre partiel ou d'ordre total ?

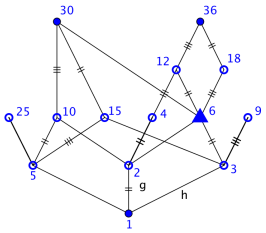
Correction
Première relation :
- Réflexive : Pour tout $x, y \in \mathbb{R}$, on a $x \leqslant x$ et $y \leqslant y$, donc $(x,y) \preceq_1 (x,y)$
- Antisymétrique :Soient $x, y, x'y' \in \mathbb{R}$ tels que $(x,y) \preceq_1 (x',y')$ et $(x',y') \preceq_1 (x,y)$
  Donc $x \leqslant x'$, $x' \leqslant x$, $y \leqslant y'$ et $y' \leqslant y$.
  Donc $x = x'$ et $y = y'$ (car $\leqslant$ est antisymétrique sur $\mathbb{R}$).
  Finalement $(x,y) = (x',y')$
- Transitive : Soient $x, y, x', y', x'', y'' \in \mathbb{R}$, tels que $(x,y) \preceq_1 (x',y')$ et $(x',y') \preceq_1 (x'',y'')$.
  On a donc $x \leqslant x' \leqslant x''$ et $y \leqslant y' \leqslant y''$, donc $(x,y) \preceq_1 (x'',y'')$

Cette relation n'est pas totale : il n'y a aucune relation entre $(1,0)$ et $(0,1)$ (et pas de relation d'ordre totale sur $\mathbb{C}$). Première relation :
- Réflexive : Pour tout $x, y \in \mathbb{R}$, on a $x = x$ et $y \leqslant y$, donc $(x,y) \preceq_2 (x,y)$
- Antisymétrique :Soient $x, y, x'y' \in \mathbb{R}$ tels que $(x,y) \preceq_2 (x',y')$ et $(x',y') \preceq_2 (x,y)$
  On ne peut avoir $x < x'$, sinon, on aurait pas $(x',y') \preceq_2 (x,y)$, donc $x = x'$.
  Puis $y \leqslant y'$ et $y' \leqslant y$ donc $y = y'$.
  Finalement $(x,y) = (x',y')$
- Transitive : Soient $x, y, x', y', x'', y'' \in \mathbb{R}$, tels que $(x,y) \preceq_2 (x',y')$ et $(x',y') \preceq_2 (x'',y'')$.
  Alors $x \leqslant x' \leqslant x''$.
  - Ou bien $x < x''$ et donc $(x,y) \preceq_2 (x'',y'')$
  - Ou bien $x = x''$ et donc $x = x' = x''$
    et donc $y \leqslant y' \leqslant y''$ et ainsi $(x,y) \preceq_2 (x'',y'')$

  Dans tous les cas $(x,y) \preceq_2 (x'',y'')$

Cette relation est totale : elle permet d'écrire le dictionnaire !
C'est aussi l'ordre total qui permet de classer les nombres écrits décimalement (ou une base quelconque, d'ailleurs).

Représentation - Treillis de diviseurs de 30 et 36



4.3. Ensemble avec ordre partiel

Définition - Ordre partiel
Soit $\preceq$ une relation d'ordre sur un ensemble E. On dit que c'est une relation d'ordre partiel s'elle n'est pas total.
C'est-à-dire : il existe $(x,y) \in E^2$ tel que $x \not\preceq y$ et $y \not\preceq x$.

Exercice
Soit Ω un ensemble et $E = \mathscr{P}(\Omega)$. On définit sur E la relation $\mathscr{R}$ par
$$\forall (A,B) \in E^2,\ A\mathscr{R}B \Leftrightarrow A \subset B.$$
Vérifier que la relation $\mathscr{R}$ est une relation d'ordre. S'agit-il d'une relation d'ordre total ?

Correction
- Elle est réflexive : pour tout ensemble A, on a $A \subset A$.
- Elle est antisymétrique : soient A et B tels que $A \subset B$ et $B \subset A$, alors $A = B$.
- Elle est transitive : soient A, B et C tels que $A \subset B$ et $B \subset C$, alors $A \subset C$.

Mais ce n'est pas une relation d'ordre totale : si $\mathrm{Card}(E) \geqslant 2$, il n'y a pas de relation entre $\{a\}$ et $\{b\}$ si $a \neq b$.

Exemple - Divisibilité sur $\mathbb{N}$
La relation « divise » : $n|m$, si il existe $k \in \mathbb{N}$ tel que $m = nk$ est une relation d'ordre partielle.

Exercice
Montrer ce résultat

Correction
C'est une relation reflexive, antisymétrique et transitive

Remarque - Treillis
On peut faire un treillis de divisibilité de certains nombres entiers.
Ce n'est pas une droite, comme avec $(\mathbb{R}, \leqslant)$ par exemple.

4.4. Eléments particuliers

Majorant/minorant

Définition - Majorants,minorants
Soit $\preceq$ une relation d'ordre sur un ensemble E. Pour $A \subset E$, on définit les éléments suivants :
- $M \in E$ est un majorant de A si $\forall x \in A, x \preceq M$;
- $m \in E$ est un minorant de A si $\forall x \in A, m \preceq x$;

Exemple - Majorant sur $(\leqslant, \mathbb{R})$
Pour la relation d'ordre $\leqslant$ sur $\mathbb{R}$,
3 est un majorant de l'ensemble $\{\frac{1}{n}, n \in \mathbb{N}\}$.
D'une certaine façon, ce n'est pas le meilleur.

Exemple - Majorant sur $(|, \mathbb{N})$
Pour la relation d'ordre $|$ sur $\mathbb{N}$,
- 120 est un majorant de $\{1,2,3,4,5\}$
  Ce n'est pas le meilleur. On dit que c'est un multiple.
  La majorant le plus intéressant serait le plus petit multiple. (PPCM)
- 3 est un minorant de $\{6,9,12\}$.
  On dit que c'est un diviseur.
  C'est d'une certaine façon le meilleur car c'est le plus grand des diviseurs (PGCD).

Exercice
Pour la relation d'ordre $\subset$ sur $\mathbb{R}$.
Donner un majorant et un minorant de $\{\{1,2,3\},\{2,3,5\}\}$

Correction
On peut prendre par exemple : $A = \{1,2,3,5\}$ et $B = \{2,3\}$ respectivement.
En fait tout majorant doit contenir A et tout minorant est inclus dans B

Plus grand/petit élément

Définition - Plus grand élément, plus petit élément
Soit $\preceq$ une relation d'ordre sur un ensemble E. Pour $A \subset E$, on définit les éléments suivants :
- $a \in E$ est un plus grand élément de A si $a \in A$ et $\forall x \in A, x \preceq a$;
- $a \in E$ est un plus petit élément de A si $a \in A$ et $\forall x \in A, a \preceq x$.

En fait a est respectivement un majorant de A et élément de A ou bien un minorant et élément de A

Théorème - Unicité
Un plus petit grand élément de $A \subset E$, lorsqu'il existe, est unique, noté $\max(A)$.
Un plus petit petit élément de $A \subset E$, lorsqu'il existe, est unique, noté $\min(A)$.

Démonstration
Supposons que A admettent (au moins) deux plus petits éléments : a_1 et a_2.
Alors pour tout $x \in A$, $a_1 \preceq x$, donc en particulier pour $x = a_2 \in A$: $a_1 \preceq a_2$.
Et pour tout $x \in A$, $a_2 \preceq x$, donc en particulier pour $x = a_1 \in A$: $a_2 \preceq a_1$.
Par antisymétrie : $a_1 = a_2$. A admet au plus un seul plus petit élément. □

Attention - Attention au mot
Ici il ya une source d'erreur classique. On fera bien attention aux mots définis ici : (un) majorant, (un) minorant, (le) plus grand élément, (le) plus grand élément.
S'ajoutent à ces mots : élément maximal, minimal…
Il y aura bientôt également l'expression borne supérieure, borne inférieure…

On rencontre très souvent le cas suivant :
Exercice
On suppose que $\preceq$ est une relation d'ordre total sur E.
Soit $A \subset E$. On suppose que A est fini.
Montrer que A admet nécessairement un plus grand élément

Correction
On fait une récurrence sur $\mathrm{Card}(A)$.
$\mathscr{P}_n$: Si $\mathrm{Card}(A) = n$, alors A admet un plus grand élément. Pour l'hérédité, on note que si $A = A_n \uplus \{a\}$, alors $\max(A) = \max(\max(A_n), a)$…
Exercice
On admet qu'un ensemble fini admet toujours un plus petit élément (il suffit de faire au plus $\frac{n(n-1)}{2}$ comparaisons - mais on peut se contenter de $n-1$ comparaisons…).
Montrer que tout sous-ensemble de $\mathbb{N}$ admet un plus petit élément.

Correction
Soit $A \subset \mathbb{N}$. Soit $a \in A$.
Alors $A' = A \cap [\![0, a]\!]$ est fini (car inclus dans $[\![0, a]\!]$), il admet un plus petit élément a'.
Pour tout $x \in A$,
ou bien $x > a$ et donc $a' \leqslant a < x$, ou bien $x \leqslant a$ donc $x \in A'$ et donc $a' \leqslant x$.
Ainsi a' est le plus petit élément de A

Eléments maximaux/minimaux

Remarque - Généralisation : élément maximal ou minimal
On peut également définir la notion d'élément maximal ou minimal :
- $M \in A$ est un *élément maximal* de A si $\forall x \in A, M \preceq x \Rightarrow x = M$;
- $m \in A$ est un *élément minimal* de A si $\forall x \in A, x \preceq m \Rightarrow x = m$.

S'il s'agit d'une relation d'ordre total, ces éléments coïncident avec les plus grand et plus petit éléments (s'ils existent).

Exemple - Ensemble avec plusieurs éléments maximaux
Pour qu'il y en ait plusieurs, il ne faut pas qu'ils coïncident avec l'unique plus grand élément.
Donc d'après la remarque, l'ordre ne doit pas être total.
On peut prendre l'ordre produit sur $E = \mathbb{R}^2$ et $A = \{(x, y) \in E \mid x^2 + y^2 \leqslant 1\}$, le disque unité.
Alors A n'admet pas de plus grand élément et tous les éléments de $M = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1, x \geqslant 0, y \geqslant 0\}$ sont des éléments maximal de A.
En effet, si $(x_0, y_0) \in M$ et $(x, y) \in A$, avec $(x_0, y_0) \preceq_1 (x, y)$, alors $x_0 \leqslant x$ et $y_0 \leqslant y$.
Alors $1 = x_0 + y_0 \leqslant x^2 + y^2 \leqslant 1$, on a donc $x^2 + y^2 = 1 = x_0^2 + y_0^2$,
Ainsi $(x^2 - x_0^2) + (y^2 - y_0^2) = 0$, avec un somme de termes positifs, donc $x^2 - x_0^2 = 0$ et $y^2 - y_0^2 = 0$.
Enfin pat positivité de x_0 et y_0 : $x = x_0$ et $y = y_0$, donc $(x, y) = (x_0, y_0)$.

Borne supérieure/inférieure

Une dernière définition, pour des cas plus simples que celui de l'exemple précédent :

Définition - Borne inférieure, borne supérieure
Soit $A \subset \mathbb{R}$.
- Si l'ensemble des majorants de A est non vide et admet un plus petit élément a, a est appelé borne supérieure de A, on note $a = \sup A$.
- Si l'ensemble des minorants de A est non vide et admet un plus grand élément b, b est appelé borne inférieure de A, on note $b = \inf A$.

Cette définition sera au coeur de la définition de l'ensemble $\mathbb{R}$ (à partir de $\mathbb{Q}$ avec la relation d'ordre totale $\leqslant$). Mais elle sert aussi à d'autres moments du cours

Exemple - Borne inférieure et supérieure pour $(|, \mathbb{N})$
Comme leur nom l'indique :
- La borne supérieure de l'ensemble fini d'entiers $\{u, v\}$ est le $PPCM(u, v)$.
- La borne inférieure de l'ensemble fini d'entiers $\{u, v\}$ est le $PGCD(u, v)$.

Savoir faire - Montrer que $a = \sup E$
On montre en deux temps :
1. $\forall x \in E, x \preceq a$
2. $\forall z$ tel que $\forall x \in E, x \preceq z$, alors $a \preceq z$
(tout majorant z de E est plus grand que a)
OU (de manière équivalente)
$\forall u \preceq a, \exists x \in E$ tel que $u \preceq x$
(tout élément plus petit que a ne peut pas être un majorant de E)

Exercice
Comment repérer sur le treillis des multiples et diviseurs de u et de v, leur PGCD et leur PPCM ?

Correction
C'est le grand père commun (PPCM) ou le petit fils commun (PGCD)
Exercice
Comment peut-on définir l'ensemble borne supérieure de deux ensembles A et B pour la relation $\leqslant$?
Même question avec la borne inférieure ?

Correction
Tout simplement : $A \cup B$ et $A \cap B$ respectivement

Pour aller plus loin - Espaces vectoriels
On indiquera que dans le cadre des espaces vectoriels, où l'on exige en outre une stabilité pour l'addition vectoriel, la borne supérieure des sous-espaces vectoriels F_1 et F_2 est donnée par l'~~ensemble~~ $F_1 + F_2$

4.5. Ordre strict

Définition - Ordre strict
Soit $(E, \preceq)$ un ensemble ordonné. On définit la relation $\prec$ par :

$$x \prec y \Leftrightarrow (x \preceq y \text{ et } x \neq y)$$

ce n'est pas une relation d'ordre sur E car elle n'est pas réflexive.

Exemple - Sur $\mathbb{R}$
La relation $\leqslant$ est une relation d'ordre (totale).
Alors que $<$ est une relation d'ordre strict.

5. Relation d'équivalence

5.1. Propriétés caractéristiques

Définition - Relation d'équivalence
Soit $\mathcal{R}$ une relation sur un ensemble E. On dit que c'est une relation d'équivalence si elle est réflexive, symétrique et transitive.

Pour aller plus loin - Relation d'équivalence : volonté de définir =
Sur le site images des maths, un article intéressant : http ://images.math.cnrs.fr/Egalite

Exemple - Stade Toulousain
On a vu une première relation d'équivalence, avec l'exemple du stade Toulousain.

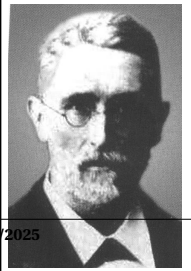
Exemple - Fractions rationnelles
Montrer que $\mathcal{R}$ définie sur $\mathbb{Z} \times \mathbb{N}$ par $(a,b)\mathcal{R}(c,d)$ ssi $a \times d = b \times c$ est une relation d'équivalence.
Montrons que $\mathcal{R}$ ainsi définie est :
- réflexive.
  $a \times b = b \times a (= ab)$ donc $(a,b)\mathcal{R}(a,b)$.
- symétrique.
  Supposons que $(a,b)\mathcal{R}(c,d)$, donc $a \times d = b \times c$
  donc $c \times b = d \times a$ donc $(c,d)\mathcal{R}(a,b)$.
- transitive.
  Supposons que $(a,b)\mathcal{R}(c,d)$ et $(c,d)\mathcal{R}(e,f)$ donc $a \times d = b \times c$ et $c \times f = d \times e$.
  donc $(a \times f) \times d = f \times (a \times d) = f \times (c \times b) = (f \times c) \times b = d \times e \times b$.
  et comme d est non nul, il est inversible (dans $\mathbb{R}$) et donc $a \times f = e \times b$ donc $(a,b)\mathcal{R}(e,f)$.

Savoir faire - Montrer que $\mathcal{R}$ est une relation d'équivalence
Il s'agit de montrer, tour à tour, que la relation est réflexive, symétrique et transitive.

Exercice
Montrer que $\mathcal{R}$ définie sur $(\mathbb{R}^{\mathbb{N}})^2$ (ensemble des suites) par $(u_n)\mathcal{R}(v_n)$ ssi $\lim\limits_{n\to+\infty} \dfrac{u_n}{v_n} = 1$ est une relation d'équivalence.

Correction
Montrons que $\mathcal{R}$ ainsi définie est :
- réflexive.
  $\lim\limits_{n\to+\infty} \dfrac{u_n}{u_n} = 1$ donc $(u_n)\mathcal{R}(u_n)$.
- symétrique.
  Supposons que $(u_n)\mathcal{R}(v_n)$, donc $\lim\limits_{n\to+\infty} \dfrac{u_n}{v_n} = 1$
  donc $\lim\limits_{n\to+\infty} \dfrac{v_n}{u_n} = \dfrac{1}{1} = 1$ donc $(v_n)\mathcal{R}(u_n)$.
- transitive.
  Supposons que $(u_n)\mathcal{R}(v_n)$ et $(v_n)\mathcal{R}(w_n)$ donc $\lim\limits_{n\to+\infty} \dfrac{u_n}{v_n} = 1$ et $\lim\limits_{n\to+\infty} \dfrac{v_n}{w_n} = 1$.
  donc $\lim\limits_{n\to+\infty} \dfrac{u_n}{w_n} = \lim\limits_{n\to+\infty} \dfrac{u_n}{v_n} \times \lim\limits_{n\to+\infty} \dfrac{v_n}{w_n} = 1$ et donc $a \times f = e \times b$ donc $(u_n)\mathcal{R}(w_n)$.

Histoire - Construction de $\mathbb{Z}$
Etant donné $\mathbb{N}$, construit par un principe de type récurrence (par Péano) ; on peut suivre Dedekind est construire $\mathbb{Z}$.
On note sur $\mathbb{N}^2$, $\mathcal{R}$ telle que $(n,m)\mathcal{R}(n',m')$ ssi $n + m' = n' + m$
Les classes d'équivalence sont de la forme $(0,n) = \{(k, k+n), k \in \mathbb{N}\}$, représenté de l'entier relatif : $-n$.



Richard Dedekind (1831-1916) est un brillant mathématicien allemand, hanté par une question : « qu'est-ce que sont les nombres ? ».

Exercice
Soit $f : E \to F$.
On définit la relation $\mathcal{R}_f$ sur E par $x\mathcal{R}_f y$ ssi $f(x) = f(y)$.
Montrer que $\mathcal{R}_f$ est une relation d'équivalence sur E.

Correction
Trivial

5.2. Classes d'équivalence

Définition - Classe d'équivalence
Soit $\mathcal{R}$ une relation d'équivalence sur E.
Pour $a \in E$, on appelle classe d'équivalence de a l'ensemble $C(a) = \{x \in E \,|\, x\mathcal{R}a\}$. a est un représentant de $C(a)$.

Exemple - Fractions rationnelles
Les classes d'équivalence des fractions rationnelles sont exactement les couples dont les fractions sont égales.
On voit sur cette exemple le but de la notion de classe d'équivalence : préciser et généraliser la notion d'égalité !
Les fractions rationnelles simplifiés sont des représentants particulièrement simple de leur classe d'équivalence.

Exercice
Montrer que $\mathcal{R}$ définie sur $\mathbb{C}^{*2}$, par $z = a + \mathrm{i}b\mathcal{R}z' = a' + \mathrm{i}b'$ ssi $a \times b' = a' \times b$ est une relation d'équivalence.
Quelles sont les classes d'équivalence de $\mathcal{R}$?

Correction
Montrons que $\mathcal{R}$ ainsi définie est :
- réflexive.
  $a \times b = b \times a (= ab)$ donc $a + \mathrm{i}b\mathcal{R}a + \mathrm{i}b$).
- symétrique.
  Supposons que $a + \mathrm{i}b\mathcal{R}c + \mathrm{i}d$, donc $a \times d = b \times c$
  donc $c \times b = d \times a$ donc $c + \mathrm{i}d\mathcal{R}a + \mathrm{i}b$.
- transitive.
  Supposons que $a + \mathrm{i}b\mathcal{R}c + \mathrm{i}d$ et $c + \mathrm{i}d\mathcal{R}e + \mathrm{i}f$ donc $a \times d = b \times c$ et $c \times f = d \times e$.
  donc $(a \times f) \times d = f \times (a \times d) = f \times (c \times b) = (f \times c) \times b = d \times e \times b$.
  et comme d est non nul, il est inversible (dans $\mathbb{R}$) et donc $a \times f = e \times b$ donc $a + \mathrm{i}b\mathcal{R}e + \mathrm{i}f$.

Les classes d'équivalence peuvent représentées par les droites passant par 0.

Exercice
Montrer que $\mathcal{R}$ définie sur $\mathbb{R}$, par $\theta\mathcal{R}\theta'$ ssi $\exists\, k \in \mathbb{Z}$ tel que $\theta - \theta' = 2k\pi$ est une relation d'équivalence.
Quelles sont les classes d'équivalence de $\mathcal{R}$?

Correction
Montrons que $\mathcal{R}$ ainsi définie est :
- réflexive.
  $\theta - \theta = 0 = 0 \times 2\pi$ donc $\theta\mathcal{R}\theta$.
- symétrique.
  Supposons que $\theta\mathcal{R}\theta'$, donc $\theta - \theta' = 2k\pi$
  donc $\theta' - \theta = -2k\pi$ donc $\theta'\mathcal{R}\theta$.
- transitive.
  Supposons que $\theta\mathcal{R}\theta'$ et $\theta'\mathcal{R}\theta''$ donc $\theta - \theta' = 2k\pi$ et $\theta' - \theta'' = 2k'\pi$.
  donc $\theta - \theta'' = (\theta - \theta') + (\theta' - \theta'') = 2k\pi + 2k\pi = 2(k + k')\pi$.
  et donc $\theta\mathcal{R}\theta''$.

Les classes d'équivalence peuvent représentées par les arguments principaux. En fait, on retrouve la même classe d'équivalence que précédemment.

Proposition - Caractéristique par les classes d'équivalence
Soient $\mathcal{R}$ une relation d'équivalence sur un ensemble E, a et b deux éléments de E. Alors

$$a\mathcal{R}b \Leftrightarrow C(a) = C(b)\,.$$

Démonstration
Supposons que $a\mathcal{R}b$.
Soit $x \in C(b)$, alors $x\mathcal{R}b$ et par transitivité (et réflexivité) : $x\mathcal{R}a$, donc $x \in C(a)$.

$\forall\, x \in C(b)$, $x \in C(a)$, donc $C(b) \subset C(a)$.
Et, si $y \in C(a)$ alors $y \mathscr{R} a$, donc $y \mathscr{R} b$, donc $y \in C(b)$. Et $C(a) \subset C(b)$.
Bilan : $C(a) = C(b)$.
Réciproquement, si $C(a) = C(b)$, alors $a \in C(a) \subset C(b)$, donc $a \in C(b)$ et $a \mathscr{R} b$. □

Exercice
On note $\mathscr{P}$ le plan usuel. On définit sur $\mathscr{P} \times \mathscr{P}$ la relation $\mathscr{R}$ par

$$(A,B)\mathscr{R}(C,D) \Leftrightarrow ABDC \text{ est un parallélogramme.}$$

Il s'agit d'une relation d'équivalence. Que représentent les classes d'équivalence de cette relation ?

Correction
Les classes d'équivalence sont données par l'ensemble de tous les vecteurs (pas d'origine).

Définition - Système de représentants
Soit $\mathscr{R}$ une relation d'équivalence définie sur un ensemble E.
Si il existe $S \subset E$ tel que pour tout $x \in E$, $\exists\, ! s \in S$ tel que $x \mathscr{R} s$,
on dit que S est un système de représentants de la classe d'équivalence $\frac{E}{\mathscr{R}}$.
(Il y a une bijection naturelle entre S et $\frac{E}{\mathscr{R}}$).
On note souvent $S_{E\setminus\mathscr{R}}$ un tel système.
Si E est fini, il existe toujours un système de représentants (sinon cela peut nécessiter l'axiome du choix).

Remarque - Notation floue
La notation $S_{E\setminus\mathscr{R}}$ est très imprécise (pas de différence entre un système et un autre). Souvent ce qui compte pour les démonstrations est d'un considérer un système quelconque, sans précision

5.3. Partition de E

Heuristique - Classe d'équivalence : partition de E
Avoir une relation d'équivalence, c'est faire l'assimilation entre différents objets à priori différents et finalement identique (ou plutôt équivalent) du point de vue de la relation. L'ensemble du départ est alors réduit en partie plus petite, ces éléments sont les classes d'équivalence. Elles forment une partition de l'ensemble initial.

Définition - Partition d'un ensemble
Une partition de E est un ensemble de sous-ensembles (non vides) de E tel que :
— leur réunion fait E
— leur intersection 2 à 2 est vide

Proposition - Partition de E
Si $\mathscr{R}$ est une relation d'équivalence sur E, alors ses classes d'équivalence forment une partition de E.

Démonstration
On note O_i, la famille des classes d'équivalence (la notion de famille est vue en fin de chapitre).
Pour tout $x \in E$, x appartient à sa propre classe d'équivalence, donc $x \in \bigcup_i O_i$,
donc $E \subset \bigcup_i O_i$.
Réciproquement, toutes les classes d'équivalences O_i sont des parties de E.
Donc $\bigcup_i O_i \subset E$.
Finalement $E = \bigcup_i O_i$.
Soit O_i et O_j deux classes d'équivalence.
Si $x \in O_i \cap O_j$, alors tous les éléments de O_i sont en relation avec x donc $O_i = C(x)$.
De même tous les éléments de O_j sont en relation avec x donc O_j est la classe de x.
Donc ou bien $O_i = O_j (= C(x))$, ou bien $O_i \cap O_j = \emptyset$. □

Remarque - La réciproque est vraie
Etant donnée une partition sur E : $E = \bigcup_{i\in I} O_i$.
Considérons alors $\mathscr{R}$: $(x \mathscr{R} y)$ ssi $\exists\, i \in I$ tel que $x \in O_i$ ET $y \in O_i$.
$\mathscr{R}$ est une relation d'équivalence sur E.

Remarque - Classes d'équivalence et dénombrement
Si E fini se décompose en classe d'équivalence $(O_i)_{i\in I}$, alors $\#E = \sum_{i\in I} \#O_i$.
Il arrive souvent que E se décompose en n classes d'équivalence toutes de même cardinal c. Dans ce cas : $\#E = c \times n$.

Application - Dénombrement et classe d'équivalence
La relation $\mathscr{R}$ définie sur $F \times G$ par :

$$(a,b)\mathscr{R}(c,d) \Longleftrightarrow a = c$$

est une relation d'équivalence.
Les classes d'équivalence sont en nombre de $\#F$. Et chacune des classes possède exactement $\#G$ éléments.
Donc $\#(F \times G) = \sum_{i\in I} \#O_i = \sum_{a\in F} \#G = \#G \times \sum_{a\in F} 1 = \#G \times \#F$.
Il s'agit vraiment de la formalisation du premier résultat de dénombrement…

6. Bilan

Synthèse

⇝ Les ensembles, dont on a vu qu'ils étaient à la base des raisonnements mathématiques, peuvent être « travaillés ». Ils peuvent être coupés en morceaux, avec des classes d'équivalence ou bien structurés visuellement avec une relation d'ordre.

⇝ Selon chaque situation, on fait évoluer notre regard !

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Montrer que $\mathscr{R}$ est une relation d'ordre
— Savoir-faire - Montrer que $a = \sup E$
— Savoir-faire - Montrer que $\mathscr{R}$ est une relation d'équivalence

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$:=$	Egalité, par définition (du terme de gauche)		autre notation : $\overset{\text{def.}}{s} =$
$\Leftrightarrow, \sim, \equiv, \dots$	Relations d'équivalence variées	Réflexive, Symétrique, Transitive	
$\frac{E}{\mathscr{R}}$	Ensemble des classes d'équivalence sur E pour la relation d'équivalence $\mathscr{R}$	Les classes d'équivalence forment une partition de E	
$S_{E\setminus\mathscr{R}}$	Système de représentants de $\frac{E}{\mathscr{R}}$	$S_{E\setminus\mathscr{R}} \subset E$ et $\forall\, x \in E, \exists\, ! s \in S_{\frac{E}{\mathscr{R}}}$ tel que $x \mathscr{R} s$.	
$\Rightarrow, \leqslant, \subset, \vert, \dots$	Relations d'ordre variées	Réflexive, Antiymétrique, Transitive	
$\max E$	Plus grand élément de E pour UNE relation d'ordre fixée a priori	$\max E \in E$ et $\forall\, x \in E$, $x \leqslant \max E$ (ou $\subset$.....)	Si la relation est totale, $\max E$ est au plus unique.
$\min E$	Plus petit élément de E pour UNE relation d'ordre fixée a priori	$\min E \in E$ et $\forall\, x \in E$, $\min E \leqslant x$ (ou $\subset$.....)	Si la relation est totale, $\min E$ est au plus unique.
$\sup E$	Plus petit des majorants de E	$\forall\, x \in E$, $x \leqslant \sup E$ et $[\forall\, x \in E, x \leqslant y \Rightarrow \sup E \leqslant y$	Au plus unique.
$\inf E$	Plus grand des minorants de E	$\forall\, x \in E$, $\inf E \leqslant x$ et $[\forall\, x \in E, y \leqslant x \Rightarrow y \leqslant \inf E$	Au plus unique.

Retour sur les problèmes

54. Voir cours
55. Voir cours
56. Voir cours
57. Pas de plus grand élément à $[0,1[$. Mais un plus petit élément à tous ses majorants : $\sup[0,1[= 1$, on l'appelle la borne supérieure.

58. Si les applications sont bien définies.
    Alors une relation $\mathscr{R}$ est une application f de E^2 dans $\{0,1\}$, avec $f((a,b)) = 1$ ssi $a\mathscr{R}b$.
Si les relations sont bien définies.
    Alors une application f de E sur F est définie par $f(a) = b$ ssi $a\mathscr{R}b$.

Troisième partie

Arithmétique & Structures élémentaires

Chapitre 13

Groupes

Résumé -

Comme structure algébrique, nous devons étudier les groupes (une seule loi, interne), les anneaux et corps (deux lois internes) et les espaces vectoriels (deux lois internes et une externe). Nous parlerons sûrement à l'occasion d'algèbre et sûrement d'espace affine.
Le chapitre qui suit est assez court, et se concentre sur la structure de groupes.
La notion de groupe a été formalisée au début du XIX-ième siècle mais n'a trouvé toute sa force qu'à la fin du siècle. Nous préparerons quelques notions de seconde année. Et nous reprendrons cette notion en étudiant au second semestre le groupe des permutations, et ensuite nous verrons agir des groupes sur les matrices carrées.

— *Michaël Launay - Structure algébrique - https ://www.youtube.com/watch ?v=RaqlxOihGxw*
— *PoincareDuality - « Les maths ne sont qu'une histoire de Groupe » Poincaré par Etienne Ghys - https ://www.youtube.com/watch ?v=dLwi_opxLxs*
— *Interview Cirm - Claire voisin - https ://www.youtube.com/watch ?v=vcwMTpgNlQA*

Sommaire

1. Problèmes 256
2. Lois de composition internes 257
2.1. Définitions 257
2.2. Propriétés directes 258
2.3. Induction 258
3. Structure de groupe 258
3.1. Définition et propriétés 258
3.2. Groupes produits 259
3.3. Exemples 260
4. Sous-groupe 263
4.1. Définition et caractérisations 263
4.2. Intersection 264
4.3. Sous-groupe engendré 265
4.4. Démontage d'un groupe 267
5. Morphismes de groupes 270
5.1. Définition et propriété immédiate 270
5.2. Image et noyau d'un morphisme 270
5.3. Premier théorème d'isomorphisme 271
6. Bilan 272

1. Problèmes

Problème 59 - Structure

En MPSI, la recherche de la démonstration, optimale la plupart du temps conduit à réfléchir précisément sur les hypothèses qui permet d'obtenir les résultats. Ainsi les objets sont épurés sur les hypothèses principales.
De quel ensemble et avec quelle loi (structure) minimale doit-on partir pour l'essentiel de nos théorèmes à l'origine ?

Problème 60 - Résolution des équations polynomiales

Comment démontrer qu'en règle générale, un polynôme de degré 5 n'admet pas de formules explicites des racines du polynôme ?
C'est l'une des questions qui a conduit GALOIS à créer (inventer, découvrir) la notion de groupe… Quel chemin l'a conduit à cette construction ?

Histoire - Evariste Galois



La vie (très courte et très romantique) d'Evariste Galois (1811-1832) pourrait faire la base d'un excellent film…
On le présente souvent comme le premier, avec de nombreuses années d'avance, qui a compris le rôle fondamental de la structure de lois internes et de groupe. Il a ainsi démontré que pour $\geqslant 5$, il n'existe pas de formule explicite et avec des racines n^e exprimant les racines d'un polynôme quelconque de degré n.

Problème 61 - Groupe de Poincaré

En physique relativiste, les éléments de l'espace sont des quadruplets (x, y, z, t).
On appelle groupe de Poincaré l'ensemble $(G, \circ)$ des transformations $\varphi : \mathbb{R}^4 \to \mathbb{R}^4 \in G$ tel que pour tout paire de quadruplets (x, y, z, t) et (x', y', z', t'), la distance est conservée :
$(x-x')^2+(y-y')^2+(z-z')^2-c^2(t-t')^2 = (X-X')^2+(Y-Y')^2+(Z-Z')^2-c^2(T-T')^2$
où $\varphi(x, y, z, t) = (X, Y, Z, T)$ et $\varphi(x', y', z', t') = (X', Y', Z', T')$.
Montrer qu'il s'agit bien d'un groupe.

Problème 62 - Mariage chez les Murngin (citation)

A New York, [Lévi-Strauss] s'était lancé dans un vaste travail de sociologie théorique qui devint sa thèse de doctorat (aujourd'hui célèbre) sur les structures ?élémentaires de la parenté. Un jour, dans l'étude d'un certain type de mariage, il se heurta à des difficultés inattendues et pensa qu'un mathématicien pourrait lui venir en aide.
D'après ce qu'ont observé les sociologues travaillant ? sur le terrain ?, les lois de mariage des tribus indigènes d'Australie comportent un mélange de règles exogamiques et endogamiques dont la description et l'étude posent des problèmes combinatoires parfois compliqués. Le plus souvent le sociologue s'en tire par l'énumération de tous les cas possibles dans l'intérieur d'un système donné. Mais la tribu des Murngin, à la pointe Nord de l'Australie, s'était donné un système d'une telle ingéniosité que Lévi-Strauss n'arrivait plus à en dérouler les conséquences. En désespoir de cause il me soumit son problème.
Le plus difficile pour le mathématicien, lorsqu'il s'agit de mathématique appliquée, est souvent de comprendre de quoi il s'agit et de traduire dans son propre langage les données de la question. Non sans mal, je finis par voir que tout se ramenait à étudier deux permutations et le groupe qu'elles engendrent. Alors apparut une circonstance imprévue. Les lois de mariage de la tribu Murngin, et de beaucoup d'autres, comportent le principe suivant : ? Tout homme peut épouser la fille du frère de sa mère ? ou, bien entendu, l'équivalent de celle-ci dans la classification matrimoniale de la tribu. Miraculeusement, ce principe revient à dire que les deux permutations dont il s'agit sont échangeables, donc que le groupe qu'elles engendrent est abélien. Un système qui à première vue menaçait

> d'être d'une complication inextricable devient ainsi assez facile à décrire dès lors qu'on introduit une notation convenable. Je n'ose dire que ce principe a été adopté pour faire plaisir aux mathématiciens, mais j'avoue qu'il m'en est resté une certaine tendresse pour les Murngin.
> Oeuvres scientifiques, André Weil, 1979 p. 567-568

2. Lois de composition internes

2.1. Définitions

Définition - Loi de composition interne (Magma)
Une loi de composition interne sur un ensemble E est une application de $E \times E$ dans E : $\Phi : E \times E \to E, (x, y) \mapsto x \star y$.
On note, pour $(x, y, z) \in E^3$,
$(x \star y) \star z = \Phi(\Phi(x, y), z)$ et $x \star (y \star z) = \Phi(x, \Phi(y, z))$.
Un tel couple $(E, \star)$ est appelé un magma.
Quand la loi interne est clairement identifiée, par abus, on peut dire que E est un magma sans précision supplémentaire.

Exemple - $\mathbb{N}$
$(\mathbb{N}, +)$ ou $(\mathbb{N}, \times)$ sont des magmas.

Définition - Caractéristiques
On dit que le magma $(E, \star)$:
- est *commutatif* si $\forall (x, y) \in E \times E$, $x \star y = y \star x$
- est *associatif* si $\forall (x, y, z) \in E \times E \times E$, $x \star (y \star z) = (x \star y) \star z$
- est unifère ou possède un élément *neutre* s'il existe $e \in E$ tel que $\forall x \in E$, $e \star x = x \star e = x$ (e est alors l'élément neutre.)

Pour x élément de E, on dit qu'un élément y de E est un *symétrique* ou un *inverse* de x pour $\star$ si $x \star y = y \star x = e$, ($e$ neutre de E)

Définition - Monoïde
Un magma $(M, \star)$ associatif et unifère est appelé un monoïde.

Remarque - Notations
Plusieurs remarques

1. Les lois de composition interne sont usuellement notées $\star$, $\perp$, $\top$, $+$, $\times$, en notation multiplicative $x \star y = xy$.
2. La notation additive est usuellement réservée à une loi commutative et associative, dans ce cas le symétrique de x (s'il existe) est noté $-x$.
3. Lorsque la loi est commutative et associative, on peut écrire :
$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n \text{ (notation additive) } ou \prod_{i=1}^{n} x_i = x_1 \dots x_n \text{ (notation multiplicative).}$$
4. Si la loi $\star$ est associative, on peut écrire $x^{\star n} = x \star \cdots \star x$ (n termes x).
En notation multiplicative on obtient ainsi x^n et en notation additive nx.

Définition - Distributivité
Supposons que l'ensemble E est muni de deux lois internes $\star$ et $\top$.
On dit que $\star$ est *distributive* par rapport à la loi interne $\top$ si :
$\forall (x, y, z) \in K^3$, $x \star (y \top z) = (x \star y) \top (x \star z)$ (distibutive à gauche)
$\forall (x, y, z) \in K^3$, $(x \top y) \star z = (x \star z) \top (y \star z)$ (distibutive à droite)

2.2. Propriétés directes

Proposition - Unicités (éléments neutres, symétrique)... si existence
Soit $(F, \top)$ un magma.
Si F est unifère, l'élément neutre pour $\top$ est unique.
Soit $(E, \star)$ un monoïde.
Si $x \in E$ admet un symétrique alors celui-ci est unique ;
Si $x, y \in E$ admettent des symétriques x^{-1} et y^{-1}
alors $x \star y$ admet un symétrique : $y^{-1} \star x^{-1}$.
Si x est symétrique alors x est régulier (à gauche et à droite) :
$\forall\, y, z \in E$, $x \star y = x \star z \Rightarrow y = z$ et $y \star x = z \star x \Rightarrow y = z$.

Démonstration
On va faire chacun des cas
- Supposons que e_1 et e_2 soit deux éléments neutres de $(F, \top)$.
Alors comme e_2 est neutre : $e_1 = e_1 \top e_2$ et $e_1 \top e_2 = e_2$
car e_1 est neutre.
Donc $e_1 = e_2$. Il y a au plus un élément neutre.
- Si y_1 et y_2 deux symétriques de x : $y_1 = y_1 \star e = y_1 \star (x \star y_2) = (y_1 \star x) \star y_2 = e \star y_2 = y_2$
- $(y^{-1} \star x^{-1}) \star (x \star y) = y^{-1} \star (x^{-1} \star x) \star y = y^{-1} \star e \star y = y^{-1} \star y = e$
car $\star$ est associative. De même : $(x \star y) \star (y^{-1} \star x^{-1}) = x \star (y \star y^{-1}) \star x^{-1} = x \star e \star x^{-1} = e$.
- Si $x \star y = x \star z$, alors en starisant par x^{-1} (x symétrique) à gauche : $y = x^{-1} \star x \star y = x^{-1} \star x \star z = z$.
De même à droite.

□

2.3. Induction

Il s'agit de l'induction de la loi sur une partie ou une restriction d'un magma E.

Définition - Loi induite
Soit $A \subset E$, avec $(E, \top)$ magma.
A est stable par $\top$ (loi de composition interne sur E) si $\forall x, y \in A$, $x \top y \in A$.
$\top_A = \top_{|A \times A}$ s'appelle la loi induite (par $\top$ sur A).

Remarque - Transmission des propriétés
$\top_A$ est alors une loi interne sur A, i.e. $(A, \top_A)$ est un magma (induit).
Si $\top$ est commutative (resp. associative), $\top_A$ est nécessairement commutative (resp. associative).
En revanche l'élément neutre de $\top$ ou l'élément symétrique de $x \in A$ pour $\top$ (s'ils existent) ne sont pas nécessairement dans A.

3. Structure de groupe

3.1. Définition et propriétés

Un groupe est un monoïde dont tous les éléments sont inversibles :

Définition - Groupe
On appelle groupe un ensemble G muni d'une loi de composition interne $\top$ vérifiant :
- la loi $\top$ est associative ;
- G possède un élément neutre pour $\top$;
- tout élément x de G possède un symétrique pour $\top$ (ou tout élément de G est inversible, est symétrisable).

Si de plus la loi $\top$ est commutative, on dit que le groupe est abélien (ou

commutatif).

Exemple - Groupes des racines de l'unité
L'ensemble $(\mathbb{U},\times)$ est un groupe.
• En effet, $(\mathbb{C},\times)$ est associatif donc en prenant trois éléments z_1,z_2,z_3 de $\mathbb{U}$, donc de $\mathbb{C}$, on a $z_1\times(z_2\times z_3)=(z_1\times z_2)\times z_3$). Ainsi $(\mathbb{U},\times)$ est associative
• Si $z_1,z_2\in\mathbb{U}$, alors $|z_1z_2|=|z_1||z_2|=1$ donc $z_1z_2\in\mathbb{U}$.
• $1\in\mathbb{U}$ est un élément neutre de $\mathbb{U}$: $1\times z=z\times 1=z$.
• Soit $z\in\mathbb{U}$, alors $\frac{1}{z}=\overline{z}\in\mathbb{U}$. Pour les mêmes raisons, puisque si $z\in\mathbb{U}_n$, $\overline{z}\in\mathbb{U}_n$, on peut dire que $(\mathbb{U}_n,\times)$ est un groupe.

Remarque - Sous-groupe
Finalement, on a utilisé ici le fait que $(\mathbb{C},\times)$ était lui même un groupe, que $\mathbb{U}$ est stable par la loi induite, que $1_{\mathbb{C}}\in\mathbb{U}$ et pour tout $z\in U(\subset\mathbb{C})$, $\frac{1}{z}(\in\mathbb{C})\in\mathbb{U}$.
On reviendra sur ces propriétés plus loin.

Histoire - Plusieurs naissances
En fait, cela est comme toujours plus subtil. Il semble que l'idée de groupe est en germe à la fin du XVIII siècle (en particulier chez Lagrange) et donc le concept apparait clairement ensuite mais à plusieurs endroits en même temps : chez Galois en France, dans les écrits de Cayley en Grande-Bretagne ou dans les oeuvres de Dedekind en Allemagne.
Les définitions étant parfois légèrement différentes… (citation : http ://images.math.cnrs.fr/ Un-concept-mathematique-trois)

Proposition - Régularité
Dans un groupe tous les éléments sont réguliers à gauche et à droite

Démonstration
Tous les éléments sont symétriques donc réguliers d'après un point précédent □

Comme des groupes sont des magmas unifère, où tous les éléments sont inversibles par définition :

Théorème - Existence et unicité
Soit $(G,\top)$ un groupe. Alors :
— L'élément neutre est unique.
— Tout élément possède un unique symétrique.
— En notant x^{-1} le symétrique (l'inverse) de x, on a $(x^{-1})^{-1}=x$.
— $(x\top y)^{-1}=y^{-1}\top x^{-1}$.

3.2. Groupes produits

Définition - Produit de groupes
Soient $(G,\perp)$ et $(H,\top)$ deux groupes.
On appelle groupe produit (de ces deux groupes) le groupe $(G\times H,\star)$ tel que

$$\forall\,(x_1,y_1),(x_2,y_2)\in G\times H,\qquad (x_1,y_1)\star(x_2,y_2)=(x_1\perp x_2,y_1\top y_2)$$

Pour aller plus loin - Produit direct. Produit indirect
En réalité, le produit comme il apparait ici est souvent qualifié de produit direct.
Le produit semi-direct est alors le produit de décomposition d'un groupe G sous la forme $G=HK$, où H est un sous-groupe normal ou distingué de G et K est isomorphe à $\frac{G}{H}$.

Il s'agit bien d'un groupe :

Démonstration
• Il est associatif. Pour tout $(x_1,y_1),(x_2,y_2),(x_3,y_3)\in G\times H$,

$$(x_1,y_1)\star\big((x_2,y_2)\star(x_3,y_3)\big)=(x_1,y_1)\star(x_2\perp x_3,y_2\top y_3)=(x_1\perp(x_2\perp x_3),y_1\top(y_2\top y_3))=(x_1\perp x_2\perp x_3,y_1\top y_2\top_3)$$
$$\big((x_1,y_1)\star(x_2,y_2)\big)\star(x_3,y_3)\big)=(x_1\perp x_2,y_1\top y_2)\star(x_3,y_3)=\cdots=(x_1\perp x_2\perp x_3,y_1\top y_2\top_3)$$

• Son élément neutre est (e_G,e_H), car pour tout $(x,y)\in G\times H$,

$$(e_G,e_H)\times(x,y)=(e_g\perp x,e_H\top y)=(x,y)=(x\perp e_g,y,\top e_h)=(x,y)\star(e_g,e_H)$$

• Tous ses éléments sont inversibles, pour tout $(x,y)\in G\times H$,

$$(x^{-1},y^{-1})\times(x,y)=(x^{-1}\perp x,y^{-1}\top y)=(e_g,e_H)=\cdots=(x,y)\star(x^{-1},y^{-1})$$

□

Remarque - Souvent $G=H$
On considère donc le groupe produit noté$(G^2,\perp)$ plutôt que $(G^2,\perp^2)$.
Et par récurrence, on peut étendre le produit de groupes à plus de deux groupes.

3.3. Exemples

Groupes triviaux

Exemple - Avec l'addition
Les ensembles de nombres munis de l'addition : $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ sont des groupes commutatifs.

Exemple - Avec la multiplication
Les ensembles de nombres munis de la multiplication : $(\mathbb{Q}^*,\times),(\mathbb{R}^*,\times),(\mathbb{C}^*,\times)$ sont des groupes commutatifs.
Moins trivialement : $(\mathbb{U}_n,\times)$ est un groupe.

Ensemble $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Définition - Ensemble des classes d'équivalence modulo n
Soit $n\in\mathbb{N}$, fixé.
La relation $\equiv_n$ ou encore $\cdot\equiv\cdot[n]$ est une relation d'équivalence sur $\mathbb{Z}$.
L'ensemble des classes d'équivalence associées est noté $\frac{\mathbb{Z}}{n\mathbb{Z}}$.
Un système de représentant est $[\![0,n-1]\!]$, puisque $\frac{\mathbb{Z}}{n\mathbb{Z}}=\{\overline{0},\overline{1},\dots\overline{n-1}\}$,
où pour tout $k\in[\![0,n-1]\!]$, $\overline{k}=\{k,k+n,k+2n\dots k-n\dots\}=\{k+rn,r\in\mathbb{Z}\}$.
On peut alors définir sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ les lois $\overline{+}$ et $\overline{\times}$ par :

$$\overline{h}\overline{+}\overline{k}=\overline{h+k}\qquad\overline{h}\overline{\times}\overline{k}=\overline{h\times k}$$

Remarque - Le plus dur dans ce qui précède
est de démontrer que les lois $\overline{+}$ et $\overline{\times}$ sont bien définies.
C'est-à-dire qu'elles sont indépendantes des représentants de $\overline{k}$ et $\overline{h}$ choisis.
Nous ferons cette démonstration dans le cours d'arithmétique

Proposition - Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},\overline{+}\right)$
Pour tout entier n, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},\overline{+}\right)$ est un groupe commutatif.
Son élément neutre est $\overline{0}$, et l'opposé de $\overline{k}$ est $\overline{n-k}$.

Démonstration
Pour tout $h,k\in\mathbb{Z}$, $\overline{h}\overline{+}\overline{k}=\overline{h+k}=\overline{k+h}=\overline{k}\overline{+}\overline{h}$.
Pour tout $k\in\mathbb{Z}$, $\overline{k}\overline{+}\overline{0}=\overline{k+0}=\overline{k}\qquad\overline{k}\overline{+}\overline{n-k}=\overline{k+n-k}=\overline{n}=\overline{0}$. □

Analyse - Et pour la multiplication $\overline{\times}$?
En revanche, il existe des diviseurs de 0, donc des éléments non inversibles, pour la multiplication modulo n : les diviseurs de n.
Mais si k est premier avec n, alors d'après le théorème de Bézout :

$$\exists\,u,v\in\mathbb{Z}\mid uk+vn=1\qquad\overline{u\times k}=\overline{uk}=\overline{uk+vn}=\overline{1}$$

Proposition - Groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}},\overline{\times}\right)$ avec p premier
Pour tout nombre premier p, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}},\overline{\times}\right)$ est un groupe commutatif.
Son élément neutre est $\overline{1}$, et l'opposé de $\overline{p}$ est obtenu en exploitant le théorème de Bézout.

On peut donc obtenir l'inverse de $\overline{k}$ en exploitant l'algorithme d'Euclide.

Exercice
A démontrer

Correction
Pour tout $h,k\in\mathbb{Z}$, $\overline{h}\times\overline{k}=\overline{h\times k}=\overline{k\times h}=\overline{k}\times\overline{h}$.
Pour tout $k\in\mathbb{Z}$, $\overline{k}+\overline{1}=\overline{k\times 1}=\overline{k}$.
Pour l'existence de l'inverse, voir l'analyse précédente.

Remarque - Autre point de vue

Dans le cours sur les anneaux, nous définirons le groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}^{\star},\overline{\times}\right)$, valable pour tout entier n, en ne considérant que les classes inversibles, modulo n.
Dans le cas où n est premier, on retrouve le groupe précédent.

« Petits » groupes

Comme les groupes sont réguliers, il ne peut y avoir chaque lettre ne peut apparaite plus d'une fois par ligne et par colonne.
Remplir ces tableaux, c'est comme remplir un carré latin (nom mathématique des sudoku).

Analyse - Groupe à deux éléments

Essayons de construire un groupe à deux éléments : a et b.
L'un des deux éléments est le neutre, supposons qu'il s'agisse de a.
On a donc $a^2=a$ et $ab=ba=b$.
b est inversible, nécessairement $b^2=a$.
Ce groupe se résume dans le tableau :

$\nearrow_\top$	a	b
a	a	b
b	b	a

C'est le seul groupe à deux éléments. Notons qu'il est commutatif.
Mais surtout remarquons qu'il s'incarne ou a de nombreux avatars :

- a = fonction croissante, b = fonction décroissante et $\top=\circ$
- $a=1$ (ou classe des nombres positifs), $b=-1$ (ou classe des nombres négatifs) et $\top=\times$
- $a=0$ (ou classe des entiers pairs), $b=1$ (ou classe des entiers impairs) et $\top=+$ dans $\frac{\mathbb{Z}}{2\mathbb{Z}}$
- $a=\mathrm{id}_C$ et b = symétrie (ou involution quelconque) et $\top=\circ$
- …

Exercice
Construire un (le) groupe de 3 éléments

Correction
Par essais/erreurs, il s'agit de

$\nearrow_\top$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dans la construction, on voit une notion importante : à cause de la régularité, il n'est pas possible de trouver sur une même ligne ou une même colonne deux valeurs identiques.
Par suite, dans chaque ligne et chaque colonne, on retrouve toutes les valeurs de G.
Une incarnation possible est $\frac{\mathbb{Z}}{3\mathbb{Z}}$.

Groupes matriciels

L'ensemble des matrices $(\mathcal{M}_{n,p}(\mathbb{K}),+)$ est un groupe. Il nous intéresse assez peu.
L'ensemble $(\mathcal{M}_n(\mathbb{K}),\times)$ n'est pas un groupe! (c'est un monoïde) Tous les éléments ne sont pas inversibles.
En revanche

- $(GL_n(\mathbb{K}),\times)$, ensemble des matrices inversibles est un groupe appelé, le groupe linéaire. Par définition : $GL_n(\mathbb{K})=\{M\in\mathcal{M}_n(\mathbb{K})\mid\exists N\in\mathcal{M}_n(\mathbb{K})\text{ tel que }M\times N=N\times M=I_n\}$

Pour aller plus loin - Au début d'année…
Nous avons vu apparaître à plusieurs reprises des calculs avec $\{1,j,j^2\}$ (expression des racines d'un polynôme de degré 3 ou bien calcul de la somme $S_k=\sum_{i\equiv k[3]}\binom{n}{i}\ldots$). Cela était nécessaire, car il s'agit de la meilleure incarnation du groupe (unique) à trois éléments

Pour aller plus loin - Groupes à 4 éléments
Il existe deux groupes à 4 éléments : $D_4\simeq\{1,i,-1,-i\}\simeq\frac{\mathbb{Z}}{4\mathbb{Z}}$ et V_4 le groupe de Klein.

$V_4:=$

$\nearrow_\top$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Il s'incarne par exemple dans le groupe des symétries par rapports aux médiatrices d'un triangle équilateral et de la transformation identité.
$a:[BCD]\to[BCD]$, $b:[BCD]\to[BDC]$, $c:[BCD]\to[DCB]$ et $d:[BCD]\to[CBD]$

- $(\mathcal{O}_n(\mathbb{K}),\times)$, ensemble des matrices orthogonales est un groupe appelé, le groupe orthogonal.
  Par définition : $\mathcal{O}_n(\mathbb{K})=\{M\in\mathcal{M}_n(\mathbb{K})\mid M^T\times M=I_n\}$

Groupes des permutations

Un groupe très important, on reviendra sur cette notion plus tard…

Proposition - Groupe des permutations d'un ensemble
Soit X un ensemble non vide. On note S_X l'ensemble des permutations de X (c'est-à-dire des bijections de X dans X). Alors $(S_X,\circ)$ est un groupe, généralement non commutatif, appelé groupe des permutations de X.

Remarque - Permutation
Qu'est-ce qu'une permutation de X ?
Il s'agit, par σ de changer « l'ordre » ou notre regard sur tous les éléments de X.
Donc cela signifie que

$$\{\sigma(x),x\in X\}=X$$

et donc σ est surjective. Il suffit de montrer que σ est injective : $\sigma(i)=\sigma(j)\Rightarrow i=j$..

Démonstration
Point par point :

- Pour tout $\sigma_1,\sigma_2\in S_X$,
$$\forall\, x\in X,(\sigma_1\circ\sigma_2)(x)=\sigma_1(\underbrace{\sigma_2(x)}_{\in X})\in X$$
  On notera que $\sigma_1\circ\sigma_2$ est bien une bijection de X.
  Donc $\circ$ est bien une loi de composition interne de S_X.
- Puis cette loi est associative.
  Pour tout $\sigma_1,\sigma_2,\sigma_3\in S_X$,
$$\forall\, x\in X,(\sigma_1\circ(\sigma_2\circ\sigma_3))(x)=\sigma_1(\sigma_2(\sigma_3(x)))=((\sigma_1\circ\sigma_2)\circ\sigma_3)(x)$$
- S_X possède un élément neutre : $id_X:x\mapsto x$:
  $id\in S_X$ et pour tout $\sigma\in S_X:\forall\, x\in X,\ id(\sigma(x))=\sigma(x)=\sigma(id(x))$.
- Last but not least : on note pour tout $\sigma\in S_X$,
$$\sigma':x\mapsto y\text{ tel que }x=\sigma(y)$$
  Clairement $\sigma^{-1}\circ(\sigma(y))=\sigma^{-1}(x)=y$ et $\sigma\circ\sigma^{-1}(x)=\sigma(y)=x$,
  donc σ est bien inversible et d'inverse σ^{-1}.
  Mais il faudrait vérifier que σ^{-1} ainsi définie existe bien. Pour cela, il est nécessaire que tout $x\in X$ soit aussi l'image d'un y par σ, ou encore que $\sigma(X)=X$.
  Or σ est une permutation de X, donc cette hypothèse est bien vérifiée (cf. remarque).

□

Ce groupe non commutatif sera longuement étudié plus tard dans l'année.

Groupes et géométrie

Proposition - Groupes des similitudes directes du plan $\mathbb{C}$
L'ensemble des similitudes directes est un groupe pour la loi $\circ$.
L'élément neutre est l'identité.
L'inverse de la similitude de centre Ω, d'angle θ et de rapport k est la similitude de centre Ω, d'angle $-\theta$ et de rapport $\frac{1}{k}$.
L'inverse de la translation de vecteur $\vec{u}$ est la translation de vecteur $-\vec{u}$.

Démonstration
Nous sommes bien obligé de considérer les translations car la composition de deux rotations de centre A et B respectivement, d'angle θ et $2\pi-\theta$ et de rapports 1 est la translation de vecteur $2\overrightarrow{AB}$.
Rappelons que la similitude de centre $\Omega(\omega)$, d'angle θ et de rapport k est $z\mapsto ke^{i\theta}(z-\omega)+\omega$.
A partir de cette notation, on peut tout démontrer. □

Pour aller plus loin - Programme d'Erlangen
Felix Klein (1849-1925) est un mathématicien allemand qui proposa dans le programme d'Erlangen de re« voir » toute les géométries en étudiant les groupes de symétrie qui agisse sur l'espace en question…
Il a eu une grosse influence sur Henri Poincaré.



4. Sous-groupe

4.1. Définition et caractérisations

Par la suite, on considérera $(G, \top)$ un groupe.

Définition - Sous-groupe
$H \subset G$ (non vide) est un sous-groupe de G si H est stable pour la loi interne et si la loi induite (restriction de la loi à H) munit H d'une structure de groupe. On note $H < G$

Proposition - Elément neutre et symétriques
Soit H un sous-groupe de G.
Alors l'élément neutre de H est l'élément neutre de G.
Si $x \in H$, le symétrique de x dans H est le symétrique de x dans G.

Démonstration
Soit e_1 l'élément neutre de H et e celui de G. $\underbrace{e_1 \top e_1}_{\in H} = e_1 = \underbrace{e \top e_1}_{\in G}$
Et comme e_1 est régulier (dans G) : $e_1 = e$.
Puis si on note x' l'inverse de x dans H, $x \top x' = e = x \top x^{-1}$
Par régularité :
en « composant à gauche » par x^{-1}, inverse de x dans G (par la suite, tout se passe dans G)

$$x' = x^{-1} \top x \top x' = x^{-1} \top x \top x^{-1} = x^{-1}$$

□

Théorème - Caractérisation 1
Soit $H \subset G$. H est un sous-groupe de G si et seulement si il vérifie :
- $H \neq \emptyset$
- $\forall (x, y) \in H^2, x \top y \in H$
- $\forall x \in H, x^{-1} \in H$

Théorème - Caractérisation 2
Soit $H \subset G$. H est un sous-groupe de G si et seulement si il vérifie :
- $H \neq \emptyset$
- $\forall (x, y) \in H^2, x \top y^{-1} \in H$
  (en notation multiplicative : $\forall (x, y) \in H^2, xy^{-1} \in H$;
  en notation additive : $\forall (x, y) \in H^2, x - y \in H$)

Savoir faire - Démontrer que H est un (sous-)groupe
Dans la pratique, lorsque H est une partie de E, groupe. On démontre qu'il s'agit d'un sous-groupe de E
- avec la caractérisation 1, lorsque H et E sont explicites
- avec la caractérisation 2, lorsque H et E sont théoriques

Démonstration
On a trois propositions équivalentes à démontrer, nous allons faire en trois temps

$$A_1 \Longrightarrow A_2 \Longrightarrow A_3 \Longrightarrow A_1$$

1. Supposons que H est un sous-groupe de G.
   - Nécessairement H n'est pas vide.
   - H est stable pour la loi interne donc $\forall (x, y) \in H^2, x \top y \in H$
   - Et le dernier point : $\forall x \in H, x^{-1} \in H$ à été démontré dans la proposition précédente.
2. Supposons que H vérifie les trois assertions de la caractérisation 1.

Pour aller plus loin - Le « monstre »
Il s'agit du plus gros groupe fini « connu ». On l'appelle le Monstre M ou groupe de Fischer-Griess F_1. Son ordre (= son cardinal ici) est $246 \times 320 \times 59 \times 76 \times 112 \times 133 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71 = 808017424794512875886459904961710757005754368000000000 \approx 8 \times 10^{53}$.
C'est bien un nombre fini (mais c'est gros). Il a été découvert (est-ce le bon verbe?) ou construit en 1980

Pour aller plus loin - Action de groupe et représentation
Étant donné un groupe G, dont la loi est notée multiplicativement et dont l'élément neutre est noté e, on peut définir une action (ou opération) de G sur un ensemble E par une application : $G \times E \to E$, $(g, x) \mapsto g \cdot x$ vérifiant les propriétés suivantes : $\forall\, x \in E$, $e \cdot x = x$ et $\forall\, g, g' \in G, \forall\, x \in E$, $g' \cdot (g \cdot x) = (g \top g') \cdot e$.
(Très) nombreuses situations de présence de groupe sont de cette forme là, avec un ensemble E donné.
Réciproquement, si on connait très bien E sur lequel agit G, alors on apprend à connaître G.
La notion d'orbite, de permutations de E,

   - $H \neq \emptyset$
   - $\forall (x, y) \in H^2$, $z = y^{-1} \in H$, d'après la troisième assertion.
     Puis $x \top z = x \top y^{-1} \in H$ d'après la seconde assertion.
     Donc $\forall (x, y) \in H^2$, $x \top y^{-1} \in H$.
3. Supposons que H vérifie les deux assertions de la caractérisation 2.
   - H n'est pas vide, on doit montrer qu'il est stable pour la loi interne.
     La loi $\top$ est nécessairement associative sur $H \subset G$.
     Soit $x \in H$, alors $x \in G$, et $e = x \top x^{-1} \in H$ d'après la seconde assertion.
     En outre, tout élément $x \in H \subset G$ possède un symétrique x^{-1} dans G, qui est aussi dans H :

$$e, x \in H \Longrightarrow e \top x^{-1} = x^{-1} \in H$$

□

Exercice
Montrer que si $H_1 < (G_1, \perp)$ et $H_2 < (G_2, \top)$ alors $H_1 \times H_2$ est un sous-groupe du groupe produit $(G_1 \times G_2, \star)$.

Correction
On va exploiter la seconde caractérisation.
Puisque $e_1 \in H_1$, $e_2 \in H_2$, alors $(e_1, e_2) \in H_1 \times H_2$ et donc $H_1 \times H_2$ est non vide.
Puis si $(x_1, x_2), (y_1 y_2) \in H_1 \times H_2$, alors

$$(x_1, x_2) \star (y_1, y_2)^{-1} = (x_1, x_2) \star (y_1^{-1}, y_2^{-1}) = (\underbrace{x_1 \perp y_1^{-1}}_{\in H_1}, \underbrace{x_2 \perp y_2^{-1}}_{\in H_2}) \in H_1 \times H_2$$

Donc $H_1 \times H_2$ est un sous-groupe du groupe produit $(G_1 \times G_2, \star)$.

4.2. Intersection

Théorème - Intersection de deux sous-groupes
Soit H et K deux sous-groupes de $(G, \top)$.
Alors $H \cap K$ est un sous-groupe de G.

Démonstration
$e \in H$ et $e \in K$, donc $H \cap K$ n'est pas vide.
Soit $x, y \in H \cap K$, alors $xy^{-1} \in H$ et $xy^{-1} \in K$, donc $xy^{-1} \in H \cap K$. □

L'exercice suivant donne TOUS les sous-groupes de $(\mathbb{Z}, +)$:
Exercice

1. Soit $a \in \mathbb{Z}$. Montrer que $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
2. Soit G un sous-groupe de $(\mathbb{Z}, +)$, $G \neq \{0\}$.
   Justifier que $G \cap \mathbb{N}^*$ a un plus petit élément $a > 0$.
   Montrer que $G = a\mathbb{Z}$ (utiliser la division euclidienne).

Correction

1. $0 \in a\mathbb{Z}$ et si $x, y \in a\mathbb{Z}$, alors $x - y = ka - ha = (k - h)a \in a\mathbb{Z}$.
2. $G \cap \mathbb{N}^* \subset \mathbb{N}^*$, donc il a un plus petit élément, noté $a > 0$.
   On a nécessairement $a\mathbb{Z} \subset G$ Soit $x \in G$, on applique la division euclidienne : $x = pa + q$.
   Or $q = x - pa \in G$, par stabilité et donc $q \in G$, mais $q \in [\![0, a[\![$, donc $q = 0$, sinon, on a une contradiction avec la définition de a.
   Donc $x = pa$ et $G \subset a\mathbb{Z}$.

La démonstration s'adpate à une infinité de sous-groupe.

Théorème - Intersection de sous-groupes
Soit $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, \top)$. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration
$\forall\, i \in I$, $H_i < G$, donc $\bigcap_{i\in I} H_i \subset G$.
$\forall\, i \in I$, $e \in H_i$, car H_i est un groupe. Donc $e \in \bigcap_{i\in I} H_i$, qui n'est pas vide, donc.
Soit $x, y \in \bigcap_{i\in I} H_i$, alors pour tout $i \in I$, $x, y \in H_i$ et $xy^{-1} \in H_i$
Donc $xy^{-1} \in \bigcap_{i\in I} H_i$. □

4.3. Sous-groupe engendré

Première manipulation (trouver un candidat)

Analyse - Plus petit groupe contenant une partie A de G
Considérons une partie A (ensemble) d'un groupe G.
On note $\mathscr{A} = \{H < G \mid A \subset H\}$, l'ensemble de tous les sous-groupes de G contenant A.
Alors $\mathscr{A}$ est non vide car $G \in \mathscr{A}$.
On se souvient, qu'en théorie des ensembles, on a vu que $\inf(A, B) = A \cap B$
(inf est ici la borne inférieure pour la relation d'ordre de l'inclusion, i.e. le plus grand ensemble des plus petits ensembles que A et B).
Considérons alors $< A >:= \bigcap_{H\in\mathscr{A}} H$, l'intersection (non dénombrable, peut-être) de tous les sous-groupe contenant A.
Cette intersection est un sous-groupe et elle contient A.
En fait $< A >$ est le plus petit élément de $\mathscr{A}$.

Définition - Groupe engendré
Soit $(G, \top)$ un groupe. Soit A une partie de G.
On appelle groupe engendré par A, le plus petit sous-groupe de G, parmi les sous-groupes de G contenant A.
On le note $< A >$. On a donc $< A >= \bigcap_{H\in\mathscr{A}} H = \min \mathscr{A}$
(où $\mathscr{A} = \{H < G \mid A \subset H\}$).

Il faut démontrer que $\bigcap_{H\in\mathscr{A}} H$ est bien le plus petit sous-groupe de G contenant A.

Démonstration
Comme, pour tout $H \in \mathscr{A}$, $A \subset H$, on a bien $A \subset \bigcap_{H\in\mathscr{A}} H$.
Par ailleurs, $\bigcap_{H\in\mathscr{A}} H$ est une intersection de sous-groupes de G. Donc il forme bien d'un sous-groupe de G.
Il reste à démontrer que c'est le plus petit.
Soit K, un sous-groupe de G contenant A. Alors nécessairement $K \in \mathscr{A}$.
Donc K fait partie des sous-groupes donc l'intersection définie $< A >$,
on a donc $< A >= K \cap \left(\bigcap_{H\in\mathscr{A}\setminus K} H \right) \subset K$. □

Proposition - Croissance de l'engendrement
Si $A \subset B$ sont deux parties d'un groupe G.
Alors $< A > \subset < B >$

Démonstration
$< B >$ est le plus petit sous-groupe contenant B donc A car $A \subset B$.
Donc $< B >$ est un sous-groupe de G contenant A.
Mais $< A >$ est le plus petit des sous-groupe contenant A, donc il est plus petit que B : $< A > \subset < B >$. □

Application - Réflexes
Si A est un sous-groupe de G qui est contenu dans B, alors nécessairement $< A >= A \subset < B >$.
Si B est un sous-groupe de G qui est contient A, alors nécessairement $< A > \subset < B >= B$.

Savoir faire - Comment trouver le sous-groupe engendré par une partie A?
Il faut
1. *Pré-sentir* la bonne description (efficace) de ce sous-groupe. On donne alors un nom à cet ensemble K.
2. Montrer que K est bien un groupe, qui contient A
3. Montrer que K est nécessairement entièrement inclus dans $< A >$ ou dans tout sous-groupe de $\mathscr{A}$.

Comme $< A >$ est le plus petit sous-groupe contenant A, propriété vérifiée par K, alors $< A >= K$

Croissance par engendrement (deuxième point de vue)

Attention - Nom contradictoire?
Ce nom semble contradictoire. Par groupe engendré on entend plutôt quelque chose qui s'agrandit (pour l'inclusion) à partir de A, alors qu'il s'agit visiblement de quelque chose qui diminue à partir de G.
A-t-on la même chose?

Analyse - Engendrement
On aurait plutôt envie de considérer $\overline{A} := \{a_1 \star a_2 \star \cdots \star a_k \mid k \in \mathbb{N}, a_1, a_2, \cdots a_k \in \mathbb{N}\}$,
ensemble de tous les éléments obtenables à partir de répétition de produit (fini) de A.
C'est bien en ensemble engendré par A. En fat :
• cet ensemble contient bien A, avec $n = 1$ et a_1 décrivant tous les éléments de A. • cet ensemble est un groupe A, avec $n = 2$ et $a_2 = a_1^{-1}$, on a $e_G \in \overline{A}$.
si $a_1 \star a_2 \star \cdots \star a_k$, $b_1 \star b_2 \star \cdots \star b_m \in \overline{A}$, alors,
$(a_1 \star a_2 \star \cdots \star a_k) \star (b_1 \star b_2 \star \cdots \star b_m)^{-1} = a_1 \star a_2 \star \cdots \star a_k \star b_m^{-1} \star b_{m-1}^{-1} \star \cdots \star b_1^{-1} \in \overline{A}$.
Enfin, il contient tous les sous-groupe H contenant A,
car pour tout $i \in \mathbb{N}_k$, $a_i \in A \subset H$. H est un groupe donc $a_1 \star a_2 \star \cdots \star a_k \in H$.

Exemple - Groupes engendré par p dans $\mathbb{Z}$.
On considère le groupe $(\mathbb{Z}, +)$. Le groupe $< p >$ contient nécessairement tous les nombres de la forme : $\underbrace{p + p + \cdots + p}_{r \text{ fois}} = rp$, c'est à dire les multiples de $\mathbb{Z}$.
Donc $p\mathbb{Z} \subset < p >$.
Par ailleurs $p\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Donc $< p >= p\mathbb{Z}$.

Exercice
Quel est le sous-groupe engendré par $\{p, q\}$ dans $(\mathbb{Z}, +)$?

Correction
On pense qu'il s'agit du sous-groupe engendré par le PGCD de p et q, dont on a déjà un nom : $(p \wedge q)\mathbb{Z}$.
On sait déjà que c'est un groupe.
Comme $p \wedge q$ est un diviseur de p et de q, $p \in (p \wedge q)\mathbb{Z}$ et $q \in (p \wedge q)\mathbb{Z}$. Donc $\{p, q\} \subset (p \wedge q)\mathbb{Z}$.
Le groupe $< \{p, q\} >$ contient tous les nombres de la forme $up + vq$ où $u, v \in \mathbb{Z}$.
D'après le théorème de Bézout, il contient donc $p \wedge q$, le PGCD de p et q.
Comme il s'agit d'un groupe, il contient également tous les multiples de $p \wedge q$, donc tout $(p \wedge q)\mathbb{Z}$.
Donc $(p \wedge q)\mathbb{Z} \subset < \{p, q\} >$.
Et comme $< p \wedge q >$ est le plus petit sous-groupe contenant $\{p, q\}$: $< p, q > (= < \{p, q\} >) = (p \wedge q)\mathbb{Z}$

Groupe monogène

Définition - Groupe monogène
On dit que G est un groupe monogène, s'il existe $x \in G$ tel que $G = < x >$.
Dans ce cas $G = \{x^k, k \in \mathbb{Z}\}$.

Savoir faire - Etudier des groupes monogènes

Si G est un groupe que l'on sait monogène, alors il existe $x \in G$ (référence, que l'on fixe) tel que $G =< x >$.
L'application $\varphi : \mathbb{Z} \to G$, $k \mapsto x^k$ est bien définie, surjective. Elle peut être injective ou non (cas fini).
On transfère ensuite par φ (ou φ^{-1}) l'étude de G, à partir de propriétés de $\mathbb{Z}$.

Exercice
Montrer qu'un groupe monogène est nécessairement abélien

Correction
Soit $(G, \times)$ monogène, donc il existe $x \in G$ tel que $G =< x >$.
Soient $a, b \in G$, alors il existe $n, m \in \mathbb{Z}$ tel que $a = x^n$ et $b = x^m$.
Ainsi $a \times b = x^n \times x^m = x^{n+m} = x^m \times x^n = b \times a$

Exemples à partir de $\mathbb{U}$

L'exercice suivant nous aide à faire le point.

Exercice
On considère le groupe $(\mathbb{U}, \times)$.

1. Soit $z_k = e^{\frac{2i\pi}{k}}$. Que vaut le groupe $< z_k >$?
2. Avec les mêmes notations, que vaut le groupe $< z_r, z_s >$?
3. A-t-on pour tout $n \in \mathbb{N}$, pour tout $z \in \mathbb{U}_n$, $\mathbb{U}_n =< z >$?
   Sinon, à quelle condition sur z, a-t-on : $\mathbb{U}_n =< z >$?
4. Quel est le groupe $\mathbb{U}_n \cap \mathbb{U}_m$?
5. $\mathbb{U}$ est-il monogène ?

Correction

1. $< z_k >$ continent toutes les puissances de z_k, donc tous les nombres complexes z_k^r de $\mathbb{U}_k$.
   Donc $\mathbb{U}_k \subset < z_k >$ et $\mathbb{U}_k$ est un groupe, ainsi $< z_k >= \mathbb{U}_k$.
2. Tous les nombres complexes de la forme $z_r^u \times z_s^v = \exp 2i\pi \frac{us+vr}{sr}$ appartiennent à $< z_r, z_s >$, avec $u, v \in \mathbb{Z}$.
   D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tel que $us + vr = s \wedge r$, puis $sr = (s \wedge r)(s \vee r)$ donc $z_{s \vee r} \in < z_r, z_s >$.
   Et donc $< z_{r \vee s} > \subset < z_r, z_s >$.
   Par ailleurs, $r | (r \vee s)$, donc il existe r' tel que $r \vee s = rr'$ et donc $z_{r \vee s}^{r'} = z_r$ donc $z_r \in < z_{r \vee s} >$.
   De même $z_s \in < z_{r \vee s} >$ et donc $\{z_r, z_s\} \subset < z_{r \vee s} >$, donc $< z_r, z_s > \subset < z_{r \vee s} >$.
   Par double inclusion $< z_r, z_s >=< z_{r \vee s} >$.
3. Non, clairement. En effet, pour tout $n \in \mathbb{N}$, $1 \in \mathbb{U}_n$ et $< 1 >= \{1\} \neq \mathbb{U}_n$.
   Lorsque $z \in \mathbb{U}_n$ vérifie $< z >= \mathbb{U}_n$, on dit que z est une racine *primitive* première de l'unité.
   On sait que $z \in \mathbb{U}_n$ signifie qu'il existe $k \in [\![0, n-1]\!]$ tel que $z = \exp \frac{2ik\pi}{n}$.
   Si $k \wedge n = 1$. Alors d'après Bézout (toujours) : il existe $u, v \in \mathbb{Z}$ tel que $uk + vn = 1$
   et donc $z^u = \exp \frac{2iuk\pi}{n} \times \exp 2iv\pi = \exp \frac{2i(uk+vn)\pi}{n} = z_n$.
   Donc $z_n \subset < z >$ et donc $\mathbb{U}_n =< z_n > \subset < z >$.
   Comme $z \in \mathbb{U}_n$. On a donc $< z > \subset < \mathbb{U}_n >= \mathbb{U}_n$.
   Par double inclusion $\mathbb{U}_n =< z >$.
   Réciproquement, si $\mathbb{U}_n =< z >$, alors il existe $u \in \mathbb{Z}$ tel que $z^u = z_n (\in \mathbb{U})$
   et donc $uk \equiv 1 [n]$ i.e. $k \wedge n = 1$ (réciproque de Bézout).
4. Soit $z \in \mathbb{U}_{n \wedge m}$, alors $z^{n \wedge m} = 1$. Et comme $n \wedge m | n$,
   on a donc $z^n = (z^{n \wedge m})^{n/(n \wedge m)} = 1$ donc $z \in \mathbb{U}_n$. De même $z \in \mathbb{U}_m$.
   Par conséquent : $\mathbb{U}_{n \wedge m} \subset \mathbb{U}_n \cap \mathbb{U}_m$.
   Evidemment, si $z \in \mathbb{U}_n \cap \mathbb{U}_m$, alors pour tout $u, v \in \mathbb{Z}$, $z^{un+vp} = (z^n)^u (z^m)^v = 1$.
   Donc $z^{n \wedge m} = 1$ et $z \in \mathbb{U}_{n \wedge m}$.
   Par double inclusion $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}$
5. Non, sinon $\mathbb{U}$ serait dénombrable.

Pour aller plus loin - De qui parle Felix Klein ?

« Depuis longtemps déjà, il s'occupait à étudier des groupements de racines complexes de l'unité sur la base de sa théorie des racines primitives. Et voilà que ce matin-là (le 30 mars 1796) en se réveillant, il lui apparut clairement qu'à partir de sa théorie, on pouvait construire un polygone à 17 cotés[...]. Cet événement marqua un grand tournant dans sa vie : c'est précisément ce jour-là qu'il décida d'abandonner les langues pour se consacrer exclusivement aux mathématiques ». Les mathématiques y ont beaucoup gagné !

4.4. Démontage d'un groupe

Théorème de Lagrange

Proposition - Relation d'équivalence modulo un sous-groupe
Soit $(G, *)$ un groupe et $H < G$, un sous-groupe de G.
On note $\mathscr{R}_H$, la relation définie sur G par :

$$a \mathscr{R}_H a' \iff a^{-1} * a' \in H$$

Alors $\mathscr{R}_H$ est une relation d'équivalence.

Démonstration
$\mathscr{R}_H$ est :
- réflexive : pour tout $a \in G$, $a^{-1}a = e \in H$. Donc $\forall\ a \in G$, $a \mathscr{R}_H a$.
- symétrique : si $a \mathscr{R}_H a'$, alors $a^{-1} * a' \in H$.
  Mais H est un groupe donc $(a^{-1}a')^{-1} = a'^{-1}a \in H$ donc $a' \mathscr{R}_H a$
- transitive : si $a \mathscr{R}_H a'$ et $a' \mathscr{R}_H a''$, alors $a^{-1} * a', a'^{-1} * a'' \in H$.
  Mais H est un groupe donc $(a^{-1} * a') * (a'^{-1} * a'' = a^{-1} * a'' \in H$ donc $a \mathscr{R}_H a''$

□

Remarque - Lien relation d'équivalence et sous-groupe

On voit sur cette démonstration le lien très étroit qui unit les caractéristiques d'un sous-groupe et les propriétés d'une relation d'équivalence. Plus précisément : l'élément neutre à la réflexivité, l'inversibilité à la symétrie et la stabilité à la transitivité
Quand on a une relation d'équivalence, on a naturellement une décomposition en réunion disjointe

Proposition - Décomposition de G
Soit H un sous-groupe de G.
On note $S := S_{\frac{G}{\mathscr{R}_H}}$ un système de représentant des classes d'équivalences de $\mathscr{R}_H$.
Alors $G = \uplus_{a \in S} \overline{a}$, la réunion disjointes des classes de a.
$\overline{a}$ n'est pas un groupe, mais il est en bijection avec H.
Par la suite, on notera aH, cet ensemble. On a donc $aH = a'H \Leftrightarrow a \mathscr{R}_H a' \Leftrightarrow a^{-1}a' \in H$
Le produit cartésien $H \times S$ et le groupe G sont en bijection (c'est la décomposition).

Démonstration
La première partie de la proposition a été donnée dans le cours sur les classes d'équivalence.
Soit $\varphi : H \mapsto \overline{a}$, $x \mapsto ax$.
Montrons que φ est bien définie à valeurs dans $\overline{a}$.
On a, en effet, $a \mathscr{R}_H ax = \varphi(x)$, car $a^{-1} * ax = x \in H$.
φ est bijective car elle admet une application réciproque $\varphi^{-1} : b (\in \overline{a}) \mapsto a^{-1}b (\in H)$.
On a bien $\varphi^{-1}(b) = a^{-1}b \in H$, car $b \in \overline{a}$, donc $a \mathscr{R}_H b$, i.e. $a^{-1}b \in H$.
Pour l'équivalence.
On considère $g \in G$, alors il existe un unique $a \in S$ tel que $\overline{g} = \overline{a}$,
i.e. il existe un unique $h \in H$ tel que $g = ah$.
On a alors une bijection naturelle $(a, h) \mapsto g = ah$
dont la réciproque est donnée sur la ligne précédente. □

En fait, les ensembles $\overline{a}$ sont comme des sous-groupes affines de G...

Proposition - Théorème de Lagrange
Si H un sous-groupe de G, groupe de cardinal fini, alors $\text{card} H | \text{card} G$.

Démonstration
$G = \uplus_{a \in S} \overline{a}$. La réunion est disjointe, donc en terme de cardinaux :

$$\text{card}(G) = \sum_{a \in S} \text{card}(aH) = \sum_{a \in S} \text{card}(H) = \text{card}(H) \times \sum_{a \in S} 1 = \text{card}(H) \times \text{card}(S)$$

où on a exploité que H et aH sont en bijection, donc ont même cardinaux.
On aurait pu aussi exploiter le fait que $\text{card}(G) = \text{card}(H \times S) = \text{card} H \times \text{card}(S)$. □

Sous-groupe distingué

Analyse - S comme un groupe?
On a dit et redit que sauf pour $\overline{a}=H$ (exemple : $a=e$, mais pas uniquement), $\overline{a}=aH$ n'est pas un groupe et donc φ n'est pas un morphisme de groupe (cf partie suivante).
Néanmoins, on peut se demander si S, l'ensemble des représentants ne pourrait pas être un groupe. Sous quelles condition?
Pour que cela ait du sens, on devrait pouvoir créer l'opération $\overline{*}$ sur S de la façon suivante :

$$aH\overline{*}bH=(a*b)H$$

Dans ce cas, il faudrait que pour tout $a'=ax\in aH$ (avec $x\in H$) et $b'=by\in bH$ (avec $y\in H$), on ait : $a'*b'\in(a*b)H$, c'est-à-dire $axby\in(ab)H$.
Il suffit alors que pour tout $x\in H$, $xb\in bH$, ce que l'on note $Hb\subset bH\Leftrightarrow Hb=bH$.
Cette condition est également nécessaire : car elle doit être vérifiée pour tout $a\in G$ et donc $a=e$ (et $y=e$) aussi : $xb\in bH$.

Définition - Sous-groupe distingué
On dit que $H<G$ est un sous-groupe distingué (ou normal) de G si

$$\forall\ a\in G,\forall\ x\in H,\qquad a^{-1}xa\in H$$

On peut retenir que pour tout $a\in G$, $aH=Ha$.
On note alors $H\triangleleft G$

Démonstration
Montrons que : $\forall\ a\in G, x\in H, a^{-1}xa\in H$ correspond bien à ce que l'on souhaite.
Supposons donc que $\forall\ a\in G, x\in H, a^{-1}xa\in H$.
Soit $y\in aH$. Alors $\exists\ x\in H$ tel que $y=ax$.
Alors $ya^{-1}=axa^{-1}\in H$, donc $y=\underbrace{(axa^{-1})}_{z\in H}a\in Ha$. Ainsi $aH\subset Ha$.
Soit $y\in Ha$. Alors $\exists\ x\in H$ tel que $y=xa$.
Alors $a^{-1}y=a^{-1}xa\in H$, donc $y=a\underbrace{(a^{-1}xa)}_{z\in H}\in aH$. Ainsi $Ha\subset aH$.
Supposons que pour tout $a\in G$, $aH=Ha$.
Soit $a\in G$, $x\in H$. Alors $xa\in Ha=aH$, donc $\exists\ z\in H$ tel que $xa=az$ et donc $z=a^{-1}xa\in H$.
□

Proposition - Groupe quotient
Soit $(G,*)$ un groupe.
Si $H\triangleleft G$ est un sous-groupe distingué de G, alors $S=\dfrac{G}{\mathscr{R}_H}$, souvent noté $\dfrac{G}{H}$ est un groupe pour la loi $\overline{*}$ définie par $aH\overline{*}bH=(a*b)H$.

Exercice
A démontrer ! (Attention, ce n'est pas un sous-groupe. Il faut donc tout redémontrer à commencer par la bonne définition de la loi...)

Correction

Exemple - Groupe trivial
$H=\{e\}$ est un sous-groupe distingué. Mais cela n'a pas beaucoup d'intérêt.
Sauf si on l'associe avec la réciproque d'un morphisme (cf partie suivante).

Exemple - G abélien
Si G est abélien, alors tout sous-groupe H est distingué.
En effet, pour tout $a\in G$, $x\in H$: $a^{-1}xa=a^{-1}ax=x\in H$.
Ainsi, pour tout $n\in\mathbb{N}$, $n\mathbb{Z}\triangleleft\mathbb{Z}$ et donc $(\dfrac{\mathbb{Z}}{n\mathbb{Z}},\overline{+})$ est un groupe.

Pour aller plus loin - Théorie de résolution par radicaux
Comme écrit wikipédia : « Pour n supérieur ou égal à 5, le groupe alterné sur n éléments $\mathscr{A}_n$ est simple. Ce résultat est à la base de la théorie de la résolution par radicaux. »

Définition - Groupe simple
On dit qu'un groupe est simple lorsqu'il ne possède pas de sous-groupe distingué autre que $\{e\}$ et lui-même

Cela ne vous rappelle pas une autre définition?
Exercice
Soit G un groupe de cardinal p, premier.
Montrer que G est simple

Correction
Soit $H\triangleleft G$. Alors $\mathrm{card}H|\mathrm{card}G$, donc $\mathrm{card}H\in\{1,p\}$, i.e. $H=\{e\}$ ou $H=G$ respectivement.
Donc G est nécessairement simple

5. Morphismes de groupes

5.1. Définition et propriété immédiate

Soient $(G,\star)$ et $(G',\top)$ deux groupes.

Définition - Morphisme de groupes
Une application f de G dans G' vérifiant :
$\forall(x,y)\in G^2,\ f(x\star y)=f(x)\top f(y)$.
est appelé morphisme (de groupes) de $(G,\star)$ sur $(G',\top)$.

Proposition - Conservation du noyau
Soit $f:G\to G'$ un morphisme de groupes. Alors $f(e_G)=e_{G'}$.

Démonstration
Soient $x\in G$,

$$f(x)\top e_{G'}=f(x)=f(x\star e_G)=f(x)\top f(e_G)$$

Puis par régularité : $e_{G'}=e_G$ □

Proposition - Image de l'inverse
Soit $f:G\to G'$ un morphisme de groupes.
Alors pour tout $x\in G$, $f(x^{-1})=\left(f(x)\right)^{-1}$

Démonstration
Soient $x\in G$,

$$f(x^{-1})\top f(x)=f(x^{-1}\star x)=f(e_G)=e_{G'}=f(x)^{-1}\top f(x)$$

Donc par régularité : $f(x^{-1})=\left(f(x)\right)^{-1}$ □

Exemple - exp
Le morphisme du groupe $(\mathbb{R},+)$ vers $(\mathbb{R}^*,\times)$ est l'application :

$$\forall\ a,b\in\mathbb{R},\qquad f(a+b)=f(a)\times f(b)$$

On a nécessairement $f(0)=1$.
On montre :

1. par récurrence : $\forall\ n\in\mathbb{N}$, $f(n)=\left(f(1)\right)^n$
2. par passage au symétrique : $\forall\ n\in\mathbb{Z}$, $f(n)=\left(f(1)\right)^n$
3. pour $\mathbb{Q}$: pour tout $m\in\mathbb{Z}$, $n\in\mathbb{N}^*$,
   $(f(1))^m=f(m)=f(n\times\frac{m}{n})=f(\frac{m}{n}+\cdots+\frac{m}{n})=(f(\frac{m}{n}))^n$.
   donc pour tout $\forall\ q\in\mathbb{Q}$, $f(q)=\left(f(1)\right)^q$
4. si f est continue ou croissante, alors on peut passer à la limite $f:x\mapsto a^x$ avec $a=f(1)$

5.2. Image et noyau d'un morphisme

Proposition - Sous-groupe
Soit $f : G \to G'$ un morphisme de groupes.
Soit A un sous-groupe de G, alors $f(A)$ est un sous-groupe de G'.
Soit B un sous-groupe de G', alors $f^{-1}(B)$ est un sous-groupe de G.
En particulier :
- $\text{Im}\, f = f(G) = \{f(x), x \in G\}$ est un sous-groupe de G', appelé image de G
- $\text{Ker}\, f = f^{-1}(e_{G'}) = \{x \in G \mid f(x) = e_{G'}\}$ est un sous-groupe de G, appelé noyau de f.

Exemple - $\mathbb{Z} \to \mathbb{U}_n$
$f : (\mathbb{Z}, +) \to (\mathbb{U}_n, \times)$, $k \mapsto e^{ki\pi/n}$ est un morphisme de groupe.
Son noyau est $n\mathbb{Z}$.

Démonstration
$f(A) \subset G'$, non vide ($e_G \in A$, donc $e_{G'} = f(e_G) \in f(A)$).
Soient $y_1, y_2 \in G'$, il existe $x_1, x_2 \in A$ tel que $f(x_1) = y_1$ et $f(x_2) = y_2$.
$y_1 \top y_2^{-1} = f(x_1) \top f(x_2)^{-1} = f(x_1) \top f(x_2^{-1}) = f(x_1 \star x_2^{-1}) \in f(A)$ Donc $f(A)$ est bien un sous-groupe de G'.
$f^{-1}(B) \subset G$, non vide ($e_{G'} \in B$, donc $e_G \in f^{-1}(B)$ car $f(e_G) = e_{G'}$).
Soient $x_1, x_2 \in G'$, alors $f(x_1) \in B$ et $f(x_2) \in B$. Ainsi : $f(x_1 \star x_2^{-1}) = f(x_1) \top f(x_2)^{-1} \in B$ Donc $f^{-1}(A)$ est bien un sous-groupe de G. □

Exercice
Montrer que $f : G \to G'$ morphisme de groupes est :
- surjective ssi $\text{Im}\, f = G'$
- injective ssi $\text{Ker}\, f = \{e_G\}$

Correction
La première équivalence est évidente, simple écriture.
Pour la seconde,
on a si f injective,
pour tout $x \in \text{Ker}\, f$, $f(x) = e_{G'} = f(e_g)$, donc $x = e_g$ et $\text{Ker}\, f \subset \{e_G\}$.
L'inclusion réciproque est triviale, donc $\text{Ker}\, f = \{e_G\}$
Réciproquement, si $\text{Ker}\, f = \{e_G\}$.
Si $f(x) = f(x')$, alors $e_{G'} = f(x) \top f(x')^{-1} = f(x \star x'^{-1})$, donc $x \star x'^{-1} \in \text{Ker}\, f = \{e_G\}$.
Ainsi $x \star x'^{-1} = e_G$, i.e. $x = x'$. Et f est injective

Exemple - $\text{Ker}\, f$ **est un sous-groupe distingué**
On sait que $\text{Ker}\, f < G$.
Soit $a \in G$ et $x \in \text{Ker}\, f$,
$$f(a^{-1}xa) = f(a^{-1}) \underbrace{f(x)}_{=e_{G'}} f(a) = f(a)^{-1} f(a) = f(a^{-1}a) = f(e) = e_{G'}$$
Donc $a^{-1}xa \in \text{Ker}\, f$.

5.3. Premier théorème d'isomorphisme

Théorème - Premier théorème
Soient G et G' deux groupes et $f : G \to G'$, un morphisme de groupes.
Alors f induit un isomorphisme de groupes : $\hat{f} : G/\text{Ker}\, f \hookrightarrow\!\!\!\rightarrow \text{Im}\, f$.

Démonstration
$\text{Ker}\, f$ est un sous-groupe distingué de G.
$G/\text{Ker}\, f$ est la notation du groupe quotient $\frac{G}{\text{Ker}\, f}$ pour la relation d'équivalence $a\mathscr{R}b$ ssi $ab^{-1} \in \text{Ker}\, f$ i.e $f(a) = f(b)$.
Soit donc $\overline{a}$, un élément de $G/\text{Ker}\, f$ (c'est la classe de a) et $\hat{f} : \overline{a} \mapsto f(a)$.
Il faut donc commencer par vérifier que cette définition de $\hat{f}$ a bien un sens.
Compte-tenu de la définition de $\mathscr{R}$, c'est évident que $\hat{f}$ est bien définie.
$\hat{f}$ est clairement bijective, puisque $\hat{f}^{-1}$ est l'application qui $z \in \text{Im}\, f \to \overline{z}$. □

Pour aller plus loin - Une deuxième, un troisième?
Le deuxième énonce :
si $N \lhd G$ et $H < G$, alors $N \cap H \lhd H$ et $H/(N \cap H) \hookrightarrow HN/N$.
Le troisième énonce :
si $N, M \lhd G$ tels que $M < N$, alors $N/M \lhd G/M$ et $(G/M)/(N/M) \hookrightarrow G/N$.

Remarque - Notation symbolique ou formelle
On retrouve dans la littérature (mathématique) le diagramme suivant que l'on qualifie de commutatif :
$$G \twoheadrightarrow \frac{G}{\text{Ker}\, f} \hookrightarrow\!\!\!\rightarrow \text{Im}\, f \hookrightarrow G'$$

Pour aller plus loin - Dans les espaces vectoriels...
Ce théorème est à comparer avec le lemme préparatoire qui conduit au si fondamental théorème du rang dans les espaces vectoriels de dimension finie.
Ainsi si f est une application linéaire de E sur F, avec E de dimension finie.
Alors $\dim E = \dim \text{Im}\, f + \dim \text{Ker}\, f$ car $f_{|H} : H \to \text{Im}\, f$ est une application bijective (où H tel que $E = H \oplus \text{Ker}\, f$.

6. Bilan

Synthèse

- ⇝ La notion de groupe est la brique élémentaire des théories mathématique. C'est une notion primitive : un ensemble et une loi interne associative, unifère et dont tous les éléments sont symétriques. Cette structure est naturellement comparable à une relation d'équivalence : associativité↔ transitivité, élément neutre↔reflexivité et inversion↔symétrie.
- ⇝ On peut réduire des (sous-)groupes par intersection, ou bien générer des (sous-)groupes par engendrement de parties. Ces deux méthodes sont très classiques en algèbre ou en topologie.
- ⇝ On décompose ensuite les groupes en produit de sous-groupes à condition que le premier de ce produit soit un sous-groupe distingué. Finalement les sous-groupes distingués (ou normaux) sont comme des nombres premiers.
- ⇝ On peut aussi déplacer des structures avec des morphismes de groupes, voire comparer des groupes (est-ce que ces morphismes sont bijectives (isomorphisme) ?)

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Démontrer que H est un (sous-)groupe
- Savoir-faire - Comment trouver le sous-groupe engendré par une partie A?
- Savoir-faire - Etudier des groupes monogènes

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$H < G$	H est un sous-groupe de G	$e_G \in H$ et $\forall\, x, y \in H, xy^{-1} \in H$	Parfois noté : $H \lhd G$
$H \lhd G$	H est sous-groupe distingué de G	$H \lhd G$ et $\forall\, x \in G, xHx^{-1} \subset H$	Parfois noté : $H \lhd \mid G$
$\frac{G}{H}$	Ensemble des classes d'équivalence sur G pour la relation d'équivalence $a\mathscr{R}_H b \iff ab^{-1} \in H$	Les classes d'équivalence sont chacune en bijection avec H.	On en déduit le théorème de Lagrange : $\text{card}H \mid \text{card}G$

Retour sur les problèmes

59. Groupes, anneaux, corps...
60. Pas facile. Il faut plonger dans un cours sur le corps de Galois. Lorsqu'on aura fait le cours sur le groupe symétrique (= groupe des permutations d'un ensemble à n éléments), cela sera peut-être plus simple... En gros une formule de résolution, c'est une décomposition du groupe des permutations (qui agit sur l'ensemble des racines) en sous-groupe distingué × groupe quotient. Si une telle décomposition n'est pas possible (le groupe est simple), nous sommes bloqués. Or pour les équations de degré 5, on regarde S_5 (cf second semestre), il se décompose en $A_5 \, t \times \{-1, 1\}$, mais A_5 ne se décompose pas plus...
61. La composition conserve nécessairement la distance.
La question fondamentale est dans l'existence de la transformation

inverse (bijectivité de φ).
A noter qu'il s'agit d'un groupe continue (ou de LIE) par opposition aux groupes discrets (et souvent finis comme S_n).

Chapitre 14

Construction d'ensembles numériques : des entiers à la droite réelle

Résumé -

Ce chapitre est comme une application du chapitre e sur les relations pour donner une assise mathématique satisfaisante aux ensembles bien connus des élèves car largement utilisés. Dans l'histoire, ces constructions se sont passés à la fin du XIX siècle. Cela faisait des siècles (voire des millénaires) que certains de ces ensembles étaient exploités…

Il n'y a au fond qu'un seul problème : comment donner du sens aux ensembles : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$?

Quelques vidéos sur internet :

- *Yvan Monka - Ils sont fous, ces nombres ! - Classification - https ://www.youtube.com/watch ?v=kL-eMNZiARM*
- *Exo7Maths - Nombres réels - https ://www.youtube.com/watch ?v=NCWWVven9Cs*
- *Science4all - La diagonale dévastatrice de Cantor - https ://www.youtube.com/watch ?v=xqSKawORrPo*

Sommaire

1. Problèmes 276
2. Nombres algébriques 277
2.1. Nombres entiers 277
2.2. Nombres rationnels 279
2.3. Nombres algébriques 280
3. Propriétés de $\mathbb{R}$ 280
3.1. Principe de construction de $\mathbb{R}$ 280
3.2. Fonctions classiques associées à $\mathbb{R}$ 281
4. Parties de $\mathbb{R}$ et topologie 283
4.1. Bornes supérieure et inférieure 283
4.2. Densité de $\mathbb{D}$ ou $\mathbb{Q}$ dans $\mathbb{R}$ 286
5. Bilan 287

1. Problèmes

Problème 63 - Construction des entiers naturels

Au milieu du XIXième siècle, les mathématiciens se sont rendus compte que leurs sens leur faisaient défaut lorsqu'ils ont découvert les géométrie non euclidienne. Il a fallu tout reconstruire sur des bases très solides.
Comment construire l'ensemble des entiers sans équivoque !

Problème 64 - Construction des entiers relatifs, des rationnels

Une fois que les entiers $1, 2, 3\ldots$ sont définis, ainsi que le 0, comment définir proprement les nombres entiers négatifs.
A savoir que dans l'histoire, les fractions sont apparues bien avant les nombres négatifs !
Nous verrons en algèbre générale qu'il est souvent préférable d'avoir un corps plutôt qu'un anneau (tous les éléments sont inversibles).
Comment définir alors proprement l'ensemble des fractions $\frac{a}{b}$ et justifier l'égalité $\frac{a}{b} = \frac{c}{d}$, alors que $a \neq c$ et $b \neq d$?
Une fois que la construction est acquise (avec les lois + et ×), comment généraliser sur $\mathbb{Q}$ la relation d'ordre $\leqslant$ définie sur $\mathbb{Z}$?

Problème 65 - Construction des réels

Pour le familier de la calculatrice (ou de Python), les nombres réels sont obtenus en écrivant les nombres décimalement quitte à ce que cette écriture soit infini. Cela marche bien ; la preuve : le sur-développement des ordinateurs et autres objets numériques.
Comment faire cette construction et surtout comment gérer la problématique $1 - 0,999\ldots9\cdots = 0$, donc la non unicité d'écriture de certains nombres réels.
Là aussi : comment définir la relation d'ordre ?

Problème 66 - Construction des réels

Une autre possibilité : exploiter le principe de la dichotomie. Cela rappelle la méthode des coupures de DEDEKIND, en séance de cours-TP.
Pouvons-nous dès maintenant anticiper cette méthode ?

Problème 67 - Densité de $\mathbb{Q}$ dans $\mathbb{R}$

La construction de $\mathbb{R}$ conduit à voir tous les éléments de $\mathbb{R}$ comme limite d'éléments de $\mathbb{Q}$.
On dit que $\mathbb{Q}$ est dense dans $\mathbb{R}$ (associé à la continuité, c'est une propriété très forte !).
Et pourtant, les cardinaux de $\mathbb{Q}$ et $\mathbb{R}$ sont-ils comparables ? Existe-t-il une bijection de $\mathbb{N}$ sur $\mathbb{Q}$? de $\mathbb{Q}$ sur $\mathbb{R}$?

2. Nombres algébriques

2.1. Nombres entiers

Nombres entiers naturels

On commence par admettre la construction de l'ensemble des entiers naturels $\mathbb{N}$.

Heuristique - Nombres entiers naturels

La construction suivante est dûe à Péano. Soit E un ensemble non vide, possédant un élément de référence et dont tous les éléments ont un unique successeur (différent de l'élément de référence).
Cet élément de référence se note 0 (ou 1, selon). Puis on définit l'addition +1 comme le passage d'un nombre à son successeur.
On a ainsi les bases pour un raisonnement par récurrence et l'ensemble des entiers.
Ce qui suit est en fait assez naturel, même si cela peut paraître un peu compliqué la première fois qu'on le voit…

Théorème - Construction de PÉANO

Il existe un ensemble $\mathbb{N}$ non vide, munie d'une loi s (comme successeur) telle que :
- $\mathbb{N}$ étant non vide, il admet une élément premier noté 0.
- Pour tout élément $a \in \mathbb{N}$, il existe $b \in \mathbb{N}^*$ tel que $b = s(a)$.
- s est injective ($s(a) = s(a') \Rightarrow a = a'$)

Remarque - Addition +1

$s(a)$ correspond à la classique addition +1.
L'habitude consiste à associer à l'élément $s \circ s \circ \cdots s(0)$, le nombre n égal au nombre de fois que s est utilisé

Proposition - Opérations sur $\mathbb{N}$

On définit l'addition sur $\mathbb{N}$ par : $a + b = s^a(0) + s^b(0) = s^{a+b}(0)$.
On a $a + b = b + a$.
La multiplication est alors la répétition de l'addition : $a \times b = \underbrace{a + a + \cdots + a}_{b \text{ fois}}$
On a $a \times b = b \times a$.

Proposition - Relation d'ordre

$\mathbb{N}$ est naturellement ordonné (récursivement) :
$\forall\, a, b \in \mathbb{N}^*,\ a \leqslant b \iff s^{-1}(a) \leqslant s^{-1}(b)$.
L'ordre est total.

Et il existe un algorithme, qui termine, permettant de connaître le plus petit entre a et b :

Informatique - Ordre

```
def petit(a,b):
    c,d=a,b
    while c>0 and d>0 :
        c,d=c-1,d-1
    if c==0:
        return(a)
    else :
        return(b)
```


Nombres entiers naturels

Ensuite on construit l'ensemble des entiers relatifs. On propose ici un exercice.

Heuristique - Problématique

La problématique : l'addition à trou (ou recherche d'une opération réciproque) n'est qu'à moitié possible. En effet, elle dépend de la relation d'ordre entre les nombres soustraits.
Il faut donc créer un premier ensemble, afin que toute soustraction de nombres entiers soit possible.
Mais certaines soustractions peuvent conduire à un « même » résultat

Exercice
Sur $\mathbb{N}^2$,

1. Montrer que $\sim_1$ définie par :
$$(a,b) \sim_1 (c,d) \iff a + d = c + b$$
est une relation d'équivalence.
2. Montrer que tout couple (a,b) est dans la classe d'un couple $(0,d)$ ou $(d,0)$ selon que $a \leqslant b$ ou $a \geqslant b$
3. En déduire la construction de $\mathbb{Z}$ comme équivalent à l'ensemble $\dfrac{\mathbb{N}^2}{\sim_1}$

Correction

1. Elle est bien réflexive, symétrique et transitive (déjà démontré)
2. Si $a \leqslant b$, alors $b - a \geqslant 0$ et donc $(a,b) \sim_1 (0, b-a)$ car $a + (b-a) = b + 0$.
Si $a \geqslant b$, alors $a - b \geqslant 0$ et donc $(a,b) \sim_1 (a-b, 0)$ car $a = b + (a-b)$.
3. Aucun des couples $(0,c)$ ou $(d,0)$ n'est en relation avec un autre si les nombres c ou d sont différents.
On a donc trouvé un représentant de chacune des classes d'équivalences de $\mathbb{N}^2$ pour la relation $\sim_1$.
On peut noter $+c = (c,0)$ et $-c = (0,c)$. En on construit ainsi $\mathbb{Z}$.

Exemple - Le nombre -2

Selon cette construction, le nombre habituellement noté -2 correspond à la classe d'équivalence des nombres $(0,2)$, $(1,3)$,… $(n, n+2)$…
Et le nombre +3 ?

Proposition - Opération sur $\mathbb{Z}$

L'ensemble $\mathbb{Z}$ est l'ensemble $\dfrac{\mathbb{N}^2}{\sim_1}$ (des classes d'équivalence sur $\mathbb{N}^2$ de la loi $\sim_1$).
On définit alors la relation d'ordre $\leqslant_{\mathbb{Z}}$ par :
$$\overline{(a,b)} \leqslant_{\mathbb{Z}} \overline{(c,d)} \iff a + d \leqslant_{\mathbb{N}} c + b$$
L'addition est alors simplement : $\overline{(a,b)} +_{\mathbb{Z}} \overline{(c,d)} = \overline{(a +_{\mathbb{N}} c, b +_{\mathbb{N}} d)}$
La multiplication est plus compliquée :
$\overline{(a,b)} \times_{\mathbb{Z}} \overline{(c,d)} = \overline{(a \times_{\mathbb{N}} c +_{\mathbb{N}} b \times_{\mathbb{N}} d, b \times_{\mathbb{N}} c +_{\mathbb{N}} a \times_{\mathbb{N}} d)}$

Remarque - La difficulté : l'indépendance au représentant

Il faut bien vérifier que chacune de ces définitions est indépendantes du représentant de la classe d'équivalence.
Ainsi : si $\overline{(a,b)} = \overline{(a',b')}$ et $\overline{(c,d)} + \overline{(c',d')}$,
alors $(a+c) + (b'+d') = (a+b') + (c+d') = (a'+b) + (c'+d) = (a'+c') + (b+d)$.
donc on a bien : $(a+c, b+d) \sim_1 (a'+c', b'+d')$.
Ainsi la définition de $+_{\mathbb{Z}}$ est bien indépendante des représentants choisis.

Exemple - Multiplication

Vérifions sur un exemple que la multiplication donne le résultat attendu :

$$-3 \times 4 = \overline{(1,4)} \times \overline{(6,2)} = \overline{(1\times 6+4\times 2, 1\times 2+4\times 6)} = \overline{(14,26)} = -12$$

Démonstration

Il s'agit bien d'une relation d'ordre. Il faudrait montrer aussi qu'elle est indépendante des représentants choisis.
C'est l'opération d'ordre naturelle associée à une relation d'équivalence.

- Reflexive : $\overline{(a,b)} \leqslant_{\mathbb{Z}} \overline{(a,b)}$ car $a+b \leqslant_{\mathbb{N}} a+b$.
- Antisymétrique : $\overline{(a,b)} \leqslant_{\mathbb{Z}} \overline{(c,d)}$ et $\overline{(c,d)} \leqslant_{\mathbb{Z}} \overline{(a,b)}$ alors $a+d \leqslant_{\mathbb{N}} c+b$ et $c+b \leqslant_{\mathbb{N}} a+d$, donc $a+d=c+d$, donc $\overline{(a,b)} \sim_1 \overline{(c,d)}$.
- Transitive : $\overline{(a,b)} \leqslant_{\mathbb{Z}} \overline{(c,d)}$ et $\overline{(c,d)} \leqslant_{\mathbb{Z}} \overline{(e,f)}$ alors $a+d \leqslant_{\mathbb{N}} c+b$ et $c+f \leqslant_{\mathbb{N}} e+d$.
  Donc, par transitivité de $\leqslant_{\mathbb{N}}$: $a+d+f \leqslant_{\mathbb{N}} c+b+f = c+f+b \leqslant e+d+b$,
  donc avec s^{-d} : $a+f \leqslant_{\mathbb{N}} e+b$.
  Ainsi $\overline{(a,b)} \leqslant_{\mathbb{Z}} \overline{(e,f)}$

L'addition et la multiplication sont indépendants des représentants choisis.
□

Exercice
Montrer que l'ordre est total

Correction
L'ordre est total sur $\mathbb{N}$. Soient $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$.
Alors on a ou bien $a+d \leqslant_{\mathbb{N}} b+c$ ou bien $b+c \leqslant_{\mathbb{N}} a+d$.
Donc l'ordre $\leqslant_{\mathbb{Z}}$ est bien total

2.2. Nombres rationnels

La construction de $\mathbb{Q}$ est en tout point équivalente à la construction de $\mathbb{Z}$, mais pour un problème lié à la multiplication (et donc division) au lieu de l'addition (et donc la multiplication).

Exercice
Sur $\mathbb{Z}\times\mathbb{N}^*$,

1. Montrer que $\sim_2$ définie par :
$$(a,b) \sim_2 (c,d) \iff a \times_{\mathbb{Z}} d = c \times_{\mathbb{Z}} b$$
est une relation d'équivalence.
2. Montrer la construction de $\mathbb{Q}$ comme équivalent à l'ensemble $\dfrac{\mathbb{Z}\times\mathbb{N}}{\sim_2}$
3. Montrer que $\leqslant_{\mathbb{Q}}$ définie par $(a,b) \leqslant_{\mathbb{Q}} (c,d)$ ssi $a \times_{\mathbb{Z}} d \leqslant_{\mathbb{Z}} b \times_{\mathbb{Z}} c$ définie bien une relation d'ordre sur $\mathbb{Q}$
4. Comment définir $+_{\mathbb{Q}}$ et $\times_{\mathbb{Q}}$

Correction

1. Elle est bien réflexive, symétrique et transitive (déjà démontré)
2. Supposons que $(a,b) \sim_2 (c,d)$ et $b \geqslant d$ (on ne perd pas de généralité).
   Si il existe $k \in \mathbb{N}$ tel que $d = bk$, alors $abk = cb$ et donc $c = ak$. On notera alors que k divise a et b.
   On appelle couple irréductible un couple $(a,b) \in \mathbb{Z}\times\mathbb{N}$ tel que $\forall\ k \in \mathbb{N},\ k \nmid a$ ou $k \nmid b$.
   Chaque classe d'équivalence a un unique représentant irréductible, que l'on note habituellement $\frac{a}{b}$.
   En on construit ainsi $\mathbb{Q}$.
3. C'est la relation d'ordre qui découle naturellement de la relation d'équivalence sur l'ensemble ordonné $\mathbb{Z}$
4. On peut imaginer : $\overline{(a,b)} +_{\mathbb{Q}} \overline{(c,d)} = \overline{(a\times_{\mathbb{Z}} d +_{\mathbb{Z}} b\times_{\mathbb{Z}} c, b\times_{\mathbb{Z}} d}$ et $\overline{(a,b)} \times_{\mathbb{Q}} \overline{(c,d)} = \overline{(a\times_{\mathbb{Z}} c, b\times_{\mathbb{Z}} d}$

Il faudrait vérifier que $\mathbb{Q}$ est bien un corps (addition, multiplication inversible) compatible avec $\leqslant_Q$. Cela se fait sans grande difficultés…

Pour aller plus loin - Comment définir π simplement?
Nous savons que le périmètre d'une forme régulière est proportionnel à son agrandissement.
Donc pour un cercle, il existe une constante telle que son périmètre est égale au produit de cette constante par le diamètre : $p = C \times d$.
Par définition, on peut appeler pi1 π_1 cette constante.
Ou bien, de même nous savons que la surface d'une forme régulière est proportionnel au carré de son agrandissement.
Donc pour un disque, il existe une constante telle que son aire est égale au produit de cette constante par le carré du rayon : $S = C' \times r^2$. Par définition, on peut appeler π_2 cette constante.
L'enjeu : montrer que $\pi_1 = \pi_2$…

Pour aller plus loin - Généralisation
Ce principe qui permet de passer de l'anneau $\mathbb{Z}$ au corps des fractions $\mathbb{Q}$ est un principe régulièrement repris en mathématiques.
On suivra exactement ce même principe pour décrire le corps des fractions de polynômes $\mathbb{K}(X)$ à partir de l'anneau des polynômes : $\mathbb{K}[X]$

Proposition - Opération sur $\mathbb{Q}$

L'ensemble $\mathbb{Q}$ est l'ensemble $\dfrac{\mathbb{Z}\times\mathbb{N}^*}{\sim_2}$ (des classes d'équivalence sur $\mathbb{Z}\times\mathbb{N}$ de la loi $\sim_2$).
On définit alors la relation d'ordre $\leqslant_{\mathbb{Q}}$ par :

$$\overline{(a,b)} \leqslant_{\mathbb{Q}} \overline{(c,d)} \iff a \times_{\mathbb{Z}} d \leqslant_{\mathbb{Z}} c \times_{\mathbb{Z}} b$$

La multiplication est alors simplement : $\overline{(a,b)} \times_{\mathbb{Q}} \overline{(c,d)} = \overline{(a\times_{\mathbb{Z}} c, b\times_{\mathbb{Q}} d)}$
L'addition est plus compliquée : $\overline{(a,b)} +_{\mathbb{Q}} \overline{(c,d)} = \overline{(a\times_{\mathbb{Z}} d +_{\mathbb{Z}} b\times_{\mathbb{Z}} c, b\times_{\mathbb{Z}} d)}$.
L'ordre est total (démonstration comme pour comme pour $\leqslant_{\mathbb{Z}}$).

2.3. Nombres algébriques

La plupart du temps les nombres se définissent par une phrase, qui elle même se traduit en une équation (polynomiale).
On définit alors :

Définition - Nombre algébrique

Un nombre r est un nombre algébrique si il existe une fonction polynomiale P à coefficients entiers telle que $P(r) = 0$.
Si n est le plus petit degré d'un polynôme vérifiant cette relation, on dit que r est algébrique d'ordre n

Pour aller plus loin - Nombres irrationnels
Ce fut un choc dans l'antiquité lorsqu'on compris que $\sqrt{2}$, qui existe bien (longueur de la diagonale du carré de côté 1), n'est pas une nombre rationnel. Quel type de nombre est-ce?
Si l'on considère des nombres irrationnels (i.e. non rationnels) dans leur singularité, on n'en trouve pas beaucoup, ils sont en effet difficile à définir.

Exemple - Nombres rationnels

Les nombre rationnels sont des nombres algébriques d'ordre 1.
$\frac{p}{q}$ est racine du polynôme $x \mapsto qx - p$.

Exemple - Nombres quadratiques

Les nombre quadratiques sont les nombres algébriques d'ordre 2.
$\sqrt{2}$, racine de x^2-2 ou $\Phi = \dfrac{-1+\sqrt{5}}{2}$, racine de x^2+x-1 sont des nombres quadratiques.
D'une certaine façon, on peut également dire que i est quadratique.
D'autres nombres, toujours « naturels » ne s'expriment pas à partir d'une équation polynomiale à coefficients entiers. C'est le cas de π ou de e.

Définition - Nombre transcendant

Si r n'est pas algébrique, on dit qu'il est transcendant.

Démontrer qu'un nombre donné est transcendant n'est pas une mission évidente.

Pour aller plus loin - Problème ouvert
Est-ce que γ est un nombre transcendant ou algébrique?
Par définition, $\gamma = \lim(\sum_{k=1}^{n} \frac{1}{k} - \ln n)$

Pour aller plus loin - Autre complétion
L'ensemble $\mathbb{R}$ est l'ensemble que l'on obtient naturellement, à partir limites de suites de rationnels (éléments de $\mathbb{Q}$), limites définies à partir de la distance $d(a,b) = |a-b|$ où l'on retrouve la valeur absolue classique.
Mais il existe une (seule) autre façon de faire. On fixe un nombre premier p, et on mesure la distance $d\left(\frac{r_1}{s_1}, \frac{r_2}{s_2}\right) = p^{v_p(s_1)+v_p(s_2)-v_p(r_1s_2-r_2s_1)}$ où pour $a \in \mathbb{Z}$, $v_p(a) = \max\{\alpha \mid p^\alpha | a\}$.
A partir de cette distance, en complétant $\mathbb{Q}$ de limite de suite (de Cauchy) rationnelles, on

3. Propriétés de $\mathbb{R}$

3.1. Principe de construction de $\mathbb{R}$

Heuristique - Un principe : les coupures de Dedekind. Rappel

$\mathbb{Q}$ est un ensemble, relativement naturel, muni d'une relation d'ordre totale $\leqslant$.
$\mathbb{R} \sim \mathscr{C}(\mathbb{Q})$ est l'ensemble des sections ouvertes commençantes sur $\mathbb{Q}$.

$$\mathscr{C}(\mathbb{Q}) = \left\{T \subset \mathbb{Q} \mid \forall\ a \in T, b \leqslant a \Rightarrow b \in T \,\&\, \nexists\, m \in \mathbb{Q} \text{ tel que } T = \{x \in \mathbb{Q} \mid x \leqslant m\}\right\}$$

L'addition est assez naturellement prolongée, ainsi que la relation d'ordre totale.
La multiplication par des positifs est simple, ensuite c'est la règle des signes.
On obtient ensuite quelques résultats topologiques, nouveaux principes de bases ici. Cela est fondamentalement lié au fait qu'il existe des rationnels infiniment proches.

3.2. Fonctions classiques associées à $\mathbb{R}$

Valeur absolue

Définition - Valeur absolue

Pour $x \in \mathbb{R}$, on pose $|x| = \max(x,-x) = \begin{cases} x & \text{si } x \geqslant 0 \\ -x & \text{si } x < 0 \end{cases}$ (plus grand des deux réels x et $-x$).
$d(x,y) = |x-y|$ mesure la distance entre deux réels x et y de la droite réelle.

Définition - Partie positive, partie négative

Pour $x \in \mathbb{R}$, on pose $x^+ = \max(x,0)$ (partie positive du réel x)
et $x^- = \max(-x,0)$ (partie négative du réel x).
Ces deux réels sont POSITIFS.

Exercice
Ecrire $|x|$ en fonction de x^+ et x^-.
Ecrire x^+ en fonction de $|x|$ et de x.

Correction
$|x| = x^+ - x^-$, $x^+ = \frac{|x|+x}{2}$ et $x^- = \frac{|x|-x}{2}$

Proposition - Encadrements à connaître

$|x| \leqslant M \iff -M \leqslant x \leqslant M$

$|x| \geqslant M \iff (x \geqslant M \text{ ou } x \leqslant -M)$

$\forall (x,y) \in \mathbb{R}^2, \quad |xy| = |x|\,|y|$

$\forall (x,y) \in \mathbb{R}^2, \quad \Big||x|-|y|\Big| \leqslant |x+y| \leqslant |x|+|y|$

$\forall (x,y) \in \mathbb{R}^2, d(x,y) \geqslant d(|x|,|y|) \text{ ou } |x-y| \geqslant \Big||x|-|y|\Big|$

Démonstration
Première proposition :
Supposons que $|x| \leqslant M$.
- Si $x \geqslant 0$, $|x| = x$ et donc $|x| \leqslant M \Longrightarrow 0 \leqslant x \leqslant M \Longrightarrow -M \leqslant x \leqslant M$.
- Si $x \leqslant 0$, $|x| = -x$ et donc $|x| \leqslant M \Longrightarrow 0 \leqslant -x \leqslant M \Longrightarrow -M \leqslant x \leqslant 0 \Longrightarrow -M \leqslant x \leqslant M$.

Réciproquement si $-M \leqslant x \leqslant M$,
alors $M \geqslant -x \geqslant -M$, et donc x et $-x$ appartiennent à $[-M,M]$.
Comme $|x|$ est l'un des deux nombres x ou $-x$, alors $|x| \in [-M,M]$.
La seconde proposition est la contraposée de la première proposition.
Troisième proposition, par étude de cas :
- si $x,y \geqslant 0$, alors $|xy| = xy = |x|\,|y|$
- si $x \geqslant 0$, $y \leqslant 0$, alors $|xy| = -xy = x \times (-y) = |x|\,|y|$
- si $x \leqslant 0$, $y \geqslant 0$, alors $|xy| = -xy = (-x) \times y = |x|\,|y|$
- si $x,y \leqslant 0$, alors $|xy| = xy = (-x) \times (-y) = |x|\,|y|$

Quatrième proposition :
$x+y \leqslant |x|+|y|$ et $-(x+y) = -x-y \leqslant |x|+|y|$,
donc $|x+y| = \max(x+y,-x-y) \leqslant |x|+|y|$
On en déduit que $|x| = |(x+y)+(-y)| \leqslant |x+y|+|y|$, donc $|x|-|y| \leqslant |x+y|$.
De même $|y|-|x| \leqslant |x+y|$.
Ainsi : $||x|-|y|| = \max(|x|-|y|, |y|-|x|) \leqslant |x+y|$. Cinquième proposition :
On a simplement : $||x|-|y|| = ||x|-|-y|| \leqslant |x+(-y)| = |x-y|$ □

Partie entière

Proposition - Corps archimédien

Comme $\mathbb{Q}$, $\mathbb{R}$ est archimédien :

$$\forall\ (a,A) \in \in \mathbb{R}_+^* \times \mathbb{R}_+, \qquad \exists\, n \in \mathbb{N}, \text{ tel que } na \geqslant A$$

Avec $a = 1$, cela conduit à la définition :

Définition - Partie entière

Soit $x \in \mathbb{R}$. Il existe un unique $n \in \mathbb{Z}$ vérifiant $n \leqslant x < n+1$.
n s'appelle la partie entière de x, on la note $\lfloor x \rfloor$. On a donc

$$\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1 \quad \text{et} \quad x - 1 < \lfloor x \rfloor \leqslant x.$$

Démonstration
- Si $x \in \mathbb{Z}$, alors $n = x$ fonctionne.
- Si $x > 0$.
  L'ensemble $E_x = \{m \in \mathbb{N} \mid m \leqslant x\}$ est borné par k.
  Tout sous-ensemble non vide et majoré de $\mathbb{N}$ admet une borne supérieur n.
  On a alors $n \leqslant x$ et $n+1 \notin E_x$, donc $n+1 > x$.
- Et si $x < 0$ (avec $x \notin \mathbb{Z}$).
  Alors il existe $n' \in \mathbb{N}$ tel que $n' \leqslant -x < n'+1$.
  Donc $-n' \geqslant x > -n'-1$, et comme $x \notin \mathbb{Z}$, $x \neq -n'$.
  Ainsi avec $n = -n'-1$, on a $n < x < n+1$ ce qui implique $n \leqslant x < n+1$

□

Exercice
Pour tout entier $n \geqslant 1$, montrer :

$$\frac{1}{\sqrt{n+1}} < 2(\sqrt{n+1}-\sqrt{n}) < \frac{1}{\sqrt{n}}$$

En déduire la partie entière du réel $A = 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{10000}}$.

Correction
On peut faire une étude de deux fonctions.
On peut aussi penser à la quantité conjugué :

$$\sqrt{n+1}-\sqrt{n} = \frac{(\sqrt{n+1}-\sqrt{n})(\sqrt{n+1}+\sqrt{n})}{(\sqrt{n+1}+\sqrt{n})} = \frac{n+1-n}{(\sqrt{n+1}+\sqrt{n})} = \frac{1}{(\sqrt{n+1}+\sqrt{n})}$$

Et comme $2\sqrt{n} \leqslant \sqrt{n+1}+\sqrt{n} \leqslant 2\sqrt{n+1}$, on a

$$\frac{1}{\sqrt{n+1}} \leqslant 2\left(\sqrt{n+1}-\sqrt{n}\right) \leqslant \frac{1}{\sqrt{n}}$$

On peut alors sommer ces inégalités, par télescopage :

$$198 = 2(100-1) < 2\left(\sqrt{10001}-\sqrt{1}\right) = \sum_{n=1}^{10000} 2\left(\sqrt{n+1}-\sqrt{n}\right) < \sum_{n=1}^{10000} \frac{1}{\sqrt{n}} = A$$

Et de même :

$$A = 1 + \sum_{n=1}^{9999} \frac{1}{\sqrt{n+1}} < 1 + \sum_{n=1}^{9999} 2\left(\sqrt{n+1}-\sqrt{n}\right) = 1 + 2(100-1) = 199$$

Donc la partie entière de A vaut 198.

Savoir faire - Travailler avec la partie décimale

Fréquemment, on exploite également la fonction partie décimale θ :
$\theta(x) = x - \lfloor x \rfloor$.
On voit que $\theta(x) \in [0,1[$, pour tout $x \in \mathbb{R}$

Exercice
Pour tout réel x, déterminer la limite $\lim\limits_{n\to\infty} \dfrac{\lfloor x \rfloor + \lfloor 2x \rfloor + \cdots + \lfloor nx \rfloor}{n^2}$

Correction
On sait que $kx = \lfloor kx \rfloor + \theta(kx)$, avec $\theta(kx) \in [0,1[$.
Donc $\lfloor x \rfloor + \lfloor 2x \rfloor + \cdots + \lfloor nx \rfloor = x + 2x + \cdots + nx - \theta(x) - \theta(2x) - \ldots \theta(nx) = \frac{n(n+1)}{2}x - \Theta(x,n)$ avec $\Theta(x,n) \in [0,n]$.
Donc

$$\left|\frac{\lfloor x \rfloor + \lfloor 2x \rfloor + \cdots + \lfloor nx \rfloor}{n^2} - \frac{x}{2}\right| = \left|\left(\frac{n^2+n}{2n^2} - \frac{1}{2}\right)x - \frac{\Theta(x)}{n^2}\right| \leqslant |\frac{x}{2n}| + \frac{1}{n}$$

Et donc par encadrement, ceci tend vers 0 et donc la suite a pour limite $\frac{x}{2}$

4. Parties de $\mathbb{R}$ et topologie

4.1. Bornes supérieure et inférieure

On commence par quelques rappels de définitions, mais adaptés ici au cas réel :

Définition - Sous-ensemble majoré, minoré, borné
Soit A un sous-ensemble de $\mathbb{R}$. On dit que :
- A est *majoré* s'il existe un réel M tel que, pour tout x de A, on ait $x \leqslant M$.
  M est alors un majorant de A.
- A est *minoré* s'il existe un réel m tel que, pour tout x de A, on ait $m \leqslant x$.
  m est alors un minorant de A.
- Si A est majoré et minoré, on dit qu'il est borné.

Pour aller plus loin - Rappels
Un majorant M est le plus grand élément de A si et seulement si il appartient également à A.
Un minorant m est le plus petit élément de A si et seulement si il appartient à A

Remarque - Ensemble $\mathbb{N}$
Pour l'ensemble $\mathbb{N}$, on a quelques propriétés :
- Tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.
- Tout sous-ensemble non vide et majoré de $\mathbb{N}$ admet un plus grand élément.

Ce résultat n'est pas vrai si l'on remplace $\mathbb{N}$ par $\mathbb{R}$.
Rappels :

Pour aller plus loin - Récurrence
C'est la première propriété ici (avec un raisonnement par l'absurde) qui permet de montrer l'exactitude du raisonnement par récurrence (et aussi de la descente infinie) et aussi la méthode du variant de boucle en informatique.

Définition - Borne inférieure, borne supérieure
Soit $A \subset \mathbb{R}$.
- Si l'ensemble des majorants de A est non vide
  et si il admet un plus petit élément a,
  alors a est appelé borne supérieure de A, on note $a = \sup A$.
  Formellement :
$$\sup A := \min\{M \in \mathbb{R} \mid \forall\, a \in A, a \leqslant M\} \text{ (si non vide)}$$
- Si l'ensemble des minorants de A est non vide
  et si il admet un plus grand élément b,
  alors b est appelé borne inférieure de A, on note $a = \inf A$.
  Formellement :
$$\inf A := \max\{m \in \mathbb{R} \mid \forall\, a \in A, a \geqslant m\} \text{ (si non vide)}$$

Attention - Borne supérieure
Comme son nom ne l'indique pas, la borne supérieure est par définition le plus **petit** élément d'un certain ensemble (celui des majorants).

L'exercice suivant donne des exemples à toujours bien garder dans un coin de sa tête…
Exercice
Déterminer, s'ils existent, le plus grand élément, le plus petit élément, la borne supérieure, la borne inférieure (sur $\mathbb{R}$) des parties suivantes :
$$A = [0,1], \quad B = [0,1[, \quad C = \left\{\frac{1}{n} \mid n \in \mathbb{N}^*\right\}$$

Correction
- A admet 1 comme plus grand élément, 0 comme plus petit élément.
  Les majorants de A forment l'ensemble $[1,+\infty[$ et donc 1 est également la borne supérieure de A. Les minorants de A forment l'ensemble $]-\infty,0]$ et donc 0 est également la borne inférieure de A.

- B n'admet pas de plus grand élément, mais bien 0 comme plus petit élément.
  Les majorants de B forment l'ensemble $[1,+\infty[$ et donc 1 est également la borne supérieure de B. Les minorants de B forment l'ensemble $]-\infty,0]$ et donc 0 est également la borne inférieure de B.
- C n'admet pas de plus petit élément, mais bien $\frac{1}{1} = 1$ comme plus grand élément.
  Les majorants de C forment l'ensemble $[1,+\infty[$ et donc 1 est également la borne supérieure de C. Les minorants de C forment l'ensemble $]-\infty,0]$ et donc 0 est également la borne inférieure de C.

Proposition - Condition d'existence de la borne supérieure
Soit $A \subset \mathbb{R}$ non vide. On suppose que A possède un plus grand élément a (resp. plus petit élément b).
Alors A possède une borne supérieure (resp. inférieure) et $\sup A = a$ (resp $\inf A = b$).

Savoir faire - Etudier une borne supérieure
En règle générale, pour obtenir une égalité sur la borne supérieure, on exploite deux inégalités :
- $\forall\, a \in A$, $a \leqslant \sup A$ (minoration de $\sup A$)
- $\forall\, M \in \mathbb{R}$ tel que $\forall\, a \in A$, $a \leqslant M$, alors $M \geqslant \sup A$
  (majoration de $\sup A$, par tous les majorants de A)

On a évidemment des relations symétriques pour la borne inférieure…
Exercice
Soient A et B deux parties de $\mathbb{R}$ admettant des bornes supérieures. Montrer que
$$A \subset B \Rightarrow \sup A \leqslant \sup B.$$
Donner un résultat similaires avec les bornes inférieures.

Correction
Il s'agit de majorer $\sup A$.
On exploite donc la deuxième inégalité du savoir-faire (pour $\sup A$). On démontre donc que $\sup B$ est un majorant de A.
Et pour cela, on exploite la première inégalité du savoir-faire (pour $\sup B$) On « remonte » : $\forall\, a \in A$, $a \in B$ car $A \subset B$, donc $a \leqslant \sup B$.
Donc $\sup B$ est un majorant de A et $\sup A$ est le plus petit des majorants.
Ainsi $\sup A \leqslant \sup B$

Les deux propositions suivantes donnent des caractérisations *opératoires* (avec lesquelles travailler dans les démonstrations) et donc un nouveau savoir-faire :

Proposition - Caractérisation de la borne sup.
Soit $A \subset \mathbb{R}$ et $x \in \mathbb{R}$
Alors $x = \sup A$ si et seulement si
$$\begin{cases} \forall\, a \in A, a \leqslant x \\ \forall\, \epsilon > 0, \exists\, a_\epsilon \in A \mid , x - \epsilon < a_\epsilon \end{cases}$$

Proposition - Caractérisation de la borne inf.
Soit $A \subset \mathbb{R}$ et $x \in \mathbb{R}$
Alors $x = \inf A$ si et seulement si
$$\begin{cases} \forall a \in A, x \leqslant a \\ \forall \epsilon > 0, \exists a_\epsilon \in A \mid a_\epsilon < x + \epsilon \end{cases}$$

Démonstration
Si A admet une borne supérieure a.
Alors l'ensemble $M_A = \{M \mid \forall\, x \in A, x \leqslant M\}$, des majorants de A est non vide et admet a comme plus petit élément.
Ainsi $a \in M_A$ et donc $\forall\, x \in A,\ x \leqslant a$.
Ensuite, considérons $\epsilon > 0$, alors $a - \epsilon \notin M_A$, et donc $\exists\, x_\epsilon \in A$ tel que $a - \epsilon < x_\epsilon$ (absurde).
Réciproquement, si il existe a tel que $\forall\, x \in A,\ x \leqslant a$ et $\forall\, \epsilon > 0, \exists\, x_\epsilon \in A \mid, a - \epsilon < x_\epsilon$.
Alors A est majorée et l'ensemble des majorants de A (M_A) est non vide : $a \in M_A$.
Soit $m \in M_A$, un majorant de A. Supposons que $m < a$.
Soit $\epsilon = \frac{a-m}{2} > 0$.
On a alors $a - \epsilon < x_\epsilon \leqslant m$ et donc $a \leqslant m + \epsilon = m + \frac{a-m}{2} = \frac{a+m}{2} < \frac{a+a}{2} = a$.
Ceci est contradictoire. Donc si m est un majorant, alors $m \geqslant a$. □

Le théorème suivant est parfois pris comme caractérisation de $\mathbb{R}$. Nous en avons vu la démonstration dans le cours-TD (il faut une défintion pour $\mathbb{R}$)

Théorème - Existence de la borne supérieure
Toute partie non vide majorée de $\mathbb{R}$ admet une borne supérieure.
Toute partie non vide minorée de $\mathbb{R}$ admet une borne inférieure.

Attention - Propriété non vérifiée par $\mathbb{Q}$
Cette propriété différencie $\mathbb{R}$ et $\mathbb{Q}$:
— $\{x \in \mathbb{R} \mid x^2 < 2\}$ admet une borne supérieure (dans $\mathbb{R}$), que l'on notera : $\sqrt{2}$
— mais $\{x \in \mathbb{Q} \mid x^2 < 2\}$ n'admet pas de borne supérieure dans $\mathbb{Q}$ (non existence d'un plus petit élément dans $\mathbb{Q}$ de l'ensemble des majorants rationnels).

Heuristique - Manipuler l'ensemble des majorants et non l'ensemble E lui-même
L'ensemble E peut être très compliqué, un ensemble à trous par exemple $\bigcup_{n\in\mathbb{N}} \left[(1+\frac{1}{n})^n - \frac{1}{n^2}; (1+\frac{1}{n})^n + \frac{1}{n^2}\right]$.
Il vaut mieux raisonner sur l'ensemble des majorants $\mathcal{M}$: celui-ci est nécessairement un intervalle :
Mieux (mais on ne le sait pas encore) il s'agit de l'intervalle fermé $[\sup E, +\infty[$.

Exercice
Soit A une partie de $\mathbb{R}$. On note $\mathcal{M}(A)$, l'ensemble des majorants de A.
A quoi ressemble $\mathcal{M}(A)$?

Correction
Si A n'est pas majoré alors $\mathcal{M}(A) = \emptyset$.
Sinon, alors A admet une borne supérieure, notée $\sup A$. Nécessairement $\sup(A) \in \mathcal{M}(A)$.
Si $m \geqslant \sup A$, alors par transitivité, $\forall\, a \in A,\ a \leqslant \sup A \leqslant m$, donc $m \in \mathcal{M}(A)$. Ainsi $[\sup A, +\infty[\subset \mathcal{M}(A)$.
Réciproquement si $m \in \mathcal{M}(A)$, alors par minimalité de $\sup A$, $m \geqslant \sup A$. Donc $\mathcal{M}(A) \subset [\sup A, +\infty[$.
Dans ce cas $\mathcal{M}(A) = [\sup A, +\infty[$.

Corollaire - Critère de nullité d'un nombre
Un réel a vérifiant $\forall \epsilon > 0, |a| \leqslant \epsilon$ est nul.

Démonstration
Si a vérifie $\forall \epsilon > 0$, $|a| \leqslant \epsilon$, alors $|a|$ est la borne supérieur de $\{0\}$.
Or cette borne supérieur est 0, donc $a = 0$. □

On avait déjà fait une démonstration ici par contraposée.

Pour aller plus loin - Démonstration de ce résultat
$E = \{r \in \mathbb{Q}^+ \mid r^2 < 2\}$ n'admet pas de borne supérieure dans $\mathbb{Q}$ en considèrant $s = \frac{p}{q} \mapsto \frac{3p+4q}{2p+3q}$.
Si $s = \frac{p}{q} \in E$, alors $\frac{p^2}{q^2} < 2$ et $s' = \frac{3p+4q}{2p+3q} \in \mathbb{Q}$.
Par ailleurs, $s^2 < s'^2 < 2$.
En effet : $s' > 0$ et $s < s' \Leftrightarrow p(2p+3q) < q(3p+4q) \Leftrightarrow 2p^2 < 4q^2 \Leftrightarrow \frac{p^2}{q^2} < 2$
et $s'^2 < 2 \Leftrightarrow (3p+4q)^2 < 2(2p+3q)^2 \Leftrightarrow 9p^2 + 16q^2 + 24pq < 8p^2 + 18q^2 + 24pq \Leftrightarrow \frac{p^2}{q^2} < 2$
Par conséquent, si $s = \frac{p}{q}$ est le plus petit des majorants de E, alors nécessairement $s \notin E$.
Mais de même si $s = \frac{p}{q} \notin E$, alors $\frac{p^2}{q^2} > 2$ puis $s' = \frac{3p+4q}{2p+3q} \notin E$ est un majorant plus petit!
Il n'est donc pas possible de trouver un majorant, le plus petit, de E dans $\mathbb{Q}$.

4.2. Densité de $\mathbb{D}$ ou $\mathbb{Q}$ dans $\mathbb{R}$

Ensemble $\mathbb{D}$

Définition - Ensemble des décimaux
Soit $x \in \mathbb{R}$.
On dit que x est un nombre décimal s'il existe $p \in \mathbb{Z}, n \in \mathbb{N}$ tels que $x = \frac{p}{10^n}$.
On note $\mathbb{D}$ l'ensemble des nombres décimaux. On a $\mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q}$.

Remarque - Un nombre décimal…
… c'est tout simplement un nombre qui s'écrit avec une virgule et une fin dans le développement.
Par exemple : $25,456394 = \frac{25\,456\,394}{10^6}$

Définition - Valeur décimale approchée
Si $p \in \mathbb{Z}$ est tel que $\frac{p}{10^n} \leqslant x \leqslant \frac{p+1}{10^n}$,
on dit que $\frac{p}{10^n}$ (resp. $\frac{p+1}{10^n}$) est une valeur décimale approchée par défaut (resp. par excès) de x à la précision 10^{-n}.

Proposition - Obtenir la valeur décimale approchée
Soit $x \in \mathbb{R}$. Pour tout $n \in \mathbb{N}$, $\frac{\lfloor 10^n x \rfloor}{10^n}$ (resp. $\frac{\lfloor 10^n x \rfloor + 1}{10^n}$) est une valeur approchée de x par défaut (resp. par excès) à la précision 10^{-n}.

Démonstration
On fait le calcul $p = \lfloor 10^n x \rfloor \in \mathbb{Z}$, on a donc $p \leqslant 10^n x < p + 1$,
puis en divisant par 10^n : $\frac{p}{10^n} \leqslant x < \frac{p+1}{10^n}$ □

$\mathbb{D}$ (et $\mathbb{Q}$) denses dans $\mathbb{R}$

Heuristique - Une partie dense?
Une partie X est dense dans $\mathbb{R}$ si elle peut toucher (à $\epsilon > 0$ près - choisi par avance, aussi petit qu'on veut) tous les éléments de $\mathbb{R}$ avec les propres de X.

$$\forall\, x \in \mathbb{R}, \qquad \forall \epsilon > 0, \exists\, r \in X, |x - r| < \epsilon$$

Analyse - Vers une définition équivalente
Si X est dense dans $\mathbb{R}$, alors,
pour tout $x \in \mathbb{R}$ et tout $\epsilon > 0$, $\exists\, r \in X$ tel que $|x - r| < \epsilon$, donc $x - \epsilon < r < x + \epsilon$.
pour tout $x \in \mathbb{R}$ et tout $\epsilon > 0$, $]x - \epsilon, x + \epsilon[\cap X \neq \emptyset$.
Ainsi pour tout $a < b \in \mathbb{R}$, en prenant $x = \frac{a+b}{2}$ et $\epsilon = \frac{b-a}{2}$, on a $]a, b[\cap X \neq \emptyset$.
Réciproquement, si pour tout $a < b \in \mathbb{R}$, on a $]a, b[\cap X \neq \emptyset$,
alors pour tout $x \in \mathbb{R}$, $\epsilon > 0$, en prenant $a = x - \epsilon$ et $b = x + \epsilon$, on a $x - \epsilon < r < x + \epsilon$.

Définition - Partie dense dans $\mathbb{R}$
Une partie non vide X de $\mathbb{R}$ est dite dense dans $\mathbb{R}$
si elle rencontre tout intervalle ouvert non vide,
c'est-à-dire si pour deux réels a et b, $a < b$, il existe $x \in X \cap]a, b[$.

Théorème - Parties denses dans $\mathbb{R}$
$\mathbb{D}$, $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$.

Démontrons la densité de $\mathbb{D}$ et celle de $\mathbb{R}\setminus\mathbb{Q}$. Comme $\mathbb{D}\subset\mathbb{Q}$, on en déduira la densité de $\mathbb{Q}$

Démonstration
Soient $x\in\mathbb{R}$. Soit $\epsilon>0$.
Il existe $n\in\mathbb{N}$ tel que $\epsilon>10^{-n}$. Puis il existe $p\in\mathbb{Z}$ tel que $\frac{p}{10^n}\leqslant x\leqslant\frac{p+1}{10^n}$.
Puis on a $\frac{p}{10^n}\in\mathbb{D}$ et

$$\left|x-\frac{p}{10^n}\right|=x-\frac{p}{10^n}\leqslant\frac{p+1}{10^n}-\frac{p}{10^n}=10^{-n}<\epsilon$$

Donc $\mathbb{D}$ est dense dans $\mathbb{R}$.
Puis comme $\mathbb{D}\subset\mathbb{Q}$, on a donc aussi $\mathbb{Q}$ dense dans $\mathbb{R}$. Enfin, on sait que $\sqrt{2}\notin\mathbb{Q}$ (raisonnement par l'absurde). Donc si $r\in\mathbb{Q}$, $\sqrt{2}+r\notin\mathbb{Q}$
Soit $x\in\mathbb{R}$ et $\epsilon>0$. Il existe $r\in\mathbb{Q}$ tel que $|(x-\sqrt{2})-r|<\epsilon$.
Donc $|x-(r+\sqrt{2})|<\epsilon$.
Ainsi $\sqrt{2}+\mathbb{Q}\subset(\mathbb{R}\setminus\mathbb{Q})$ est dense dans $\mathbb{R}$, donc $\mathbb{R}\setminus\mathbb{Q}$ aussi. □

Par l'absurde :

Corollaire -
Tout intervalle de $\mathbb{R}$ contient donc au moins un rationnel et un irrationnel.
On en déduit qu'il y a un rationnel (ainsi qu'un irrationnel) « aussi proche que l'on veut » d'un réel x donné :

$$\text{Soit } x\in\mathbb{R}\quad:\quad\forall\epsilon>0,\exists r\in\mathbb{Q},|x-r|<\epsilon,\qquad\exists\xi\in\mathbb{R}\setminus\mathbb{Q},|x-\xi|<\epsilon$$

5. Bilan

Synthèse

- ⇝ Les ensembles numériques classiques (de $\mathbb{N}$ à $\mathbb{R}$), se déduisent les uns des autres à partir de relation d'équivalence, qui permet d'étendre la relation d'ordre $\leqslant$ toujours totale sur chaque ensemble. Au commencement, l'ensemble $\mathbb{N}$ est la répétition (récursive) de l'addition $+1$.
- ⇝ Nous proposons ici une construction originale et complète de $\mathbb{R}$, à partir de suite de bissecantes de rationnels. Le processus n'est pas nécessairement à retenir, mais il permet de TOUT démontrer, là où le programme demande d'admettre le théorème de la borne supérieure sur $\mathbb{R}$.
- ⇝ On termine par définir la fonction valeur absolue, la partie entière sur $\mathbb{R}$. On étend aussi la notion d'intervalle numérique en sur-ensemble et sous-ensemble de $\mathbb{R}$.

Savoir-faire et Truc & Astuce du chapitre

- — Savoir-faire - Manipuler des nombres réels
- — Savoir-faire - Travailler avec la partie décimale
- — Savoir-faire - Etudier une borne supérieure

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\lvert x\rvert$	Valeur absolue de x, $\lvert x\rvert=\max(x,-x)$,	$\lvert x\rvert\geqslant 0$	On note $x_+=\max(x,0)$, $x_-=\max(-x,0)$. Alors $\lvert x\rvert=x_++x_-$, $x=x_+-x_-$ et $x_+\geqslant 0$, $x_-\geqslant 0$
$\lfloor x\rfloor$	Partie entière de x. $\lfloor x\rfloor=\sup\{n\in\mathbb{N}\mid n\leqslant x\}$	$\lfloor x\rfloor\in\mathbb{N}$ et $\lfloor x\rfloor\leqslant x<\lfloor x\rfloor+1$	On note $\theta=x-\lfloor x\rfloor\in[0,1[$, partie fractionnaire ou décimale de x.
$\sup A$	Borne supérieure de A.	Le plus PETIT des éléments plus grand que TOUS les éléments de A	$m=\sup A\Leftrightarrow\begin{cases}\forall\, a\in A, a\leqslant m\\ M\geqslant a,\forall\, a\in A\Rightarrow M\leqslant m\end{cases}$

Retour sur les problèmes

62. Par récurrence...
63. Vu en cours (avec deux relations d'équivalence)
64. Vu en cours (avec une relation d'équivalence)
65. Vu en TD-cours
66. Bien que $\overline{Q}=\mathbb{R}$, on a une bijection de $\mathbb{N}$ sur $\mathbb{Q}$, mais pas de $\mathbb{N}$ sur $\mathbb{R}$.
D'après un théorème de Bernstein, il suffit de montrer qu'il existe une injection de $\mathbb{Q}$ sur $\mathbb{N}$.
On peut prendre $\mathbb{Q}\to\mathbb{N}$, $(\frac{a}{b})\mapsto 2^{\lfloor a\geqslant 0\rfloor}3^{|a|}5^b$, injective (non surjective),
on voit qu'en fait pour tout $q\in\mathbb{N}$, $\mathbb{N}^q$ s'injecte dans $\mathbb{N}$ (infinité de nombres premiers).
Par ailleurs, si il existe $\varphi:\mathbb{N}\to[0,1]$ bijective. On note $\varphi(i)=x_i=0,x_1^ix_2^i\dots x_n^i\cdots\in[0,1]$ (écriture décimale)
Considérons alors le nombre $X=0,X_1X_2,\dots X_n\dots$ tel que $X_i\equiv\varphi(i)_i+5[10]$.
Nécessairement, pour tout $i\in\mathbb{N}$, $\varphi(i)_i\neq X_i$, donc $\varphi(i)\neq X$.
Ainsi φ n'est pas surjective. Contradiction.

Chapitre 15

Divisibilité et congruence sur $\mathbb{Z}$. PGCD & PPCM

Résumé -

Nous plongeons ici dans une des parties mathématiques les plus ancestrales : la théorie des nombres (entiers) ou arithmétique. Beaucoup de résultats présentés ici datent (au moins) d'Euclide (3-ième siècle avant notre ère) : la notion de divisibilité, associée à la division euclidienne.
Etonnament, le meilleur point de vue sur la question est assez récent : il date des Disquisitiones arithmeticae de GAUSS, *publié à l'aube du XIX siècle. Ce point de vue insiste sur les congruences (modulo n) comme des nouvelles égalités.*
Nous nous concentrons ensuite, dans ce chapitre sur la notion de PGCD de deux (ou plusieurs nombres) et l'algorithme d'Euclide pour l'obtenir. Un théorème clé, ignoré des mathématiciens grecs, est la décomposition de (Bachet-)Bézout. C'est le théorème clé de ce chapitre.
On termine par l'étude du PPCM (sorte de complément symétrique du PGCD)
Youtube (parodies?) :

- *Canal Universaitaire - Arithmétique dans Z - https ://www.canal-u.tv/chaines/canal-unisciel/arithmetique-dans-z/chapitre-arithmetique-partie-1-division-euclidienne-et*
- *Optimal sup-spé - Arithmétique modulaire - https ://www.youtube.com/watch?v=jZoOGB9WUms*

Sommaire

1. Problèmes 290
2. Divisibilité dans $\mathbb{Z}$ 291
2.1. Intégrité de $\mathbb{Z}$ et régularité 291
2.2. Diviseurs, multiples 291
2.3. Division euclidienne de a par b 292
2.4. Arithmétique modulaire 294
3. Plus Grand Commun Diviseur de deux nombres 295
3.1. *PGCD* de deux nombres. Définition « naturelle » . . 295
3.2. Algorithme d'Euclide 296
3.3. Couple de Bézout 298
3.4. Deux caractérisations essentielles du PGCD 300
4. Entiers premiers entre eux. Factorisation 302
4.1. Définition et critère de Bézout 302
4.2. Lemme de Gauss et décomposition en facteurs relativement premiers 302
5. Généralisation à plusieurs entiers 303
5.1. *PGCD* d'un nombre fini d'entiers relatifs 303
5.2. Deux caractérisation du $PGCD(a_1, a_2, \dots a_k)$ 305

5.3. Entiers premiers entre eux dans leur ensemble . . . 306
6. Plus Petit Commun Multiple 307
6.1. Construction 307
6.2. Relation PPCM et PGCD 308
7. Bilan 308

1. Problèmes

? Problème 68 - Pairs, impairs et ...

L'addition de deux nombres pairs ou de deux nombres impairs donnent **toujours** un nombre pair.
L'addition d'un nombre pair et d'un nombre impair deux toujours un nombre impair.
Une multiplication donne un nombre impair si et seulement si les deux nombres multipliés sont impairs.
Comment démontrer ces résultats? Existe-t-il un résultat équivalent pour des multiples de 3, 4, 5, n?
A propos de multiples, on sait que les nombres divisibles par 9 (et 3) sont exactement ceux dont la somme des chiffres est divisible par 9 (respectivement par 3). Est-ce vrai? Pourquoi? Existe-t-il d'autres règles équivalentes?

? Problème 69 - Table de multiplication modulo n

Lorsqu'on trace les tables des multiplications modulo 5 ou modulo 6, on trouve les deux tableaux suivants :

$\times_{[5]}$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\times_{[6]}$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

on voit que sur certaines lignes, on retrouve tous les nombres possibles et pas sur d'autres. Pourquoi?
Existe-t-il des tableaux ou sur toutes les lignes on retrouve tous les nombres (comme celui de la multiplication modulo 5)?

? Problème 70 - Représentation sous un treilli

La divisibilité est l'exemple typique d'une relation d'ordre non totale.
Le treillis est le bon outil pour visualiser les relations d'ordre non totales.
Est-il possible de convertir tous les théorèmes qui suivent en un schéma visuel basé sur des treillis?

? Problème 71 - Division euclidienne et PGCD

Si la division de a par b donne combien de fois on peut placer b dans a (quotient) et la place qui reste (reste), on peut continuer l'algorithme en plaçant ensuite r dans b...
On crée ainsi l'algorithme d'Euclide. Est-ce que cela (se) termine?

. Qu'est-ce qu'on obtient au bout du compte

Problème 72 - Monde fictif

Dans un monde où il n'y aurait que des pièces de 3 euros et 5 euros, quel montant pourrions-nous payer? (Sachant que le vendeur pourrait nous rendre la monnaie).
Et s'il y a des pièces de 6 et 9 euros?
Et des pièces de 6, 10 et 15 euros?

2. Divisibilité dans $\mathbb{Z}$

2.1. Intégrité de $\mathbb{Z}$ et régularité

Proposition - Intégrité de l'anneau $\mathbb{Z}$
$\mathbb{Z}$ est un anneau intègre.
Formellement :

$$\forall\, a,b\in\mathbb{Z},\qquad a\times b=0\Longrightarrow a=0 \text{ ou } b=0$$

Démonstration
On raisonne par contraposée.
Si a et b sont non nuls.
On suppose que $a>0$ et $b>0$. Donc $a\in\mathbb{N}$.
Par récurrence : $a\times b\geqslant b>0$. Donc $a\times b\neq 0$.
Si $b<0$, de même $a\times b\leqslant b<0$. Donc $a\times b\neq 0$.
Si $a<0$, alors $-a>0$ et avec le même raisonnement $a\times b\neq 0$. □

Comme pour tout anneau intègre :

Proposition - Régularité
Les éléments non nuls de $\mathbb{Z}$ sont réguliers. Formellement :

$$\forall\, a\in\mathbb{Z},\ a\neq 0,\qquad \forall\, b,c\in\mathbb{Z},\ a\times b=a\times c\Longrightarrow b=c$$

Démonstration
Si $ab=ac$, alors par distributivité : $a\times(b-c)=0$.
Puis $a\neq 0$ donc $b-c=0$ i.e. $b=c$. □

Pour aller plus loin - Anneaux, Corps...
Nous reviendrons sur ces propriétés formalisées lorsque nous étudierons les anneaux (euclidiens).
On a vu dans le cours sur les groupes, que l'inversibilité entraine la régularité. On voit ici que la réciproque est fausse.
Il existe donc des anneaux intègres qui ne sont pas des corps

Remarque - A quoi sert cette propriété?
Ce résultat assure l'unicité de la décomposition, si a divise d, il n'y a qu'une décomposition possible de d sous la forme $a\times b$.
Par ailleurs, on remarque aussi, qu'à ce stade, n'avons pas besoin de plonger dans $\mathbb{Q}$ l'inégalité $a\times b=a\times c$ en faisant une division par a. Cela est rassurant.

2.2. Diviseurs, multiples

Définition - Diviseur, multiple
Soit $(a,b)\in\mathbb{Z}^2$. On dit que b *divise* a s'il existe $k\in\mathbb{Z}$ tel que $a=kb$ et on note $b|a$.
On dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b.
On note $b\mathbb{Z}=\{b\times k;\ k\in\mathbb{Z}\}$ l'ensemble des multiples de b.

Savoir faire - Montrer que b divise a
(Sous-entendu en arithmétique entière) Le plus important n'est pas de montrer l'existence de k tel que b divise a, mais bien montrer qu'il s'agit d'un nombre entier.

Définition - Ensemble des diviseurs
On notera par la suite $\mathscr{D}(a)$ l'ensemble des diviseurs de a. Pour $a\neq 0$, cet ensemble ne contient qu'un nombre fini d'éléments puisque

$$d|a\Rightarrow|d|\leqslant|a|.$$

Application - Majoration du cardinal
On a donc $\mathrm{Card}(\mathscr{D}(a))\leqslant 2a$. Le pire étant $\mathscr{D}(2)=\{-2;-1;1;2\}$.

Remarque - Le cas de 0 et 1

— 1 et -1 divisent tous les entiers mais ne sont divisibles que par 1 et -1.
— 0 est un multiple de tous les entiers mais n'est diviseur que de lui même.

Définition - Nombres associés
Soit $(a,b)\in\mathbb{Z}^2$. on dit que a et b sont associés si $a|b$ et $b|a$. On a la caractérisation suivante :

$$(a|b \text{ et } b|a)\Leftrightarrow|a|=|b|\Leftrightarrow a=\epsilon b \text{ avec } \epsilon\in\{-1,1\}=\mathbb{Z}^x$$

Proposition - Division de combinaison linéaire
Soit $(a,b)\in\mathbb{Z}^2$. Pour $(u,v)\in\mathbb{Z}^2$, $n\in\mathbb{Z}$, $n\neq 0$ on a :

$$(d|a \text{ et } d|b)\Longrightarrow d|au+bv$$

$$an|bn\Longleftrightarrow a|b$$

Démonstration
Si $d|a$ et $d|b$, alors il existe $a_1,b_1\in\mathbb{Z}$ tels que $a=da_1$ et $b=db_1$.
Donc $au+bv=d\times(a_1u+b_1v)$, et donc d divise $au+bv$.
Si $a|b$, alors il existe $k\in\mathbb{Z}$ tel que $b=ka$, donc $nb=nka$, donc $na|nb$.
et si $na|nb$, alors il existe $k'\in\mathbb{Z}$ tel que $nb=k'na$, donc $b=k'a$, donc $a|b$ □

Exercice
Montrer que la relation « divise » est une relation d'ordre

Correction
Elle est clairement réflexive : $a\times 1=a$.
Elle est antisymétrique ce qu'on a vu sur les nombres associés.
Elle est transitive : si $a|b$ et $b|c$, alors $b=ka$, $c=k'b$, donc $c=k'ka$, donc $a|c$.

2.3. Division euclidienne de a par b

Théorie

Heuristique - La division euclidienne : des soustractions!
A cause de l'algorithme de la division présentée au XIV-ième par Fibonacci, très efficace, on a tendance à considérer la division euclidienne comme une vraie division de a par b, qui s'arrête avant d'écrire les chiffres derrière la virgule.
Mais il est souvent beaucoup plus efficace de considérer l'algorithme d'Euclide comme une succession de soustraction de a par b (ou d'addition de b à a si $a<0$).
L'algorithme suivant le précise.

Représentation - Première représentation de la division euclidienne
sur l'exemple de 15 divisé par 4 :



Théorème - Division euclidienne
Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \text{ et } 0 \leqslant r < b.$$

q et r sont appelés respectivement *quotient* et *reste* de la division euclidienne de a par b.
Dans ce cours, nous noterons comme en Python : $a//b$ pour désigner q et $a\%b$ pour désigner r.

Démonstration
Démontrons *l'existence*. On note $R = \{a - bk, k \in \mathbb{Z}\}$.
Alors $R \subset \mathbb{Z}$, et donc $R \cap \mathbb{N}$ est un sous-ensemble de $\mathbb{N}$.
Ce dernier ensemble admet une valeur minimale : $r \geqslant 0$.
Il existe donc $q \in \mathbb{Z}$ tel que $r = a - bq$.
Si $r \geqslant b$, alors $\overline{r} = r - b \geqslant 0$, et $\overline{r} = a - b(q+1) \in R \cap \mathbb{N}$.
on a donc un nouvel élément de $R \cap \mathbb{N}$ plus petit que r.
Cela est impossible, donc $r < b$.
Démontrons *l'unicité*. Si $a = bq + r = bq' + r'$.
On a donc $b(q - q') = r' - r$. Ainsi b divise $r' - r$.
Or $r, r' \in \{0, 1, \dots b-1\}$, on a donc $r' - r \in \{-b+1; -b+2; \dots; -1; 0; 1; \dots b-2; b-1\}$.
Et le seul nombre de cet ensemble divisible par b est 0.
Donc $r - r' = 0$ i.e. $r = r'$, puis $bq = bq' = a - r$ □

Proposition - Critère de divisibilité et division euclidienne
Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$.
$b|a$ si et seulement si le reste de la division euclidienne de a par b vaut 0.

Démonstration
Si le reste vaut 0, alors avec le quotient q : $a = bq$ donc b divise a.
Réciproquement, si b divise a,
il existe $q \in \mathbb{Z}$ tel que $a = bq = bq + 0$.
Par unicité de la division euclidienne, on peut identifier : $r = 0$. □

Algorithme

Cette démonstration n'est pas explicite. On préfèrera le programme suivant :

Informatique - Division euclidienne

```
def div_eucl(a,b):
    """division euclidienne de a par b"""
    #Principe : on soustrait b autant que necessaire a a
    d,k=a,0
    if a<0 :
        c,eps=-b,-1 # si a<0, il faudra additionner b
    else :
        c,eps=b,1
    while d>=b or d<0:
        d=d-c
        k=k+eps #k = nbre de soustractions = quotient
    return(k,d)
```

Application - Déroulement de `div_eucl(12,5)` et `div_eucl(-12,5)`

Pour suivre un algorithme, on fait un tableau :

d	k	c	eps	test
12	0	5	1	$12 > 5$: vrai
7	1	5	1	$7 > 5$: vrai
2	2	5	1	$2 < 5$ et $2 > 0$: faux

d	k	c	eps	test
-12	0	-5	-1	$-12 < 0$: vrai
-7	-1	-5	-1	$-7 < 0$: vrai
-2	-2	-5	-1	$-2 < 0$: vrai
3	-3	-5	-1	$3 > 0$ et $3 < 5$: faux

Pour aller plus loin - Démontrer qu'un programme fait bien ce qu'il faut...
Pour démontrer qu'un programme fait bien ce qu'il faut, on a besoin :
- *d'un variant de boucle.*
  Il nous assure la terminaison du programme.
  Ici on prend `d`
- *d'un invariant de boucle.*
  Connaissant sa valeur initiale et finale, on obtient le résultat final donné par l'algorithme. On compare avec le résultat attendu.
  Ici, on considère `kb+d=a`

La première application du programme renvoie (2,2). C'est correct : $12 = 2 \times 5 + 2$
La seconde application du programme renvoie $(-3,3)$. C'est correct : $-12 = -3 \times 5 + 3$

Informatique - Récursivité
Une autre possibilité est d'exploiter la récursivité :

```
def div_eucl_rec(a,b):
    """calcul de la division euclidienne de a par b, par recursivite"""
    if a<b and a>-1:
        return(0,a)
    elif a>b :
        m,n=div_eucl_rec(a-b,b)
        return(m+1,n)
    else :
        m,n=div_eucl_rec(a+b,b)
        return(m-1,n)
```

2.4. Arithmétique modulaire

Relation d'équivalence

Définition - a congru à b modulo n
Soient $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.
On dit que *a est congru à b modulo n* si n divise $a - b$ ($\iff a - b \in n\mathbb{Z}$),
c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.
On note $a \equiv b[n]$.

Pour tout $n \in \mathbb{N}^*$, la relation de congruence modulo n est une relation d'équivalence (nous l'avons déjà vu).

Remarque - $\mathbb{U}_n$
Le groupe des racines n-ieme de l'unité (avec la multiplication) est bien un lieu où les congruences modulo n sont naturelles.
En effet, si on note $\xi_r = \exp(\frac{2ri\pi}{n}$, on a $\xi_r = \xi_{r'}$ ssi $r \equiv r'[n]$.
Puis, si on considère $\xi_r \times \xi_s$, on trouve $\xi_{r+s} = \xi_{(r+s)\%n}$.
La proposition suivante donne un système de représentant naturel (et donc le nombre de classe d'équivalence)

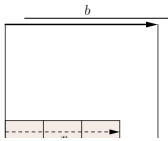
Proposition - Reste
Soit $n \in \mathbb{N}^*$. Pour tout $a, b \in \mathbb{Z}$
$a \equiv b[n] \iff a\%n = b\%n$.
Ainsi, $[\![0, n-1]\!]$ est un système de représentant de $\frac{\mathbb{Z}}{\cdot \equiv \cdot [n]}$, ensemble possédant donc n éléments

Démonstration
Pour tout $a, b \in \mathbb{Z}$, $a = (a//n) \times n + (a\%n)$, et $b = (b//n) \times n + (b\%n)$,
donc $a \equiv (a\%n)[n]$ et $b \equiv (b\%n)[n]$.
Par transitivité :

$$a \equiv b[n] \iff (a\%n) \equiv (b\%n)[n]$$

Or $(a\%n) - (b\%n) \in [\![-(n-1), n-1]\!]$ et donc $n | ((a\%n) - (b\%n)) \implies (a\%n) - (b\%n) = 0$.
Et donc $a \equiv b[n] \iff (a\%n) = (b\%n)$ □

Représentation - Voir les congruences modulo n
Si on prend l'habitude de regarder les congruences modulo n dans un damier (comme lors de la première représentation).
Alors $a \equiv b[n]$ ssi le denier carré de a et de b est dans la même colonne. Ici $15 \equiv 7[4]$.



Arithmétique modulaire

Proposition - Opérations : arithmétique modulaire
Soit $n \in \mathbb{N}$. La congruence modulo n est compatible avec l'addition et la multiplication :

Pour a, a', b, b' entiers relatifs on a

$$\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases} \Longrightarrow \begin{cases} a+b \equiv a'+b'[n] \\ a \times b \equiv a' \times b'[n] \end{cases}$$

Démonstration
Si $a = a' + kn, b = b' + hn$.
Alors $a + b = a' + b' + (k+h)n$ et $a \times b = a'b' + n(a'h + b'k + nhk)$.
□

Truc & Astuce pour le calcul - Réduction modulo n
La réduction modulo n réduit les calculs : les nombres ne dépassent pas la valeur n.
En revanche, on perd des informations ou bien parfois, on supprime les informations inutiles (à quoi sert de connaître exactement un nombre, alors que seul son dernier chiffre est demandé ?)

Remarque - Vérifier un calcul
Dans l'art de calculer, nous avons vu l'importance d'avoir des clés de vérification de calcul.
Ainsi d'après la formule précédente, si $a \equiv a'[n]$, alors $a^k \equiv a'^k[n]$,
et par linéarité, pour tout polynôme P : $P(a) \equiv P(a')[n]$.
Par exemple, montrer qu'une racine entière x d'un polynôme $P = a_0 + a_1 X + \cdots + a_d X^d \in \mathbb{Z}[X]$ vérifie : $x | a_0$.
Il suffit d'écrire : $P(x) = 0 = a_0 + a_1 x + \cdots + a_d x^d \equiv a_0[x]$.
Exercice
Avons-nous l'équivalence $a \equiv b[n] \Longleftrightarrow ca \equiv cb[n]$?
Quelle est l'implication. Donner un contre-exemple de l'implication réciproque. Une condition pour l'équivalence ?

Correction
On a d'après la proposition précédente : pour tout $c \in \mathbb{Z}$, $a \equiv b[n] \Longrightarrow ca \equiv cb[n]$.
La réciproque est fausse : $0 \times 1 \equiv 0 \times 2[3]$, mais $1 \not\equiv 2[3]$.
Si $c \wedge n = 1$, alors $ca \equiv cb[n] \Longrightarrow n | c(a-b) \Longrightarrow n | (a-b)$ (Gauss) $\Longrightarrow a \equiv b[n]$.

Remarque - Réduction modulo p, $p \in \mathscr{P}$
Si p est premier, donc premier avec tous les nombres, pour tout $a \in \mathbb{Z}$, $a \wedge p = 1$, donc d'après le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tels que $ua + vp = 1$, donc modulo p : $au \equiv 1[p]$.
Ainsi, a est inversible. Donc $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps (tous les éléments sont inversibles, donc régulier.

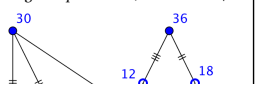
3. Plus Grand Commun Diviseur de deux nombres

3.1. $PGCD$ de deux nombres. Définition « naturelle »

Il s'agit du plus grand pour la relation d'ordre classique : $\leqslant$.

Analyse - Construction du $PGCD$
Soient a et b deux entiers relatifs non nuls.
L'intersection des deux ensembles des diviseurs de a et de b : $\mathscr{D}(a) \cap \mathscr{D}(b)$ est non vide.
En effet, 1 appartient à ces deux ensembles.
Puis, l'ensemble des diviseurs entiers de a et de b : $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}$ est un sous-ensemble de $\mathbb{N}$, non vide majorée par $|a|$ (et/ou $|b|$).
Cet ensemble admet donc un plus grand élément, c'est le plus grand diviseur commun à a et b.

Pour aller plus loin - Treillis des diviseurs
Il est possible de représenter sous forme de treillis les diviseurs de 30 et 36 et chercher le PGCD.
C'est le plus grand pour $a \leqslant b$, mais aussi $a|b$



Définition - $PGCD$ de a et b
Soient a et b deux entiers relatifs non nuls.
On appelle $PGCD$ (Plus Grand Commun Diviseur) de a et b, le nombre
$PGCD(a,b) = \max\left(\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}\right)$.
On le note également $a \wedge b$.
On a clairement $b \wedge a = a \wedge b = |a| \wedge |b|$.
Par convention on pose pour $a \in \mathbb{Z}$, $a \wedge 0 = |a|$ (y compris si $a = 0$).

Exemple - $a = 36$, $b = 30$
$\mathscr{D}(a) = \{-36, -18, -12, -9, -6, -3, -2, -1, 1, 2, 3, 4, 6, 9, 12, 18, 36\}$.
$\mathscr{D}(b) = \{-30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30\}$.
$\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N} = \{1, 2, 3, 6\}$,
et donc $PGCD(36,30) = \max\left(\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}\right) = \max(\{1,2,3,6\}) = 6$

Remarque - Divisibilité des nombres de $\mathscr{D}(30) \cap \mathscr{D}(36)$
6, le $PGCD(36,30)$ est divisible par tous les éléments de $\mathscr{D}(30) \cap \mathscr{D}(36)$.
Et c'est le seul (avec son associé : -6) !

Remarque - Algorithme des facteurs premiers
Plus jeunes, les étudiants exploitaient l'algorithme de la décomposition en facteurs premiers.
Il s'agit de faire deux listes : celles des facteurs premiers de chacun des deux nombres.
Puis on multiplie tous ceux qui sont en commun (avec leur multiplicité) pour obtenir le PGCD.
Tant que nous ne savons pas ce qu'est un nombre premier, cet algorithme attendra...

3.2. Algorithme d'Euclide

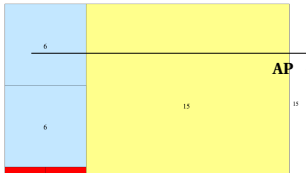
Algorithme des divisions successives pour obtenir le $PGCD$

Lemme - Stabilité par division euclidienne
Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$.
Si $a = bq + r$, alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(r) \cap \mathscr{D}(b)$ et donc $a \wedge b = b \wedge r$.

Démonstration
Supposons que $a = bq + r$.
Si $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$,
$d|a$ et $d|b$, alors $d|1a - qb = r$, donc $d \in \mathscr{D}(r) \cap \mathscr{D}(b)$.
Réciproquement, si $d \in \mathscr{D}(r) \cap \mathscr{D}(b)$,
$d|r$ et $d|b$, alors $d|qb + 1r = a$, donc $d \in \mathscr{D}(b) \cap \mathscr{D}(a)$.
Donc $\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N} = \mathscr{D}(b) \cap \mathscr{D}(r) \cap \mathbb{N}$
et nécessairement, par égalité des maximum : $a \wedge b = b \wedge r$ □

Heuristique - Algorithme pour obtenir le $PGCD$ de deux nombres
La proposition qui donne un algorithme qui exploite une suite de division euclidienne pour trouver le $PGCD(a,b)$.
Il permet également d'obtenir les coefficients de Bézout des nombres a et b.
On notera qu'il s'applique à deux nombres a et b vérifiant : $0 < b < a$. Toute recherche de $PGCD(a,b)$ se ramène à ce cas là, en effet :
— Si $b = 0$ alors $PGCD(a,b) = |a|$
— Si $b \neq 0$, notons alors que $PGCD(a,b) = PGCD(|a|,|b|) = PGCD(|b|,|a|)$,
on peut donc supposer que les deux nombres sont positifs et que le premier est le plus grand.

Représentation - Illustration de l'algorithme d'Euclide (Wikipedia)
pour $a = 21$ et $b = 15$. On complète les trous par des carrés horizontalement↔verticalement :



Proposition - Algorithme d'Euclide
Soient $a, b \in \mathbb{N}^*$. Supposons que $0 < b < a$. L'algorithme d'Euclide consiste en un succession de division euclidienne :
— On commence par poser $r_0 = a$ et $r_1 = b$;
— ensuite, k désignant un entier naturel non nul (étape de l'algo-

rithme),
tant que $r_{k+1} \neq 0$,
on note r_{k+2} le reste de la division euclidienne de r_k par r_{k+1}
(on a donc $r_{k+2} < r_{k+1}$).
Il existe $N \in \mathbb{N}^*$ tel que $r_N = 0$,
r_{N-1} est alors le dernier reste non nul de la suite (r_k), et : $a \wedge b = r_{N-1}$

Démonstration
Il faut démontrer qu'il existe bien N tel que $r_N = 0$.
En fait, à l'issue de l'algorithme, on crée une suite strictement décroissante d'entiers : $r_0 \geqslant r_1 > r_2 > \cdots \geqslant 0$.
Une telle suite est nécessairement nulle à partir d'un certain rang : il existe $N \in \mathbb{N}^*$ tel que $r_N = 0$.
(Mieux : ce rang maximal $N \leqslant r_0$).
Il reste ensuite à appliquer le lemme stabilité par division euclidienne :

$$PGCD(a,b) = PGCD(r_0,r_1) = PGCD(r_1,r_2) = \cdots = PGCD(r_{N-1},r_N)$$
$$= PGCD(r_{N-1},0) = r_{N-1}$$

□

Application - $PGCD(1542,58) = 2$
On calcule une succession de division euclidienne, le diviseur et le reste de la division euclidienne k deviennent respectivement le dividende et le diviseur de la division euclidienne $k+1$:

$1542 = 26\times58+34$, $58 = 1\times34+24$, $34 = 1\times24+10$, $24 = 2\times10+4$, $10 = 2\times4+2$, $4 = 2\times2+0$

d'où

$PGCD(1542,58) = PGCD(58,34) = PGCD(34,24) = PGCD(24,10) = PGCD(10,4) = PGCD(4,2) = PGCD(2,0) = 2.$

La division euclidienne s'exploite en pratique, c'est-à-dire avec un calcul réel, à savoir-faire (on fait plutôt des divisions que des soustractions). Ou bien

Savoir faire - Exploiter la division euclidienne (théorie)
Si $f : \mathbb{Z}^2 \to E$ (E quelconque) tel que $f(a,b) = f(b,a\%b)$, alors $f(a,b) = f(a \wedge b, 0)$.

Truc & Astuce pour le calcul - Trouver son erreur dans un algorithme d'Euclide
Une fois l'algorithme terminé, il est important de vérifier que le dernier reste non nul est bien un diviseur de a et de b.
Si ce n'est pas le cas, il faut revenir à la ligne de calcul où le reste obtenu n'est pas divisible par le PGCD-candidat.

Informatique - Division euclidienne
On peut écrire l'algorithme d'Euclide sous Python. Remarquons que dans le programme ainsi écrit, on tient compte des cas $b = 0$ et a ou b négatif.

```
def alg_eucl(a,b):
    """pgcd(a,b) par algorithme d'Euclide"""
    if b==0:
        return(a)
    a1,a2=max(abs(a),abs(b)),min(abs(a),abs(b))
    ra,rb=a1,a2
    while rb!=0:
        rc=div_eucl(ra,rb)[1]
        ra,rb=rb,rc
    return(ra)
```

Pour aller plus loin - Fractions continues
L'algorithme d'Euclide a une autre application importante : la décomposition en fractions continues. C'est clairement le cas concernant les fractions comme le montre l'exemple :

$$\frac{1542}{58} = 26 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2+\frac{1}{2}}}}}$$

Mais c'est aussi le cas concernant les nombres irrationnels

3.3. Couple de Bézout

Exploitation plus fine de l'algorithme d'Euclide

Analyse - Exploitation plus approfondie encore de l'algorithme d'Euclide
Lorsqu'on applique l'algorithme d'Euclide, on se trouve avec une suite de relations :

$$r_k = q_k r_{k+1} + r_{k+2} \qquad 0 \leqslant r_{k+2} < r_{k+1}$$

Avec $r_0 = a > b$, $r_1 = b > 0$, $r_N = 0$ et $r_{N-1} = a \wedge b$.
On peut alors affirmer (constructivement) qu'il existe u_k et $v_k \in \mathbb{Z}$ tels que

$$\forall\, k \in \mathbb{N} \qquad r_k = u_k a + v_k b$$

On a, en effet :
— $r_0 = a$, donc $u_0 = 1$ et $v_0 = 0$,
— $r_1 = b$, donc $u_1 = 0$ et $v_1 = 1$,
— si $r_k = u_k a + v_k b$ et $r_{k+1} = u_{k+1} a + v_{k+1} b$, alors

$$r_{k+2} = r_k - q_{k+1} r_{k+1} = (u_k - q_{k+1}u_{k+1})a + (v_k - q_{k+1}v_{k+1})b$$

Et en particulier pour $k = N-1$:

$$\exists\, u, v \in \mathbb{Z} \mid a \wedge b = ua + vb$$

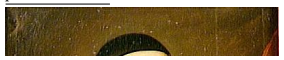
Si $a < b$, ou $a < 0 \ldots$, on applique l'algorithme à $|a|$ et $|b|$ et si nécessaire on multiplie u et v par -1.

Théorème - Coefficients de Bézout
Soit $(a,b) \in \mathbb{Z}^2$. Il existe des entiers u et v tels que $au + bv = a \wedge b$.
Un tel couple (u,v) est appelé un couple de coefficients de Bézout de a et b.

Histoire - Bézout
Etienne Bézout (1730-1783) est un mathématicien français. Il généralisa l'identité de Bachet, c'est pourquoi elle lui est couramment attachée.



Histoire - Bachet de Méziriac ou Bézout
Le théorème de Bézout est en fait obtenu pour la première fois par Gaspard Bachet de Méziriac (1581-1638). C'est un mathématicien, poète et traducteur français. Il a en particulier traduit l'arithmetica de Diophante (là où Fermat a écrit l'énoncé de son grand théorème), et est l'auteur de Problèmes plaisants et délectables qui se font par les nombres



Savoir faire - Pas unicité du couple de Bézout. Les obtenir tous
Il n'y a pas unicité du couple (u,v) :
si (u_0,v_0) est un couple de Bezout, en divisant par $\delta = a \wedge b$:

$$ua + bv = u_0 a + v_0 b \Rightarrow \frac{a}{\delta}(u-u_0) = \frac{b}{\delta}(v_0 - v) \underbrace{\Rightarrow}_{\text{lemme de Gauss}} \frac{a}{\delta} | (v - v_0) \ldots$$

Alors pour tout $n \in \mathbb{Z}$, $(u_0 + n\frac{b}{\delta}, v_0 - n\frac{a}{\delta})$ en est aussi un .

Informatique - Division euclidienne
En étendant la division euclidienne (elle garde en mémoire les calculs des quotients), on peut obtenir les coefficients de Bézout

```
def Bezout(a,b):
    """pgcd(a,b)+coefficient de Bezout"""
    if b==0:
        return(a)
    a1,a2=max(abs(a),abs(b)),min(abs(a),abs(b))
    u,uu=1,0
    v,vv=0,1
    ra,rb=a1,a2
    while rb!=0:
        q,rc=div_eucl(ra,rb)
        ra,rb=rb,rc
        u,uu=uu,u-q*uu
        v,vv=vv,v-q*vv
    return(ra,u,v)
```

Truc & Astuce pour le calcul - Obtenir un couple de Bézout

En pratique, il y a deux stratégies.

• Celle plutôt vue en terminale, assez naturelle et peut-être bien ancrée en vous. On trouve (u,v) en EN REMONTANT l'algorithme d'Euclide.

(à la main, il vaut mieux partir des valeurs numériques, elles n'arrivent qu'en fin d'algorithme).

Par exemple pour 1542 et 58 on a (en remontant les division euclidienne) :

$$\begin{aligned} 2 &= 10-2\times 4 = 10-2(24-2\times 10) = -2\times 24+5\times 10 = -2\times 24+5\times(34-24)\\ &= 5\times 34-7\times 24 = 5\times 34-7\times(58-34) = -7\times 58+12\times 34\\ &= -7\times 58+12\times(1542-26\times 58) = 12\times 1542-319\times 58 \end{aligned}$$

Donc $1542u+58v=2$, avec (par exemple) : $u=12$ et $v=-319$.

• Celle qui découle ici, avec un tableau à remplir directement :

On rappelle qu'à chaque étape $k\in\mathbb{N}^*$: $r_{k+1}=q_kr_k+q_{k-1}$ et (u_k) et (v_k) vérifient la même relation de récurrence $x_{k+1}=-q_kx_k+x_{k-1}$.

k	r_k	q_k	u_k	v_k	$1542\times u_k+58\times v_k=r_k$
0	1542		1	0	1542
1	58	26	0	1	58
2	34	1	1	−26	34
3	24	1	−1	27	24
4	10	2	2	−53	10
5	4	2	−5	133	4
6	2	0	12	−319	2

Algorithme d'Euclide, arithmétique modulaire et carrelage

Analyse - Relation de Bézout modulaire

Si on a $ua+bv=a\wedge b$, on pourrait passer cette relation modulo a :

$$bv\equiv a\wedge b[a]$$

Si la relation modulo a permet de trouver $a\wedge b$ et v (et u), cela peut valoir le coup de représenter l'algorithme d'Euclide.

Exercice

Donner une représentation théorique de la recherche du PGCD de a et de b, par algorithme d'Euclide dans un carrelage.

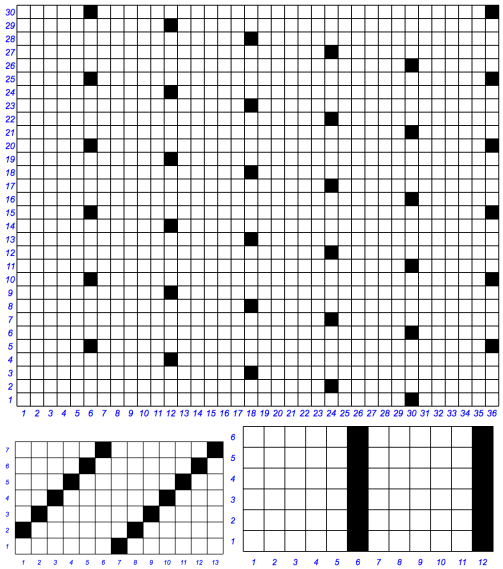
On pourra appliquer la méthode pour donner le $PGCD$ et les coefficient de Bézout pour les couples $(13,7)$ et $(12,6)$

Correction

On cherche le PGCD de a et de b.

On se place sur un carrelage de taille $a\times b$ et on repère les carreaux tous les b déplacements. Ainsi on trouve les restes $k\times b$ divisé par a, pour k de 1 à a.

Le figure obtenu nous donne des informations. Voici trois exemples avec $a=36$ et $b=30$ - $a=13$ et $b=7$ et $a=12$ et $b=6$.



Soient a et $b\in\mathbb{N}$.

Pour tout $u,v\in\mathbb{Z}$, $ua+vb=c\Rightarrow vb\equiv c[a]$

et donc la v-ième case noircie sur le carrelage se trouve en colonne c (reste de la division).

Or on sait que $a\wedge b=\min\{au+bv,u,v\in\mathbb{Z}\}$.

Donc le numéro de la colonne ayant la case noircie la plus à gauche indique le $PGCD$ de a et b.

(Il faut montrer que $\{au+bv,u,v\in\mathbb{Z}\}=\{au+bv,u\in\mathbb{Z},v\in[\![1,a]\!]\}$, mais c'est possible...).

Puis v, le facteur devant b, donne le numéro de la case noircie (c'est la v-ième case noircie).

Enfin, si $ua+bv=c$, on a $bv=-ua+c$

et donc $-u=q$ est le quotient de la division euclidienne de vb par a.

Or ce quotient est exactement égale à ℓ, le numéro de la ligne -1. Donc $u=-q=-(\ell-1)=1-\ell$

On remarque ainsi que le $PGCD$ des deux nombres a et b est toujours égal au numéro de la colonne noircie la plus à gauche. On trouve alors u et v en faisant :

- u (coeffcient de a) : est l'opposé du numéro de la colonne de la case noiricie indiquant le $PGCD$ +1.
- v (coefficient de b) : est le numéro de la case noircie, rappelons que l'on va d'abord de gauche à droite, puis de bas en haut.

Sur le premier exemple, la case noircie la plus à gauche, puis la plus basse se trouve en $(6,5)$. Donc $36\wedge 30=6$.

Puis $u=-5+1=-4$ et $v=5$, car c'est case noircie est la 5-ième.

Et en effet : $-4\times 36+5\times 30=-144+150=6$ On le lit sur le schéma :

- $13\wedge 7=1$ et on a $-1\times 13+2\times 7=1$.
- $12\wedge 6=6$ et on a $0\times 12+1\times 6=6$.

3.4. Deux caractérisations essentielles du PGCD

Caractérisation par divisibilité

En fait la définition de plus grand diviseur commun peut s'entendre d'une seconde façon : plus grand pour la relation d'ordre de divisibilité.

Remarque - Relation binaire

La relation binaire "est un diviseur de", définie par $a\mathcal{R}b\Leftrightarrow a|b$, est une relation d'ordre partiel sur $\mathbb{N}$.

Pour cette relation d'ordre $\mathcal{D}(a)\cap\mathcal{D}(b)$ admet un plus grand élément qui est $a\wedge b$.

Proposition - Caractérisation essentielle du $PGCD$
Soit $(a,b)\in\mathbb{Z}^2$.
Alors $a\wedge b$ est le seul entier naturel dont les diviseurs sont exactement les diviseurs communs à a et b :

$$\mathscr{D}(a\wedge b)=\mathscr{D}(a)\cap\mathscr{D}(b)$$

autre façon de l'écrire :

$$\forall d\in\mathbb{Z},\ (d|a \text{ et } d|b)\iff d|a\wedge b$$

Remarque - Force de cette propriété
Dans l'équivalence trouvée (ou la double inclusion d'ensemble),
une équivalence est triviale : $d|a\wedge b\Longrightarrow d|a$ et $d|b$.
L'usage fréquent que l'on fera donc de cette proposition est : $d|a$ et $d|b\Longrightarrow d|a\wedge b$.

Démonstration
D'après le lemme de stabilité :

$$\mathscr{D}(a)\cap\mathscr{D}(b)=\mathscr{D}(b)\cap\mathscr{D}(r)=\cdots=\mathscr{D}(r_{N-1})\cap\mathscr{D}(r_N)$$

(avec les notations de l'algorithme d'Euclide.
Or $r_{N+1}=0$, donc r_N divise r_{N-1}, et $\mathscr{D}(r_{N-1})\cap\mathscr{D}(r_N)=\mathscr{D}(r_N)$.
Et comme $r_N=a\wedge b$, on en conclue :

$$\mathscr{D}(a\wedge b)=\mathscr{D}(a)\cap\mathscr{D}(b)$$

En ce qui concerne l'équivalence :

$$d|a \text{ et } d|b)\iff d\in\mathscr{D}(a)\cap\mathscr{D}(b)=\mathscr{D}(a\wedge b)\iff d|a\wedge b.$$

Autre démonstration possible :
Si $d|a\wedge b$, alors comme $a=a'(a\wedge b)$, alors $d|a$, de même $d|b$.
Si $d|a$ et $d|b$, alors pour tout u,v, $d|au+bv$, en particulier avec le couple de Bézout. □

Savoir faire - Trouver un PGCD. Exploiter un PGCD.
On note $\delta=a\wedge b$.
Pour trouver le PGCD de a et b :
on démontre que si $m|a$ et $m|b$, alors nécessairement $m|\delta$.
Puis on cherche m le plus grand possible.
(si $m=1$, a et b sont premiers entre eux).
Pour exploiter le PGCD de a et b :
on exploite le fait que si $m|\delta$, alors $m|a$ et $m|b$.
Et on travaille sur cette co-divisibilité.

Caractérisation par combinaison linéaire

Proposition - Combinaison linéaire
Soient $a,b\in\mathbb{Z}$.
On note $a\mathbb{Z}+b\mathbb{Z}$ l'ensemble $\{au+bv,(u,v)\in\mathbb{Z}\}$ des combinaisons linéaires de a et b.
Alors

$$a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z}$$

Démonstration
Notons $\delta=a\wedge b$. D'après le proposition de Bézout, il existe $u_0,v_0\in\mathbb{Z}$ tels que $\delta=au_0+bv_0$.
Comme $\delta|a$ et $\delta|b$, alors pour tout $u,v\in\mathbb{Z}$, $\delta|au+bv$,
donc pour tout $u,v\in\mathbb{Z}$ $au+bv=\delta w\in\delta\mathbb{Z}$.
Ainsi $a\mathbb{Z}+b\mathbb{Z}\subset\delta\mathbb{Z}$.
Réciproquement, pour tout $w\in\mathbb{Z}$, $\delta w=a(u_0w)+b(v_0w)\in a\mathbb{Z}+b\mathbb{Z}$.
Donc $\delta\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}$ □

Pour aller plus loin - Construction classique
La tradition mathématique utilise donc une autre stratégie pour ***définir*** *le PGCD de a et b :*

1. *on s'intéresse à l'ensemble $a\mathbb{Z}+b\mathbb{Z}=\{ua+vb,u,v\in\mathbb{Z}\}$*
2. *on* ***démontre*** *qu'il existe $\delta\in\mathbb{N}^*$ tel que $a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}$*

On appelle alors δ le PGCD de a,b

Savoir faire - Combinaisons linéaires (entières)
Dès que l'on a des combinaisons linéaires d'entiers (on appelle cela un réseau d'entiers), il faut penser que la maille élémentaire est donnée par le PGCD des nombres. C'est par exemple, le cas du problème « monde fictif »

4. Entiers premiers entre eux. Factorisation

4.1. Définition et critère de Bézout

Définition - Couple d'entiers premiers entre eux
a et b sont dits *premiers entre eux* si $a\wedge b=1$.

On note que pour le théorème suivant, nous avons bien une équivalence :

Théorème - Théorème (ou identité) de Bézout
Soient a et b deux entiers relatifs non nuls. Alors

$$a\wedge b=1\iff\exists(u,v)\in\mathbb{Z}^2 \text{ tel que } au+bv=1$$

Démonstration
On applique la décomposition de Bézout : si $a\wedge b=1$ alors $\exists(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.
Réciproquement si $au+bv=1$ alors $d|a$ et $d|b\Rightarrow d|au+bv=1$ donc $d=1$. □

Comme il est plus simple de travailler avec des nombres premiers entre eux, on exploite souvent le savoir-faire suivant :

Savoir faire - Réduction à des entiers premiers entre eux (1)
Soient $a,b\in\mathbb{Z}$. On note $\delta=a\wedge b$.
Alors, $a=\delta a'$ et $b=\delta b'$, avec $a'\wedge b'=1$.
Puis on travaille avec les a' et b'

4.2. Lemme de Gauss et décomposition en facteurs relativement premiers

Enoncé

Théorème - Lemme de Gauss
Soient $a,b,c\in\mathbb{Z}$. Alors

$$(a\wedge b=1 \text{ et } a|bc)\Longrightarrow a|c.$$

Histoire - Disquisitiones Arithmeticae
En 1801, Gauss âgé de 24 ans publie les Disquisitiones Arithmeticae (recherches arithmétiques) et révolutionne totalement le genre. Pour la première fois, on pense les nombres à l'aide de l'arithmétique modulaire (congruence - voir fin de chapitre) !



Démonstration
Si $a\wedge b=1$ alors $\exists(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$
d'où $acu+bcv=c$ et $a|bc\Longrightarrow a|bcv\Longrightarrow a|c-acu$.
Or $a|acu$ d'où $a|c=(c-acu)+acu$. □

Facteur relativement premier

Proposition - Facteur relativement premier
Soient $a,b,c\in\mathbb{Z}$. Alors

$$(a\wedge b=1 \text{ et } a\wedge c=1)\Longrightarrow a\wedge bc=1 \text{ (réciproque vraie)}$$

$$(a \wedge b = 1,\ a|c,\ b|c) \Longrightarrow ab|c$$

Démonstration
D'après l'identité de Bézout il existe u, v, u', v' tels que $au + bv = 1$ et $au' + cv' = 1$,
d'où par produit $a(u(au' + cv')) + a(bu'v) + bcvv' = 1$,
ce qui peut s'écrire $aU + bcV = 1$ avec $(U, V) \in \mathbb{Z}^2$,
et par réciproque de l'identité de Bézout $a \wedge bc = 1$.
Pour la seconde implication : $a|c$ donc $c = aq$; $b|c = aq$ et $b \wedge a = 1$
donc $b|q$; $q = bp$ et $c = abp$ d'où $ab|c$. □

Exercice
On note $\mathscr{P}_a$, l'ensemble des nombres premiers avec a et $a\mathbb{Z}$, les multiples de a.
Ré-écrire les théorèmes de GAUSS avec ces ensembles.

Correction
Le lemme de Gauss : $b \in \mathscr{P}_a$. $bc \in a\mathbb{Z} \Rightarrow c \in a\mathbb{Z}$.
Facteur (1) : $b \in \mathscr{P}_a, c \in \mathscr{P}_a \Rightarrow bc \in \mathscr{P}_a$.
Facteur (2) : $b \in \mathscr{P}_a (\Rightarrow a \in \mathscr{P}_b)$,$c \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow c \in ab\mathbb{Z}$ ou $a, b \in \mathscr{D}(c) \Rightarrow ab \in \mathscr{D}(c)$.

Plusieurs facteurs (relativement premiers)

Corollaire - Facteurs premiers
Soient $a, c, b_1, \dots, b_n$ des entiers relatifs.

$$(\forall i \in [\![1, n]\!],\ a \wedge b_i = 1) \Longrightarrow a \wedge \prod_{i=1}^{n} b_i = 1$$

$$(\forall (i, j) \in [\![1, n]\!]^2,\ i \neq j \Rightarrow b_i \wedge b_j = 1 \text{ et } \forall i \in [\![1, n]\!],\ b_i|c) \Longrightarrow \prod_{i=1}^{n} b_i \Big| c$$

Démonstration
Il suffit de faire une récurrence sur $n = \text{Card}(\{b_i\})$ □

Corollaire - Forme irréductible d'un rationnel
Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ et tel que p et q soient premiers entre eux.
Cette écriture est appelée la forme irréductible de r.
Les autres écritures fractionnaires sont de la forme $r = \dfrac{\lambda p}{\lambda q}$ avec $\lambda \in \mathbb{Z}^*$.

Démonstration

— existence : $r = \dfrac{a}{b} = \dfrac{dp}{dq}$ avec $d = PGCD(a, b)$ et donc $p \wedge q = 1$.

— unicité : $\dfrac{p}{q} = \dfrac{p'}{q'}$ avec $p \wedge q = p' \wedge q' = 1$ implique $pq' = p'q$ et donc $p|p'$ (car $p \wedge q = 1$) et $p'|p$ (car $p' \wedge q' = 1$), d'où $p = p'$ et $q = q'$.

□

5. Généralisation à plusieurs entiers

5.1. $PGCD$ d'un nombre fini d'entiers relatifs

Heuristique - Définition
Au lieu de construire le $PGCD$ de k nombres en prenant :

$$\delta = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$$

nous allons prendre pour définition, une méthode récursive.
On notera ensuite l'extension de la caractéristique vue par la suite :

$$d|a \text{ et } d|b \Longrightarrow d|\delta$$

Dans ce cas le terme « plus grand » ne doit pas être pris pour la relation d'ordre $n \leqslant n$, mais pour la relation d'ordre $n|m$.

Pour aller plus loin - Lien PGCD et inf
inf E *est le plus grand des minorants de* E.
— $\forall\ x \in E, \inf E \leqslant x$
— $\forall\ m$ *tel que* $\forall\ x \in E,\ m \leqslant x$, *alors* $m \leqslant \inf E$.
$PGCD(E)$ *est le plus grand des diviseurs de* E.
— $\forall\ x \in E,\ PGCD(E)\,|\,x$
— $\forall\ m$ *tel que* $\forall\ x \in E,\ m|x$, *alors* $m|PGCD(E)$.
Ce n'est pas la méthode la plus naturelle (compte-tenu du nom PGCD), mais la plus pratique pour les démonstrations…

Définition - Définition par récurrence
Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$. Alors, on définit récursivement :

$$\bigwedge_{i=1}^{k} a_i := \left(\bigwedge_{i=1}^{k-1} a_i\right) \wedge a_k$$

L'identité de Bézout se généralise également :

Proposition - Décomposition de Bézout
Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$.

$$\exists (u_1, \dots, u_k) \in \mathbb{Z}^k \quad | \quad \bigwedge_{i=1}^{k} a_i = \sum_{i=1}^{k} u_i a_i.$$

Démonstration
Il faut faire une récurrence sur k.
Notons, pour tout $k \in \mathbb{N}^*$, $k \geqslant 2$:
$\mathscr{P}_k$: « Pour $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$, $\exists\,(u_1, \dots, u_k) \in \mathbb{Z}^k \mid \bigwedge_{i=1}^{k} a_i = \sum_{i=1}^{k} u_i a_i$. »
— $\mathscr{P}_2$ est vraie. C'est le théorème de Bézout vu plus haut.
— Soit $k \in \mathbb{N}$, $k \geqslant 2$. Supposons que $\mathscr{P}_k$ est vraie.
Soient $(a_1, a_2, \dots, a_k, a_{k+1}) \in \mathbb{Z}^k$.
Notons $\delta_1 = \bigwedge_{i=1}^{k} a_i$ et $\delta = \bigwedge_{i=1}^{k+1} a_i$.
Par définition de δ, $\delta = \delta_1 \wedge a_{k+1}$.
D'après l'identité de Bézout, il existe $u, v \in \mathbb{Z}$ tel que $\delta = u\delta_1 + va_{k+1}$.
Puis on applique $\mathscr{P}_k$, à $(a_1, a_2, \dots, a_k)$: $\delta_1 = u_1 a_1 + \cdots + u_k a_k$.
Finalement $\delta = \sum_{i=1}^{k+1} u'_i a_i$, avec $u'_{k+1} = v$ et $u'_j = u_j \times u$ pour $j \leqslant k$.
Donc $\mathscr{P}_{n+1}$ est vraie.
Notons qu'on aurait pu commencer à $k = 1$, mais le résultat obtenu n'a pas d'intérêt □

Proposition - Avec l'ensemble des diviseurs
Pour tout $j \in \mathbb{N}_k$, $\bigwedge_{i=1}^{k} a_i$ est un diviseur de a_j.
Mieux : $\bigwedge_{i=1}^{k} a_i = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$,
au choix pour max : au sens de la relation d'ordre | ou $\leqslant$.
On a $\mathscr{D}(\bigwedge_{i=1}^{k} a_i) = \bigcap_{j=1}^{k} \mathscr{D}(a_j)$.

Démonstration
On fait la démonstration par récurrence sur k.
Le résultat est vrai par définition pour $k = 2$.
Supposons que le résultat soit vrai pour un nombre $k \in \mathbb{N}$ et $k \geqslant 2$.
Soit $a_1, a_2, \dots a_{k+1} \in \mathbb{N}$.
Alors par définition du PGCD à deux éléments : $\bigwedge_{i=1}^{k+1} a_i$ divise a_{k+1},
et $\bigwedge_{i=1}^{k+1} a_i$ divise $\bigwedge_{i=1}^{k} a_i$.
Mais par récurrence, $\bigwedge_{i=1}^{k} a_i$ divise a_j, pour tout $j \leqslant k$
et par transitivité de la divisibilité : $\bigwedge_{i=1}^{k+1} a_i$ divise donc a_j, pour tout $j \leqslant k$.
Ce qui permet de montrer l'hérédité.
Cela montre également que $\bigwedge_{i=1}^{k} a_i \in \bigcap_{j=1}^{k} \mathscr{D}(a_j)$, donc $\mathscr{D}(\bigwedge_{i=1}^{k} a_i) \subset \bigcap_{j=1}^{k} \mathscr{D}(a_j)$.

Il reste à montrer la maximalité du PGCD.
Soit $n \in \mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}$, alors $n|a_1$, $n|a_2 \dots n|a_k$ et n est positif.
Donc n divise toute combinaison linéaire de ces nombres,
et en particulier $\bigwedge_{i=1}^{k} a_i$, d'après la décomposition de Bézout généralisé.
Mais on vient de voir que $\bigwedge_{i=1}^{k} a_i \in \mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}$, c'est donc bien le plus grand élément pour la divisibilité et pour la relation d'ordre classique.
Et on a également $\bigcap_{j=1}^{k} \mathscr{D}(a_j) \subset \mathscr{D}(\bigwedge_{i=1}^{k} a_i)$ □

5.2. Deux caractérisation du $PGCD(a_1, a_2, \dots a_k)$

Réécriture de la propriété précédente :

Proposition - Critère caractéristique du $PGCD(a_1, a_2, \dots a_k)$
Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$.
$\left(\bigwedge_{i=1}^{k} a_i\right)$ est l'unique entier naturel d dont les diviseurs sont exactement les diviseurs communs à tous les a_i, c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, \qquad (\forall i \in [\![1, k]\!],\ n|a_i) \iff n|d.$$

Démonstration
Notons $\delta = \bigwedge_{i=1}^{k} a_i$,
Pour tout $i \in \mathbb{N}_k$, $\delta \in \mathscr{D}(a_i)$, i.e. $\delta|a_i$.
Si $m|\delta$, alors, par transitivité pour tout $i \in \mathbb{N}_k$, $m|a_i$,
Réciproquement, si pour tout $i \in \mathbb{N}_k$, $m|a_i$. (On suppose aussi que $m \geqslant 1$)
alors m divise toute combinaison linéaire entière des a_i.
δ est une de ces combinaisons linéaires (Bézout), donc $m|\delta$. □

Cela donne bien une caractérisation

Savoir faire - Démonter/utiliser le PGCD de $(a_1, a_2, \dots a_k)$
Tout diviseur du PGCD, divise chaque a_i.
Toute diviseur de tous les a_i est un diviseur de leur PGCD.
Et le PGCD est le plus grand de tous les diviseurs au sens de la relation d'ordre de la division (c'est une borne inférieure).

Proposition - Linéarité absolue
Le PGCD de $(xa_1, xa_2, \dots xa_k)$ est $|x| \times \bigwedge_{i=1}^{k} a_i$

Démonstration
Notons d'abord qu'il existe $u_1, \dots u_k \in \mathbb{Z}$ tel que $\bigwedge_{i=1}^{k} a_i = \sum_{i=1}^{k} u_i a_i$.

1. Notons que $|x| \times \bigwedge_{i=1}^{k} a_i$ est un entier naturel.
2. Puis pour tout $j \in \mathbb{N}_k$, $\bigwedge_{i=1}^{k} a_i | a_j$, donc $|x| \times \bigwedge_{i=1}^{k} a_i | xa_j$.
3. Enfin, si pour tout $j \in \mathbb{N}_k$, $z|xa_j$, alors $z|\sum_{i=1}^{k} u_i x a_i = x \bigwedge_{i=1}^{k} a_i$, donc $z||a| \bigwedge_{i=1}^{k} a_i$.
(Attention, ce qui compte au point 3., ce sont bien les implications!!).

Donc $x| \times \bigwedge_{i=1}^{k} a_i$ est bien le plus grand des diviseurs communs des $(xa_i)_{1 \leqslant i \leqslant k}$ □

Proposition - Sous-groupe $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_k\mathbb{Z}$
Soient $a_1, a_2, \dots a_k \in \mathbb{N}$.
Alors $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_k\mathbb{Z}$ est exactement le sous-groupe de $(\mathbb{Z}, +)$: $\left(\bigwedge_{i=1}^{k} a_i\right)\mathbb{Z}$.
Autrement écrit, le groupe engendré par $\{a_1, a_2, \dots a_k\}$ est le groupe $\left(\bigwedge_{i=1}^{k} a_i\right)\mathbb{Z}$.

$$< a_1, a_2, \dots a_k >_{\mathbb{Z}} = \left(\bigwedge_{i=1}^{k} a_i\right)\mathbb{Z}$$

Démonstration
L'addition de sous-groupes est un sous-groupe de $\mathbb{Z}$.
Comme $\delta := \bigwedge_{i=1}^{k} a_i$ est une combinaison linéaire entière de $a_1, a_2, \dots a_k$ (Bézout),
on a donc $\delta \in a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_k\mathbb{Z}$,
Par stabilité de groupe : $\delta\mathbb{Z} \subset a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_k\mathbb{Z}$.
Réciproquement, puisque $\delta|a_i$, alors pour tout $i \in \mathbb{N}_k$, $a_i \in \delta\mathbb{Z}$.
Par stabilité de groupe : $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_k\mathbb{Z} \subset \delta\mathbb{Z}$ □

5.3. Entiers premiers entre eux dans leur ensemble

Définition - Entiers premiers entre eux dans leur ensemble
Les entiers $a_1, \dots, a_k$ sont dits *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Attention - Ne pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux »
Il ne faut pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».
Par exemple $a =$, $b =$, $c =$
sont
ne sont pas

Tous les savoir-faire donnés précédemment sur les PGCD se généralisent à plusieurs nombres. Nous ne les ré-écrirons pas mais il faudra savoir y penser. Voici un exemple

Savoir faire - Réduction à des entiers premiers entre eux (2)
Soient $a_1, a_2, \dots a_k \in \mathbb{Z}$. On note $\delta = \bigwedge_{i=1}^{k} a_i$.
Alors pour tout $i \in [\![1, k]\!]$, $a_i = \delta a'_i$, avec $(a'_1, a'_2, \dots, a'_k)$ premiers entre eux dans leur ensemble.
Puis on travaille avec les a'_i

Proposition - Théorème (identité) de Bézout
Soient $a_1, \dots, a_k$ des entiers relatifs. Alors

$$\bigwedge_{i=1}^{k} a_i = 1 \iff \exists (u_1, \dots, u_k) \in \mathbb{Z}^k \mid \sum_{i=1}^{k} u_i a_i = 1$$

Démonstration
Si $\bigwedge_{i=1}^{k} a_i = 1$, alors d'après la décomposition de Bézout, $\exists (u_1, \dots, u_k) \in \mathbb{Z}^k \mid \sum_{i=1}^{k} u_i a_i = \bigwedge_{i=1}^{k} a_i = 1$.
Réciproquement, si $\exists (u_1, \dots, u_k) \in \mathbb{Z}^k \mid \sum_{i=1}^{k} u_i a_i = 1$,
alors si pour tout $i \in [\![1, k]\!]$, $n|a_i$, on a $n|\sum_{i=1}^{k} u_i a_i = 1$, donc $n|1$, i.e. $n = 1$.
Par définition du PGCD : $\bigwedge_{i=1}^{k} a_i = 1$ □

Selon que l'on cherche à montrer que des nombres sont premiers entre eux, ou utiliser cette connaissance, on exploite ce l'identité de Bézout de l'une ou l'autre de ces façons :

Savoir faire - Exploiter l'identité de Bézout
Pour montrer que $(a_1, \dots a_n)$ sont premiers entre eux, ils arrivent, qu'on montre :
$\exists\ u_1, u_2, \dots u_n \in \mathbb{Z}$ tels que $\sum_{i=1}^{n} u_i a_i = 1$
Quand, on sait que $(a_1, \dots a_n)$ sont premiers entre eux, on génère alors

$u_1, u_2, \dots u_n \in \mathbb{Z}$ tels que $\sum_{i=1}^{n} u_i a_i = 1$ et on exploite ces (u_i).

6. Plus Petit Commun Multiple

6.1. Construction

On considère une borne supérieure…

Analyse - Construction du $PPCM$

Soient a et b deux entiers relatifs non nuls.
$a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$.
En effet, elle contient au moins $|ab|$, donc elle admet un plus petit élément non nul.
Ce plus petit élément est le $PPCM$ de a et b

Définition - $PPCM$ de a et de b

Soient a et b deux entiers relatifs non nuls.
On appelle $PPCM$ (Plus Petit Commun Multiple) de a et b, le nombre

$$PPCM(a,b) = \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*\right)$$

On le note également $a \vee b$.
On a clairement $b \vee a = a \vee b = |a| \vee |b|$.

Les deux caractéristiques du PGCD se fusionne en une seule, concernant le PPCM :

Proposition - Caractérisation essentielle du $PPCM$

Soit $(a,b) \in \mathbb{Z}^2$. Alors $a \vee b$ est le seul entier naturel dont les multiples sont exactement les multiples communs à a et b

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

c'est-à-dire tel que

$$\forall m \in \mathbb{Z},\ (a|m \text{ et } b|m) \iff a \vee b | m$$

Démonstration

Si $a|m$ et $b|m$, alors m est un multiple commun de a et de b.
Il est a priori plus grand que $a \vee b$, le plus petit de tous.
La division euclidienne donne : $m = q(a \vee b) + r$ avec $r < a \vee b$.
Donc $r = m - q(a \vee b)$ et divisible par a et par b. C'est un commun multiple de a et de b.
Or $r < a \vee b$, la seule possibilité est $r = 0$ et donc $a \vee b$ divise m.
Réciproquement, si $a \vee b$ divise m.
Alors $m = a \vee b \times k$. Mais $a \vee b = aa' = bb'$
Donc $m = a(a'k) = b(b'k)$. Ainsi m est un multiple de a et de b. □

Savoir faire - Trouver un PPCM. Exploiter un PPCM.

On note $\mu = a \vee b$.
Pour trouver le PPCM ,
- on démontre que si $a|m$ et $b|m$, alors nécessairement $\mu|m$.
- Puis on cherche le m le plus petit possible.

Pour exploiter le PPCM,
- on exploite le fait que si $\mu|m$, alors $a|m$ et $b|m$.
- Et on travaille sur cette co-divisibilité.

Proposition - Linéarité

Soient $a, b, \lambda \in \mathbb{Z}$, alors $\lambda a \vee \lambda b = |\lambda|(a \vee b)$.

Démonstration

Si $\lambda a|m$, alors $\lambda|m$, donc $\frac{m}{\lambda} \in \mathbb{Z}$.
On a donc les équivalentes :

$$\lambda a|m, \lambda b|m \iff a|\frac{m}{\lambda}, b|\frac{m}{\lambda} \iff a \vee b|\frac{m}{\lambda} \iff \lambda(a \vee b)|m$$

On peut identifier, en faisant attention à la positivité : $\lambda a \vee \lambda b = \lambda(a \vee b)$. □

6.2. Relation PPCM et PGCD

Proposition - Relation $PPCM$ et $PGCD$

Soient $a, b \in \mathbb{Z}$.
- si $a \wedge b = 1$ alors $|ab| = (a \vee b)$.
- dans le cas général, $|ab| = (a \wedge b) \times (a \vee b)$.

Démonstration

- ab est un multiple commun à a et b.
  Soit n un autre multiple commun. Alors $n = qa$ et $b|qa$, donc $b|q$ et $ab|n$.
  Tous les autres multiples de a et b, sont des multiples de ab.
- Soit $d = a \wedge b$, $a = da'$, $b = db'$ avec $a' \wedge b' = 1$,
  d'où $a' \vee b' = |a'b'|$ et $a \vee b = da' \vee db' = d(a' \vee b') = |da'b'|$ d'où le résultat.

□

Remarque - Généralisation à un nombre fini d'entiers

On peut également généraliser la notion de $PPCM$ à un nombre fini d'entiers relatifs.
Il existe un unique entier naturel m dont les multiples sont exactement les multiples communs à tous les a_i, c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, (\forall i \in [\![1,k]\!], a_i|n) \iff m|n.$$

On l'appelle PPPCM de $a_1, a_2, \dots, a_k$ et on le note $a_1 \vee a_2 \vee \dots \vee a_k$ ou $\bigvee_{i=1}^{k} a_i$.

7. Bilan

Synthèse

⇝ Les nombres entiers relatifs sont les premiers objets reconnus comme mathématiques rencontrés. Ils sont donc comme à la base du sentiment mathématique de tout apprenti mathématicien.

⇝ Comme un jeu, leur manipulation est ludique. On travaille uniquement avec addition et soustraction, puis multiplication ou division euclidienne (soustractions répétées). Pour deux (voire n) nombres quelconques, le commun est le PGCD. C'est comme la plus grosse molécule constitutive de chacun de ces nombres ; avec ces deux nombres, il n'est pas possible de dégager des nombres plus fins que cette molécule. De là, de nombreux lemmes, théorèmes découlent dont les essentielles : théorème de Bézout et lemme de Gauss.
On peut également réfléchir en terme de PPCM.

⇝ Reprenant une idée fondamentale simple et simplifiante de GAUSS, nous pouvons étudier les nombres entiers réduits modulo n. La plupart des propriétés arithmétiques se prolongent bien lors de cette réduction : addition et multiplication (pas très bien pour la division, car tous les nombres ne sont pas nécessairement inversibles…).

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Montrer que b divise a
- Truc & Astuce pour le calcul - Réduction modulo n
- Savoir-faire - Exploiter la division euclidienne (théorie)
- Truc & Astuce pour le calcul - Trouver une erreur dans un algorithme d'Euclide
- Savoir-faire - Pas d'unicité du couple de Bézout. Les obtenir tous
- Truc & Astuce pour le calcul - Obtenir un couple de Bézout
- Savoir-faire - Trouver un PGCD. Exploiter un PGCD.
- Savoir-faire - Combinaisons linéaires (entières)
- Savoir-faire - Réduction à des entiers premiers entre eux (1)
- Savoir-faire - Démontrer/utiliser le PGCD de $(a_1, a_2, \dots a_k)$
- Savoir-faire - Réduction à des entiers premiers entre eux (2)
- Savoir-faire - Exploiter l'identité de Bézout
- Savoir-faire - Trouver un PPCM. Exploiter un PPCM.

Notations

	Propriétés	*Remarques*
les diviseurs de a		
les multiples de a		
reste (resp.) de la division eucli- par b	$a = (a//b) \times b + (a\%b)$ avec $a\%b \in [\![0, b-1]\!]$	Notations Python. Non officielle.
$\Rightarrow \exists\, k \in \mathbb{Z}$ tel que $a = b + nk$	Relation de congruence modulo n (relation d'équivalence)	$\forall\ a \in \mathbb{Z}$, $n \in \mathbb{N}$, $a \equiv (a\%n)\ [n]$
et b (généralisable)	$a \wedge b = \max(\mathscr{D}(a) \cap \mathscr{D}(b))$ $d\|a$ et $d\|b$ ssi $d\|a \wedge b$	$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$
et b (généralisable)	$a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z})$ $a\|m$ et $b\|m$ ssi $a \vee b\|m$	$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$
les nombres premiers avec a	$b \in \mathscr{P}_a \iff a \wedge b = 1$	Equivalent à $a \in \mathscr{P}_b$ (symétrie)

Retour sur les problèmes

67. Oui, on peut tout faire. Sinon, on rajoute le nombre dans les premiers.
68. C'est les congruences.
69. Par exemple, les nombres premiers sont les nombres au premier étage du treillis des diviseurs.
    Le PGCD de deux nombres a et b est celui situé le plus haut dans les racines communes de a et de b.
    Le PPCM de deux nombres a et b est celui situé le plus bas dans les décédants commus de a et de b…
70. Oui cela termine (suite d'entiers naturels, strictement décroissantes). On obtient en dernier reste non nul, le PGCD.
71. Avec 3 et 5 euros, on peut obtenir tous les nombres entiers d'euros.
    Avec 6 et 9 euros, on peut obtenir tous les multiples de 3 euros.
    Avec 6, 10 et 15 euros, on peut obtenir tous les nombres entiers d'euros $(6 + 10 - 15)$.

Chapitre 16

Nombres premiers

Résumé -

Nous continuons notre plongée dans la reine des mathématiques : l'arithmétique. Euclide s'est particulièrement concentré sur l'ensemble des nombres premiers. C'est le but de ce chapitre.
Nous verrons que cet ensemble reste toujours le graal des mathématiciens.
Ces dernières années, les nombres premiers sont revenus au centre des mathématiques comme le coeur des applications numériques de codes secrets (internet...).
Cela nous permettra d'étudier l'énoncé et des applications du petit théorème de Fermat. Nous prendrons le temps de comprendre les idées du plus grand mathématicien toulousain!
Youtube (parodies ?) :

- *Panpan1963 - Petit théorème de Fermat - https ://www.youtube.com/watch ?v=Ei4PMxddm9Q*
- *ScienceEtonnante - Les nombres premiers - https ://www.youtube.com/watch ?v=R37JHiA-HOg*

Sommaire

1. Problèmes 312
2. Théorèmes d'Euclide 312
2.1. Définition 312
2.2. Lemmes d'Euclide 312
2.3. Théorème fondamental 313
3. L'ensemble des nombres premiers 314
3.1. Ensemble infini 314
3.2. Crible d'Eratosthène 315
4. Valuation (p-adique) 315
4.1. Fonction valuation (en base p) 315
4.2. Morphisme (de monoïde) 316
4.3. Factorisation en produit de premiers 316
4.4. Formule de Legendre 317
5. Garantir que des nombres sont premiers 318
5.1. Motivations 318
5.2. Enoncé et applications 319
5.3. Démonstrations 319
6. Bilan 322

1. Problèmes

? Problème 73 - Produit de premiers

Est-ce qu'on peut vraiment tout faire (multiplicativement) qu'avec des nombres premiers?

? Problème 74 - Construction du cours

La notion de divisibilité est toujours première dans un cours d'arithmétique d'entiers.
Puis, ici nous avons choisi (selon le programme officielle) un cours sous la forme : PGCD (et PPCM) $\Longrightarrow$ Nombres premiers $\Longrightarrow$ congruence.
Dans son cours, GAUSS avait choisi : congruence $\Longrightarrow$ PGCD (et PPCM) $\Longrightarrow$ Nombres premiers. Quant à EUCLIDE, il commence par les nombres premiers.
Quel est le choix qui vous semble plus naturel? Comment les démonstrations en sont-elles changées?

? Problème 75 - Fonctions arithmétiques

Si une fonction $f : \mathbb{N} \to \mathbb{Z}$ est un morphisme : $f(ab) = f(a) \times f(b)$ ou $f(ab) = f(a) + f(b)$, que peut-on dire de f, en particulier concernant son image sur $\mathscr{P}$, l'ensemble des nombres premiers qui génèrent $\mathbb{N}$ par multiplication?

2. Théorèmes d'Euclide

2.1. Définition

Il ne s'agit plus d'une notion relative comme précédemment (a et b sont premiers entre eux). Ici, il s'agit d'une notion absolue.

Définition - Nombre premier
Soit $p \in \mathbb{N}^*$.
On dit que p est (un nombre) premier
si $p \neq 1$ et si les seuls diviseurs de p dans $\mathbb{N}$ sont 1 et p.
On note souvent $\mathscr{P}$, l'ensemble des nombres premiers.

Pour aller plus loin - Nombres premiers
Dans un anneau euclidien (muni d'une division euclidienne), un nombre premier est un nombre qui n'est divisible que par des inversibles de l'anneau : si $p = a \times b$, alors a ou $b \in A^*$.
Ici $\mathbb{Z}^* = \{-1, 1\}$. Et pour les polynômes, un polynôme premier n'est divisible que par des constantes : $(\mathbb{K}[X])^* = \mathbb{K}$, c'est un polynôme irréductible.
Un autre anneau euclidien bien connu est $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, l'anneau des entiers de GAUSS.

Le premier théorème d'Euclide est la version « nombre premier » du lemme de Gauss.

2.2. Lemmes d'Euclide

On reconnait le lemme de Gauss et ses corollaires, mais associés à des nombres premiers.

Proposition - Premier théorème d'Euclide
Un nombre premier est premier avec tous les entiers qu'il ne divise pas.
Un nombre premier divise un produit si et seulement si il divise l'un des facteurs.

Démonstration
Soit p un nombre premier et $a \in \mathbb{Z}$.
Notons $\delta = p \wedge a$. Alors $\delta | p$, donc $\delta = 1$ ou p.
Si $\delta = p$, alors $p|a$.
Et si $\delta = 1$, alors a et p sont premiers entre eux.
Supposons $p|a \times b$.
Ou bien $p|a$,
ou bien p ne divise pas a, alors $p \wedge a = 1$ et d'après le lemme de Gauss $p|b$. □

L'intérêt des nombres premiers est d'être des briques élémentaires multiplicatives de $\mathbb{Z}$, on ne peut la couper en deux.
La remarque suivante est un savoir-faire, puisqu'elle donne un truc de manipulation de nombres premiers. Mais c'est aussi un ATTENTION, car il y est associée une erreur fréquente, dans le cas de nombres non premiers.

Savoir faire - Trouver un facteur premier avec un nombre premier
Soit $p \in \mathscr{P}$ tel que $p|ab$ alors p divise a ou p divise b.
Ce n'est pas le cas de $p = 12$ qui divise 6×4 avec $a = 6$ et $b = 4$, par exemple

Théorème -
Tout entier naturel $n \geqslant 2$ possède au moins un diviseur premier.

Démonstration
Soit $n \geqslant 2$.
L'ensemble $\mathscr{D}(n) \cap \mathbb{N} = \{d \in \mathbb{N}; d|n, d \geqslant 2\}$ est une partie non vide de $\mathbb{N}$,
donc admet un plus petit élément $p \geqslant 2$.
Or si $k \geqslant 2$ est tel que $k|p$ alors $k|n$ d'où $k \geqslant p$ et finalement $k = p$ donc p est premier. □

Corollaire - Critère de primalité entre deux entiers
Soient $a, b \in \mathbb{Z}$.
Alors a et b sont premiers entre eux si et seulement s'ils n'ont aucun diviseur premier en commun.

Démonstration
On raisonne en contraposée. Le théorème est équivalent à :
$a \wedge b \neq 1$ si et seulement si $\exists\, p$, premier tel que $p|a$ et $p|b$.
Cette équivalence est vraie en prenant p, un facteur premier de $a \wedge b$.
(c'est possible d'après le théorème) □

Pour aller plus loin - Idéaux premiers
On retrouve aussi la même notion dans la définition des idéaux premiers d'un anneau intègre (vu en seconde année).
De même un groupe simple est un groupe qui ne peut se décomposer en produit de sous-groupes (distingués). La décomposition d'un groupe en produit de sous-groupe simple suit à la même philosophie…

2.3. Théorème fondamental

Puis le théorème fondamental de l'arithmétique :

Théorème - Décomposition en produit de facteurs premiers
Soit $n \in \mathbb{N}$, $n \geqslant 2$.
Alors il existe $r \in \mathbb{N}$, $p_1, p_2, \dots p_r$, r nombres premiers et $\alpha_1, \dots \alpha_r \in \mathbb{N}^*$ tel que

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Cette écriture est unique.

Démonstration
On démontre d'abord l'existence (récurrence) de la décomposition puis son unicité.
— Posons, pour tout $n \in \mathbb{N}$, $n \geqslant 2$, $\mathscr{H}_n$:« tout entier compris entre 2 et n admet une telle décomposition. »
— $\mathscr{H}_2$ est vraie car 2 est premier.
— supposons $\mathscr{H}_n$ vraie pour un certain $n \geqslant 2$.
au rang $n+1$: si $n+1$ est premier, c'est fini,
sinon $n+1 = pq$ avec p premier et $2 \leqslant q \leqslant n$ et on applique $\mathscr{H}_n$ à q.
— Si

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{j=1}^{s} p_j^{\beta_j}$$

alors pour tout i $p_i | n$ d'où il existe j tel que $p_i | q_j$ (p_i premier) soit $p_i = q_j$ (q_j premier),
donc en fait on a les mêmes polynômes irréductibles dans les deux décompositions.
Reste à prouver que les puissances sont les mêmes.
Supposons pour un i que l'on ait alors $\alpha_i > \beta_i$, en simplifiant par $p_i^{\beta_i}$ on a

$$p_i^{\alpha_i - \beta_i} \prod_{k \neq i} p_k^{\alpha_k} = \prod_{k \neq i} p_k^{\beta_k}$$

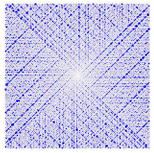
d'où $p_i | \prod_{k \neq i} p_k^{\beta_k}$ ce qui est absurde car p_i premier et $p_i \wedge p_k = 1$ pour $k \neq i$. D'où $\alpha_i = \beta_i$.
□

3. L'ensemble des nombres premiers

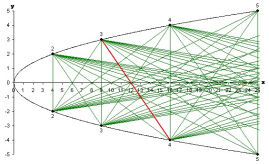
3.1. Ensemble infini

Proposition - Théorème d'Euclide
L'ensemble des nombres premiers, noté $\mathscr{P}$ (parfois $\mathbb{P}$) est infini.

Représentation - Deux visions de $\mathscr{P}$
Sans commentaires :
Spirale d'Ulam :



Crible de Matiyasevich



Démonstration
Par l'absurde :
Supposons qu'il n'y ait qu'un nombre fini de nombres premiers $p_1 < p_2 < \dots < p_n$ (ordonné).
Posons $N = p_1 p_2 \dots p_n + 1$.
On a $N \geqslant 2$ donc N possède un diviseur premier p, et il existe j tel que $p = p_j$
alors $p|p_1 p_2 \dots p_n$ et $p|N$ donc $p| = N - \prod_{i=1}^{n} p_i = 1$ et $p = 1$, ce qui est impossible.
Donc l'ensemble des nombres premiers est infini. □

Cet ensemble mystérieux représente une sorte de graal du mathématicien.

Remarque - Ensemble dénombrable
Comme tout ensemble inclus dans $\mathbb{N}$ et infini, $\mathscr{P}$ est dénombrable, c'est-à-dire il existe une bijection de $\mathbb{N}$ dans $\mathscr{P}$. Et cela signifie qu'on peut donc écrire $\mathscr{P} = \{p_1, p_2, \dots p_r, \dots\}$, où $p_1 = 2$ est le premier des nombres premiers, $p_2 = 3$, $p_3 = 5 \dots$, p_r est le r-ième nombre premier.

Proposition - Enumération des nombres premiers
Il existe une bijection $\rho : \mathbb{N}^* \to \mathscr{P}$, $i \mapsto p_i$, le i-ième nombre premier

Exercice
Que vaut p_{10} ?

Correction
On n'a pas d'autre option que de faire la liste des 20 premiers nombres premiers.
$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$ et $p_{10} = 29$

Démonstration
On construit par récurrence une suite d'ensembles $\mathbb{P}_i$ et une suite d'éléments (p_i) où $p_i \in \mathbb{P}_i$:
— Au rang 1 : $\mathbb{P}_1 = \mathscr{P}$ et $p_1 = \rho(1) = \min \mathbb{P}_1$, on a bien $p_1 \in \mathbb{P}_1$
— On suppose qu'au rang n, $\mathbb{P}_n$ et p_n sont bien définies (avec $p_n \in \mathbb{P}_n$).
On définit alors $\mathbb{P}_{n+1} = \mathbb{P}_n \setminus \{p_n\}$ et $p_{n+1} = \rho(n+1) = \min \mathbb{P}_{n+1}$.
On a bien $p_{n+1} \in \mathbb{P}_{n+1}$
La construction ne s'épuise pas car $\mathscr{P}$ est infini, et qu'à chaque étape, $\mathscr{P}_n$ reste infini. □

3.2. Crible d'Eratosthène

Informatique - Crible d'Eratosthène

Pour obtenir la liste des nombres premiers, nous n'avons pas trouvé beaucoup mieux que le crible d'Eratosthène (3-ième siècle avant J-C).
Il s'agit d'écrire la liste des entiers de 1 à n. Puis d'enlever les multiples des nombres qui restent. Une fois terminée (deux boucles), il ne reste que la liste des nombres premiers plus petit que n.

```
def Eratosthene(n):
    """Crible d'Erathostene adapte"""
    L=[1]*n
    for k in range(2,n):
        if L[k]==1 :
            h=2*k
            while h<n :
                L[h]=0
                h=h+k
    P=[]
    for k in range(1,n):
        if L[k]==1 :
            P=P+[k]
    return(P)
```

Remarque - Conjectures

L'ensemble $\mathscr{P}$ est infini, mais une question résiste : contient-il une infinité de nombres premiers jumeaux?
On dit que $(p, p+2)$ est un couple de nombres premiers jumeaux si ils sont tous les deux premiers. Par exemple $(3,5)$ ou $(11,13)$ sont des nombres premiers jumeaux.
Ben Green(1977-) et Terence Tao (1975-) ont démontré ce qui est désormais connu sous le nom de théorème de Green-Tao (pré-publié en 2004 et publié en 2008). Ce théorème établit qu'il existe des progressions arithmétiques de nombres premiers arbitrairement longues.
Un résultat culturel (mais pas nécessairement à retenir)

Théorème - Hadamard - De la Vallée Poussin (1896)

Notons $\pi(n)$, le nombre de nombres premiers plus petit que n. Alors

$$\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\ln n}$$

Le livre Merveilleux nombres premiers de Jean-Paul Delahaye donne une foule d'informations et d'anecdotes concernant les nombres premiers (par exemple : l'histoire des jumeaux John et Michael qui voient les nombres premiers...).

Exercice

En exploitant le théorème de Hadamard-De la vallée Poussin, donner une valeur approchée du 1000 nombre premiers (i.e. de p_{1000})

Correction

On a $\pi(p_{1000})$ qui est le nombre de nombres premiers plus petit que p_{1000}, par construction, il y en a exactement 1000.
Donc si $n = p_{1000}$, on a $\frac{n}{\ln n} \equiv 1000$.
Il faut inverser la fonction $n \mapsto \frac{n}{\ln n}$. Ce qui est difficile.
Nécessairement, $n \geqslant 1000$, on peut penser que si $n = 1000a$, on a $\ln n = \ln 1000 + \ln a$ et donc

$$\frac{1000a}{\ln 1000 + \ln a} = 1000 \Rightarrow \frac{a}{\ln 1000 + \ln a} \approx 1 \Rightarrow a \approx \ln 1000 = 6,90775$$

Donc $n \approx 6900$

Histoire - Conjecture de Riemann

Parmi les problèmes qui résistent aux mathématiciens, ce trouve la fameuse conjecture de Riemann. Elle concerne directement les nombres premiers même si elle s'énonce avec des nombres complexes. L'esthétisme de cette conjecture réside en partie dans le lien miraculeux entre l'arithmétique à l'ensemble des fonctions de la variable complexe. L'énoncé est :
Les zéros non triviaux de la fonction

$$\begin{array}{rccc} \zeta : & \mathbb{C} & \to & \mathbb{C} \\ & s & \to & \sum_{n=1}^{+\infty} \frac{1}{n^s} \end{array}$$

ont une partie réelle exactement égale à $\frac{1}{2}$.
A lire : la symphonie des nombres premiers de Marcus du Sautoy

4. Valuation (p-adique)

4.1. Fonction valuation (en base p)

Définition - Valuation p-adique

Soit p un nombre premier. Pour $n \in \mathbb{N}$, on appelle *valuation p-adique* de n le plus grand entier $k \in \mathbb{N}$ tel que p^k divise n. On le note $v_p(n)$.
Donc pour p premier, $p|n \Leftrightarrow v_p(n) \geqslant 1$.

On a les caractérisations suivantes, qu'il faut savoir exploiter comme savoir-faire :

Savoir faire - Caractérisations de $v_p(a)$.

$$\begin{array}{ll} p^h|a & \iff v_p(a) \geqslant h. \\ p^h q = a \text{ et } p \wedge q = 1 & \iff v_p(a) = h. \end{array}$$

Démonstration

- $v_p(a) = \max\{h \mid p^h|a\}$ et ainsi $\{h \mid p^h|a\} = [\![0, v_p(a)]\!]$.
  Donc $p^h|a \iff h \in [\![0, v_p(a)]\!] \iff h \leqslant v_p(a)$.
- Si $p^h \times q = a$, alors $p^h|a$, et donc $h \leqslant v_p(a)$.
  Notons $r = v_p(a) - h \in \mathbb{N}$, on a donc $p^h p^r = p^{v_p(a)}|a = p^h q$ donc $p^r|q$.
  Or $p \wedge q = 1$ donc $p^r \wedge q = 1$ et donc $p^r = 1$, donc $r = 0$ et $h = v_p(a)$.

Réciproquement, si $v_p(a) = h$, alors $p^h|a$. On note $q \in \mathbb{N}$ tel que $p^h q = a$.
Soit $\delta = p \wedge q$, alors $\delta|p$, et p premier, donc $\delta = 1$ ou $\delta = p$.
Si $\delta = p$, alors $p|q$ et donc $p^{h+1}|a$, impossible. Donc $\delta = 1$. □

Exercice

Montrer que $v_p(pb) = 1 + v_p(b)$

Correction

$p^{v_p(pb)}|pb \Rightarrow p^{v_p(b)-1}|b \Rightarrow v_p(b) \geqslant v_p(pb) - 1$
$p^{v_p(b)}|b \Rightarrow p^{v_p(b)+1}|pb \Rightarrow v_p(pb) \geqslant v_p(b) + 1$.
Par double inégalité : $v_p(b) = v_p(pb) - 1$.

Remarque - Réécriture du théorème fondamentale de l'arithmétique

Pour tout $n \in \mathbb{N}$,

$$n = \prod_{i=1}^{+\infty} p_i^{v_{p_i}}(n) = \prod_{p \in \mathscr{P}} p^{v_p}(n)$$

le produit en réalité, nécessairement (à support) fini puisqu'à partir d'un certain rang, $v_{p_k}(n) = 0$.

4.2. Morphisme (de monoïde)

Proposition - Valuation, fonction logarithmique

Pour tout $a, b \in \mathbb{Z}$ et $p \in \mathscr{P}$, $v_p(a \times b) = v_p(a) + v_p(b)$

Démonstration

Si on décompose a et b : $a = p^{v_p(a)} q$ et $b = p^{v_p(b)} r$ avec $q \wedge p = 1$ et $r \wedge p = 1$.
Donc $ab = p^{v_p(a)+v_p(b)} qr$.
Et comme d'après le lemme de Gauss : $p \wedge qr = 1$, on a donc $v_p(ab) = v_p(a) + v_p(b)$. □

4.3. Factorisation en produit de premiers

Proposition - Liste des diviseurs

Soient $a, b \in \mathbb{N}$ non nuls. Si

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \text{ et } b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

où les p_i sont des nombres premiers distincts deux à deux, $\alpha_i, \beta_i \in \mathbb{N}$ (éventuellement nuls), alors

$$a|b \iff \forall i \in [\![1,k]\!],\ \alpha_i \leqslant \beta_i$$

$$a \wedge b = PGCD(a,b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)}$$

$$a \vee b = PPCM(a,b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}$$

Ce qui peut aussi s'écrire :

Corollaire - Liste des diviseurs, avec la valuation

$$a|b \iff \forall p \text{ premier}, v_p(a) \leqslant v_p(b)$$

$$\forall p \text{ premier}, v_p(a \wedge b) = \min(v_p(a), v_p(b)) \text{ et } v_p(a \vee b) = \max(v_p(a), v_p(b))$$

$$a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(v_p(a),v_p(b)} \qquad a \vee b = \prod_{p \in \mathscr{P}} p^{\max(v_p(a),v_p(b)}$$

Cette dernière formule se généralisant sans difficulté au cas de k entiers distincts.

Application - Algorithme de recherche du PGCD

On retrouve un algorithme bien connu pour réduire les fractions (simplifier par le PGCD) :
il suffit de chercher la liste des facteurs premiers du numérateur et dénominateur…

Démonstration

Si a divise b, alors $p_i^{\alpha_i}$ divise b et donc $\alpha_i \leqslant \beta_i$.

La réciproque est trivial, avec $c = p_1^{\beta_1-\alpha_1} p_2^{\beta_2-\alpha_2} \dots p_k^{\beta_k-\alpha_k}$, on a $a \times c = b$ Supposons que $d|a$, et $d|b$,

alors $d = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$, avec $\delta_k \leqslant \alpha_k$.
de même $\delta_k \leqslant \beta_k$. Donc $\delta_k \leqslant \min(\alpha_k, \beta_k)$.
C'est le cas pour $d = a \wedge b$.

Par ailleurs : $\prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)}$ divise a et b, donc divise $a \wedge b$.

On peut donc assimiler : $a \wedge b = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)}$ La démonstration pour le $PPCM$ est laissé en exercice. □

Exercice
Soit $n \in \mathbb{N}^*$. Donner une expression de $\text{card}\mathscr{D}(n)$, utilisant les valuations $v_p(n)$

Correction
D'après la proposition : $m|n \iff \forall\ p$, premier $v_p(m) \leqslant v_p(n)$.
Il y a donc pour chacun de ces facteurs p tel que $p|n$, $v_p(n)+1$ choix possibles (de 0 à $v_p(n)$).
Puis d'après le principe de décomposition, il faut tenir compte du produit de ces nombres. Ainsi
$\text{card}\mathscr{D}(n) = \prod_{p|n} (v_p(n)+1)$

4.4. Formule de Legendre

On termine par un exercice

Exercice
Soit p un nombre premier.
Montrer que $v_p(n!) = \sum_{k=1}^{+\infty} \lfloor \frac{n}{p^k} \rfloor$ (la somme étant en réalité finie).
On pourra s'intéresser aux ensembles $N_a = \{k \in \mathbb{N}_n \mid p^a | k\}$.

Correction
Par morphisme : $v_p(n!) = \sum_{k=1}^{n} v_p(k)$. Considérons $N_a = \{k \in \mathbb{N}_n \mid p^a|k\}$. Cet ensemble se décrit facilement :

$$N_a = \{p^a, 2p^a, 3p^a, \dots r_a p^a\}$$

où $r_a p^a \leqslant n$ et $(r_a+1)p^a > n$, donc $r_a = \lfloor \frac{n}{p^a} \rfloor = \text{card} N_a$.
Notons maintenant $M_a = \{k \in \mathbb{N}_n \mid v_p(k) = a\}$.
On a $k \in M_a \iff k \in N_a$ et $k \notin N_{a+1}$.
Donc comme $N_{a+1} \subset N_a$, on a exactement : $N_a = M_a \uplus N_{a+1}$.
Ainsi, en terme de cardinal : $\text{card}(M_a) = \text{card}(N_a) - \text{card}(N_{a+1})$.
Enfin, tous les nombres plus petit que n ont une et une seule valuation p-adique,

$$\mathbb{N}_n = \biguplus_{a \in \mathbb{N}} M_a \qquad \text{(réunion finie)}$$

On note s, la plus grande puissance de p qui divise un nombre plus petit que n : donc $p^s \leqslant n < p^{s+1}$, i.e. $s = \lfloor \frac{\ln n}{\ln p} \rfloor$ Ainsi (par sommation par paquets) :

$$\begin{aligned} v_p(n!) &= \sum_{k \in \mathbb{N}_n} v_p(k) = \sum_{a=0}^{s} \left(\sum_{k \in M_a} v_p(k) \right) = \sum_{a=0}^{s} \left(a \sum_{k \in M_a} 1 \right) = \sum_{a=0}^{s} (a\text{card}(M_a)) \\ &= \sum_{a=1}^{s} a(\text{card}(N_a) - \text{card}(N_{a+1})) = \sum_{a=1}^{s} a\text{card}(N_a) - \sum_{a=0}^{s} a\text{card}(N_{a+1}) \\ &= \sum_{a=1}^{s} a\text{card}(N_a) - \sum_{a=1}^{s+1} (a-1)\text{card}(N_a) = \sum_{a=1}^{s} (a-(a-1))\text{card}(N_a) + s\text{card}(N_{s+1}) \\ &= \sum_{a=1}^{s} \text{card}(N_a) + 0 = \sum_{a=1}^{s} \left\lfloor \frac{n}{p^a} \right\rfloor \end{aligned}$$

5. Garantir que des nombres sont premiers

5.1. Motivations

Heuristique - Décomposable vs. décomposition

L'analyse de la primalité éventuelle d'un nombre n entier peut déboucher sur quatre questions de complexités différentes :

1. Prouver que n n'est pas premier
2. Si n n'est pas premier, le décomposer
3. Garantir, avec un risque d'erreur faible que n est premier
4. Certifier que n est premier

Cela semble comparable, mais le petit théorème de Fermat permet de répondre « aisément » aux questions 1 et 3. Les deux autres questions qui semblent équivalentes sont bien plus compliquées…

Remarque - Obtenir des nombres premiers

L'arithmétique et avec la géométrie la plus vieille branche des mathématiques. Pendant deux millénaires, on s'y intéresse « pour le plaisir ». Mais avec le renouveau de l'algorithmique et la développement exponentielle des ordinateurs, se sont développés deux branches :

— la cryptanalyse
— les codes correcteurs.

Dans ces disciplines, on a très largement besoin de grands nombres premiers. C'est le cas du codage RSA, grand consommateur de nombres premiers qui permet de coder et décoder les messages numérisés (internet, banque…). Il faut trouver des nombres premiers, savoir les reconnaitre. Peut-on faire mieux qu'avec le simple crible d'Eratosthène ?

Pour aller plus loin - Plus grand nombre premier connu (janvier 2016)

C'est un nombre de Mersenne : $2^{74\,207\,281} - 1$, *il contient plus de 22 millions de chiffres.*

Analyse - Et pour Fermat ?

Pierre de Fermat était fasciné par la proposition de Diophante :
« si $s(n) = 1 + 2 + \dots + 2^{n-1}$ *est un nombre premier, alors* $2^{n-1}s(n)$ *est un nombre parfait »*
Or $s(n) = 2^n - 1$. Il fallait savoir si ce nombre est premier. Les nombres premiers de cette forme sont appelés les nombres de Mersenne.
En 1640, Frénicle de Bessy défie Fermat et lui demande de trouver un nombre parfait de 20 chiffres environ.
Pour Fermat, il s'agit de trouver un nombre parfait compris entre 10^{20} et 10^{22}, et donc un nombre premier $s(n) = 2^n - 1$ avec $10^{20} < 2^{n-1}(2^n-1) < 10^{22}$.
Donc $10^{20} < 2^{2n-1} - 2^{n-1} < 10^{22}$.
Or on sait qu'approximativement $2^{10} = 10^3$.

Cela donne donc $10^{20} = 10^{3\cdot 6} \times 100 \approx 2^{60} \times 100 > 2^{66}$ et $10^{22} = 10^{3\cdot 7} \times 10 < 2^{74}$.
Comme le premier ordre est donné par 2^{2n-1}, on trouve $66 < 2n-1 < 74$, $33,5 < n < 37,5$.
Et donc : $34 \leqslant n \leqslant 37$. Il y a 4 nombres $2^n - 1$ avec $n \in \{34, 35, 36, 37\}$ et il faut savoir s'ils sont premiers.
Remarquons d'abord que si $n = ab$ n'est pas premier, par télescopage :

$$2^{ab} - 1 = 2^{ab} - 1^b = (2^a - 1) \sum_{k=0}^{b-1} 2^{ak}$$

Ainsi, le seul possible serait $2^{37} - 1$.

Fermat affirme qu'il n'est pas premier ! Comment s'y est-il pris ?

5.2. Enoncé et applications

Théorème - Petit théorème de Fermat (1640)
Pour p premier et $n \in \mathbb{Z}$, on a $n^p \equiv n[p]$.
Si $n \wedge p = 1$ (i.e. p ne divise pas n) , alors $n^{p-1} \equiv 1[p]$

Savoir faire - Exploiter le petit théorème de Fermat
Il y a deux façons d'exploiter ce théorème pour un nombre N :
- Trouver une factorisation (plus exactement un facteur premier) du nombre N de la forme $a^n - 1$ (voir l'application qui suit)
- Montrer que le nombre N est probablement premier ; dans ce cas N joue le rôle de p (voir la remarque : nombre de Carmichaël)

Application - $2^{37} - 1$ est-il premier ?
Ici, on applique le théorème de Fermat avec $n = 2$ et p, un diviseur premier (s'il existe) de $N = 2^{37} - 1$.
On a donc
- $p | N = 2^{37} - 1$,
- mais aussi $p | 2^{p-1} - 1$ ($p \neq 2$, donc $2 \wedge p = 1$).

Alors Fermat affirme que $37 | p - 1$.
En effet, on considère le PGCD de 37 et $p - 1$: $r = 37 \wedge (p - 1)$.
Comme 37 est un nombre premier, alors $r = 37$ ou $r = 1$.
On applique l'identité de Bézout (modulo p) :

$$2^r \equiv 2^{37u+v(p-1)} \equiv (2^{37})^u \times (2^{p-1})^v \equiv 1[p]$$

L'hypothèse $r = 1$ est impossible : $2^1 = 2 \not\equiv 1[p]$.
finalement $r = 37$ et nécessairement $37 | p - 1$.
Puis comme $p - 1$ est pair, divisible par 2, donc $p - 1 = 2 \times 37 \times q = 74q$.
Et finalement $p = 74q + 1$. Il faut cherche $q \in \mathbb{N}$.
- 75 n'est pas premier.
- Il essaye donc avec $149 = 74 \times 2 + 1$ (nombre premier), cela ne marche.
- Il essaye ensuite le calcul (division) avec $223 = 74 \times 3 + 1$ (nombre premier) et trouve

$$2^{37} - 1 = 223 \times 616\,318\,177$$

Remarque - Réciproque ? Nombre de Carmichaël
Malheureusement, la réciproque du théorème de Fermat est fausse.
Il existe des nombres non premiers P tels que $P | 2^P - 2$:

$$341 | 2^{341} - 2$$

C'est le plus petit contre-exemple. On se restreint ici au cas $n = 2$.
Mais il y a pire, des nombres p, non premiers qui vérifient : $\forall\, a \in \mathbb{N}$, $p | a^p - a$.
Ces nombres sont appelés *les nombres de Carmichaël*.
Le plus petit connu est $p = 561 = 3 \times 11 \times 17$.
On sait depuis peu (1994) qu'il en existe une infinité.

Exercice
Montrer que $341 | 2^{341} - 2$ sans que 341 soit premier.

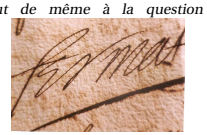
Correction
On note que $341 = 31 \times 11$.
Puis $2^{341} = 2^{10\times34+1} = 2^{10^{34}} \times 2 \equiv 1^{34} \times 2 = 2$ [11] d'après le petit théorème de Fermat.
Puis $2^{341} = 2^{30\times11+11} = 2^{33^{11}} \times 2^5 \times 2^5 \times 2 \equiv 1^{11} \times 1 \times 1 \times 2 = 2$ [31] d'après le petit théorème de Fermat et $2^5 = 32 \equiv 1[31]$.

5.3. Démonstrations

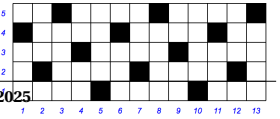
Nous ferons plusieurs démonstrations. Chacune apporte un résultat mathématique différent.

Histoire - Nombres parfaits
Depuis l'antiquité, de nombreux mathématiciens se sont intéressés aux nombres parfaits. Ce sont les nombres égaux à la somme de leurs diviseurs stricts (sans eux-mêmes).
Ainsi $6 = 1 + 2 + 3$ *est parfait. C'est aussi le cas de* 28 *ou* 496*…*

Histoire - De la main de Fermat
« Tout nombre premier mesure infailliblement une des puissances -1 *de quelques progression que ce soit ; et l'exposant de la dite puissance est sous-multiplie du nombre premier donné* -1 *; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question »*



Représentation - Illustration de la démonstration
Dans le cas de $p = 13$ *et* $n = 31$.
On a alors $n \equiv 5[13]$ *et donc* $kn \equiv r_k$ *se voit sur le carrelage* $(a = p = 13, b = 5)$.
On remarque alors que tous les restes sont obtenus, et une et une seule fois



Démonstration
Si n est divisible par p, alors $n^p \equiv 0[p]$ et $n \equiv 0[p]$, donc $n^p \equiv n[p]$.
Supposons n non divisible par p.
Notons $N = n \times 2n \times 3n \times \cdots \times (p-1)n$.
Considérons r_k, le reste de la division euclidienne de kn par p. $kn \equiv r_k[p]$.
- Le calcul direct donne $N = (p-1)! \times n^{p-1}$.
- Mais aussi d'après l'arithmétique modulaire : $N \equiv r_1 \times r_2 \times \cdots \times r_{k-1}[p]$.
- $r_i \neq 0$, sinon : $p | i \times n$, impossible : p premier, n non divisible par p et $i < p$.
- Or si $r_i = r_j$, on a $(i-j)n \equiv 0[p]$, donc $p | (i-j)$, car p est premier et ne divise pas n.
  Or $i, j \in [\![1, p-1]\!]$, donc $i - j \in [\![-p+1, p-1]\!]$ et ainsi $i - j = 0$, i.e. $i = j$.
- Comme tous les i sont distincts, il en est de même des r_i dans $[\![1, p-1]\!]$.
  $N \equiv (p-1)![p]$
- Conclusion : $n^{p-1}(p-1)! \equiv (p-1)![p]$, i.e. $p | (n^{p-1} - 1) \times (p-1)!$.
  Comme p premier, pour tout $k < p$, $p \wedge k = 1$ et donc $p | n^{p-1} - 1$.
  En multipliant par n : $n^p \equiv n[p]$

□

Pour aller plus loin - Fécondité d'un théorème
On peut choisir de mesurer l'intérêt d'un résultat mathématique aux domaines touchés.
Le petit théorème de Fermat *dont la plupart des démonstrations datent d'*Euler *est assurément un théorème fécond. Chacune des démonstrations présentés ici exploite une partie différente des mathématiques : la structure du groupe* $(\frac{\mathbb{Z}}{p\mathbb{Z}}^*, \times)$ *pour la première, le morphisme de* Froebenius *:* $a \mapsto a^p$ *dans le groupe* $(\frac{\mathbb{Z}}{p\mathbb{Z}}, +)$ *pour la seconde. La troisième démonstration assez proche de la première exploite un raisonnement de type combinatoire. La quatrième fait le lien entre la première et la troisième. Elle montre mieux : le petit théorème d'*Euler, $n^{\varphi(p)} = 1[p]$.

Voici la première démonstration historique d'Euler et probablement de Leibniz :

Exercice
Considérons p un nombre premier.
1. Montrer que $\forall k \in [\![1, p-1]\!], p | \binom{p}{k}$
2. $\forall (a, b) \in \mathbb{Z}^2, (a+b)^p \equiv a^p + b^p[p]$
3. En déduire le petit théorème de Fermat

Correction
1. Pour $k \neq 0$, $k \neq p$:
$$k\binom{p}{k} = k\frac{p!}{k!}(p-k)! = p\frac{(p-1)!}{(k-1)!(p-1-k+1)!} = p\binom{p-1}{k-1}$$
Or le coefficient $\binom{p-1}{k-1}$ est un nombre entier, donc p divise $k \times \binom{p}{k}$. Mais p premier, $k < p$, donc d'après le premier théorème d'Euclide : p divise $\binom{p}{k}$.
2. Soient $(a, b) \in \mathbb{Z}^2$, d'après le binôme de Newton,
$$(a+b)^p = \sum_{k=0}^{n} \binom{p}{k} a^k b^{p-k} \equiv a^p + 0 + b^p[p]$$
d'après l'arithmétique modulaire.
3. Démontrons maintenant par récurrence (sur n), le petit théorème de Fermat.
Posons, pour tout $n \in \mathbb{N}^*$, $\mathscr{P}_n$: « $n^p \equiv n[p]$ ».
- $1^p = 1$, donc $\mathscr{P}_1$ vraie.
- Soit $n \in \mathbb{N}^*$, supposons $\mathscr{P}_n$ vraie. On a d'après le résultat plus haut :
$$(n+1)^p \equiv n^p + 1^p \equiv n + 1[p]$$
Donc $\mathscr{P}_{n+1}$ est vraie.

Remarque - Morphisme de Fröbenius
Si p est premier, alors $(a+b)^p = a^p + b^p[p]$ et $(ab)^p = a^p b^p$.
Donc $x \mapsto x^p$ est un morphisme de corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$. C'est un morphisme de corps, a priori non trivial (différent de l'identité). Il s'appelle le morphisme de Fröbenius.
Autre méthode, par double dénombrement :

Exercice
Soit p un nombre premier et n, un entier quelconque.
Considérons un alphabet de n lettres.
1. Combien y a-t-il de mots (possibles) de p lettres avec au moins deux lettres distinctes ? On notera N ce nombre.
2. On note $\mathscr{R}$, la relation d'équivalence sur l'ensemble des mots de p lettres $A = a_1 a_2 \dots a_p$:
$$A \mathscr{R} B \iff \exists\, h \mid B = a_{h+1} a_{h+2} \dots a_p a_1 \dots a_h$$
(Il existe une permutation circulaire des lettres pour passer des mots A à B.
On peut aussi noter que $A = A_1 A_2$ et $B = A_2 A_1$ avec A_1 premier sous-mot de A de longueur h et A_2 de longueur $p - h$.) Montrer qu'il s'agit bien d'une relation d'équivalence.

3. Combien existe-t-il de mots différents dans chaque classe d'équivalence ?
4. On note H le nombre de classe d'équivalence avec au moins deux mots.
   Quelle relation existe-t-il entre H, p et N ?
5. En déduire le petit théorème de Fermat.

Correction

1. Il y a n^p mots distincts, mais il y en n ayant exactement les mêmes lettres.
   Donc $N = n^p - n$.
2. Elle est réflexive et symétrique clairement.
   Si $B = a_{h+1}a_{h+2}\dots a_p a_1 \dots a_h = b_1 \dots b_p$ et $C = b_{k+1}\dots b_p b_1 \dots b_k = a_{h+k+1}\dots a_p a_1 \dots a_{k+h}$
   (si $h+k > p$, il faut prendre plutôt $h+k-p$.)
   donc la relation est transitive.
3. Au plus, il y a p mots différents dans chaque classe d'équivalence : celui qui commence par a_1, celui qui commence par $a_2 \dots$ par a_p.
   Supposons que $A = B$, avec $A = a_1 a_2 \dots a_p$ et $B = a_{h+1}a_{h+2}\dots a_p a_1 \dots a_h$.
   Alors $a_i = a_{h+i}$ pour tout $i \in [\![1, p-h]\!]$ et $a_j = a_{h+j-p}$ pour tout $j \in [\![p-h+1, p]\!]$
   Puis, se crée alors un cycle de même lettre (notons K sa taille) :

   $$a_1 = a_{h+1} = a_{2h+1} = \dots = a_{kh+1[p]} = \dots = a_{(K-1)h+1[p]} = a_{(Kh+1[p]} := a_1$$

   Et finalement $Kh+1 \equiv 1[p]$ i.e. p divise Kh.
   D'après le premier théorème d'Euclide : $p|K$ et donc $K = p$:
   toutes les lettres sont les mêmes. Au final : ou bien les classes d'équivalence ne contiennent qu'un mot : ceux avec une seule lettre, ou bien ces classes ne contiennent que des mots différents, en nombre p.
4. Il y a n classes avec un seul mot,
   et il y a H classes avec p différents.
   On a donc $H \times p + n = n^p$
5. Donc $p|n^p - n$ i.e. $n^p \equiv n[p]$

La seconde démonstration d'Euler exploite (sans le savoir) un théorème dû par la suite à Lagrange.
Cet exercice est un bilan algébrique de l'exercice précédent et de la première démonstration.

Exercice

Soit p premier. Soit $n \in \mathbb{Z}$, supposons que p ne divise pas n.
Notons r le reste de la division euclidienne de n par p.

1. On note $G = ([\![1, p-1]\!], \times)$. Montrer que $(G, \times)$ est un groupe
2. Montrer qu'il existe $k \in \mathbb{N}$ tel que $r^k \equiv 1[p]$. On note $k_0 = \min\{k \in \mathbb{N} \mid r^k \equiv 1[p]\}$
3. Montrer que $\mathscr{R}$: $a\mathscr{R}b$ ssi $\exists\, k \in \mathbb{Z}$ tel que $a = r^k b$
   est une relation d'équivalence.
4. Quelle est la taille de chacune des classe d'équivalence ?
5. On note H le nombre de classe d'équivalence. Montrer que $p - 1 = k_0 \times h$.
   En déduire r^{p-1}, puis le théorème de Fermat

Pour aller plus loin - Théorème d'Euler
En affinant ce dernier exercice, on montre que : pour $t > 0$, n tel que $n \wedge t = 1$, alors $n^{\varphi(t)} \equiv n[t]$, avec $\varphi(a)$ est le nombre de diviseur de a.
Pour cela on considère le groupe des $\varphi(t)$ éléments de $[\![1, t-1]\!]$ inversible (i.e. premier avec t).
On notera que si p est premier : $\varphi(p) = p - 1$.

Correction

1. D'après Bézout, il existe $u, v \in \mathbb{Z}$ tel que $ur + vp = 1$.
   Donc $ur \equiv 1[p]$, quitte à prendre $u_0 \equiv u[p]$, il existe $u_0 \in G$ tel que $u_0 \times r = 1$.
   La stabilité par produit est simple.
2. $\{r^k[p], k \in \mathbb{N}\} \subset G$ est un ensemble fini, il a au plus $p-1$ éléments.
   Donc il existe $k_1 < k_2 \in \mathbb{N}$ tel que $r^{k_1} \equiv r^{k_2}[p]$, alors $r^{k_2-k_1} \equiv 1[p]$.
3. Ok
4. Chacune des classes d'équivalence à k_0 éléments.
5. On a donc $\mathrm{Card}(G) = p - 1 = H \times k_0$, donc $r^{p-1} \equiv r^{H \times k_0} \equiv (r^{k_0})^H \equiv 1^H = 1[p]$.
   Enfin $n^{p-1} \equiv r^{p-1} \equiv 1[p]$ et l'on retrouve le théorème de Fermat.

En fait, si p est premier, on démontre que $r_0 = p - 1$ et $H = 1$.

6. Bilan

Synthèse

- ⇝ Les nombres entiers relatifs sont les premiers objets reconnus comme mathématiques rencontrés. Ils sont donc comme à la base du sentiment mathématique de tout apprenti mathématicien.
- ⇝ Plus généralement, au lieu d'étudier des nombres premiers relativement à a, on peut étudier les nombres premiers relativement à tous les nombres. Ce sont les nombres premiers, atomes minimaux des multiplications/divisions d'entiers.
- ⇝ Gauss a eu la merveilleuse idée de plonger $\mathbb{Z}$ dans des sous-ensemble modulo le nombre a qui nous intéresse. Cela marche bien car la structure d'anneau est conservée, mais cela peut être encore plus fort si a est premier, car on crée une structure de corps ! Avec cette façon de penser, beaucoup de théorèmes devient faciles à démontrer voire à comprendre : c'est le cas du petit théorème de Fermat.
  Nous re-investirons ce point de vue lors de l'étude des polynômes
- ⇝ Nous terminons par l'étude hors-programme de quelques fonctions arithmétiques. La motivation est la même que celle pour les séries génératrices. Il est souvent mathématiquement plus simple d'étudier directement toute la suite (u_n) plutôt qu'un seul de ces éléments $u_n \dots$

Savoir-faire et Truc & Astuce du chapitre

- — Savoir-faire - Trouver un facteur premier, avec un nombre premier.
- — Savoir-faire - Caractérisations de $v_p(a)$.
- — Savoir-faire - Exploiter le petit théorème de Fermat

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\mathscr{P}_a$	Ensemble des nombres premiers avec a	$b \in \mathscr{P}_a \iff a \wedge b = 1$	Equivalent à $a \in \mathscr{P}_b$ (symétrie)
$\mathscr{P}$	Ensemble des nombres premiers	$\mathscr{D}(p) = \{1, -1, p, -p\}$ et $p \in \mathbb{N}$, $p \geqslant 2$	$p \in \mathscr{P} \Leftrightarrow \forall\, k \in [\![2, p-1]\!]$, $k \in \mathscr{P}_p$
$v_p(a)$	Valuation p-adique de a	$v_p(a) = r \Leftrightarrow a = p^r q$ avec $p \wedge q = 1$	On raisonne plutôt par double inégalité

Retour sur les problèmes

72. En effet, en simplifiant par $(n-1)!$, premier avec n (si n est premier), on trouve $k^{n-1} \equiv 1[n]$
73. Par exemple si l'on commence par les nombres premiers, le lemme de Gauss s'applique avec le théorème 1 d'Euclide…
    Nous ne faisons pas ici tous les 6(=3!) cas possibles
74. $f(p_1 p_2) = f(p_1) \times f(p_2)$ et il suffit de connaître $f(p)$, pour tout $p \in \mathbb{N}$:
    $f(\prod_{i=1}^{r} p_i^{r_i}) = \prod_{i=1}^{r} f(p_i)^{r_i}$.

Chapitre 17

Anneaux et corps

Résumé -

Après les groupes, deux nouvelles structures jouent un rôle important en mathématiques : les anneaux et les corps. Ils possèdent chacun deux lois internes et quelques régularités.
L'exemple type d'anneau est l'ensemble $\mathbb{Z}$. Nous baserons notre étude des anneaux sur ce que l'on a pu faire en arithmétique. En retour, nous verrons que le second exemple de l'année $\mathbb{K}[X]$ (anneau intégre des polynômes) possède beaucoup de points commun (notion de PGCD, primamlité...).
Les corps sont des anneaux où tous les éléments sont inversibles pour la seconde loi. C'est un ensemble fréquent : $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, et il sera important pour l'étude des espaces vectoriels...

Sommaire

1. Problèmes 324
2. Structures d'anneau 324
2.1. Définitions et propriétés premières 324
2.2. Construction d'anneaux 326
2.3. Idéaux 328
2.4. Anneau euclidien. Anneau principal 331
3. Structures de corps 332
3.1. Corps 332
3.2. Idéaux maximaux 332
3.3. Sous-corps. Morphisme (de corps) 333
4. Bilan 333

1. Problèmes

Problème 76 - Structures fondamentales associées à $\mathbb{Z}$

Les deux chapitres précédents nous ont prouvé qu'il est possible de faire beaucoup de chose avec une structure aussi limitée que $\mathbb{Z}$.
Pouvons-nous généraliser? Quelles sont les propriétés fondamentales vérifiées par $\mathbb{Z}$?
Rappelons que $\mathbb{Z}$ est créé par addition $+1$. Mais que très vite, c'est la multiplication qui nous intéresse et en particulier la décomposition (unique) en facteurs premiers.

Problème 77 - Théorème de Bézout et le lemme de Gauss dans un anneau

Notons (a) et (b), l'ensemble des multiples de a et b respectivement.
Nous avons vu que le théorème de Bézout était d'une importance capitale. Il exprime que $\mathbb{Z} = (a) + (b)$ lorsque $a \wedge b = 1$.
Plus généralement, comment s'exprime-t-il pour des anneaux? Et le lemme de Gauss?

Problème 78 - Quotienter un anneau

Considérons A, un anneau et munissons le d'une relation d'équivalence $\mathscr{R}$.
A quelle condition suffisante (nécessaire) sur $\mathscr{R}$, peut-on transformer l'ensemble des classes d'équivalence $\frac{A}{\mathscr{R}}$ (avec les lois induites) en anneau voire en corps?

2. Structures d'anneau

2.1. Définitions et propriétés premières

Définition d'un anneau

Définition - Anneaux
Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\star$. On dit que $(A,+,\star)$ est un *anneau* si :
— $(A,+)$ est un groupe commutatif;
— la loi $\star$ est associative;
— la loi $\star$ est distributive par rapport à la loi $+$:

$$\forall (x,y,z) \in A^3,\ x \star (y+z) = x \star y + x \star z \quad \text{(distibutive à gauche)}$$

$$\forall (x,y,z) \in A^3,\ (x+y) \star z = x \star z + y \star z \quad \text{(distibutive à droite)}$$

— A possède un élément neutre pour $\star$, noté 1.
Si de plus la loi $\star$ est commutative, on dit que $(A,+,\star)$ est un anneau commutatif.

Exemple - Anneaux classiques
Les deux anneaux essentiels vus cette année : $\mathbb{Z}$ et $\mathbb{K}[X]$.
Un autre anneau important (mais qui est surtout une algèbre) : $\mathcal{M}_n(\mathbb{K})$.
Un dernier exemple : $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (on en reparlera plus loin)
Soit $(A,+,\star)$ un anneau. On note 0 l'élément neutre de + et 1 celui de $\star$.

Règles de calcul immédiates

Proposition - Lien + et $\star$
On a les relations suivantes :
- $\forall x \in A,\ x\star 0 = 0\star x = 0$ (on dit que 0 est absorbant).
- $\forall (x,y)\in A^2,\ (-x)\star y = x\star(-y) = -(x\star y)$
- $\forall (x,y)\in A^2,\ (-x)\star(-y) = x\star y$

Démonstration
Pour tout $x\in A$, $0+0=0$, car $(A,+)$ est un groupe. Donc

$$0\star x = (0+0)\star x = 0\star x + 0\star x \Longrightarrow 0\star x = 0$$

par régularité dans le groupe $(A,+)$.
De même, on montre que $x\times 0 = 0$.
$(x\star y)+((-x)\star y) = (x+(-x))\star y = 0\star y = 0$, donc $(-x)\star y = -(x\star y)$.
de même $(x\star y)+(x\star(-y)) = (x)\star(y+(-y)) = x\star 0 = 0$, donc $x\star(-y) = -(x\star y)$ Puis $(-x)\star(-y) = -(x\star(-y)) = -(-(x\star y)) = x\star y$ □

Intégrité

Définition - Diviseur de 0 et anneau intègre
Soit $(A,+,\star)$ un anneau.
- $a\in A\setminus\{0\}$ est un diviseur de 0 si il existe $b\in A\setminus\{0\}$ tel que $a\star b = 0$ ou $b\star a = 0$.
- A est dit intègre s'il est commutatif et sans diviseurs de 0.

Pour aller plus loin - Commutativité
Il arrive que certains mathématiciens n'exigent pas la commutativité comme condition à l'intégrité (ex : cours d'Algèbre de Roger Godement), mais c'est une exception à la tradition largement adoptée.

Proposition - Simplification (division)
Si A est un anneau intègre, tout élément non nul a de A est régulier pour $\star$, c'est-à-dire que l'on peut simplifier par a :

$$a\star b = a\star c \Rightarrow b = c.$$

Démonstration
$a\star b = a\star c \Rightarrow a\star b + a\star(-c) = a\star c + a\star(-c) \Rightarrow a\star(b-c) = 0 \Rightarrow b = c$
car $a\neq 0$ et A intègre. □

Exemple - $\mathbb{Z}$ et $\mathcal{M}_n(\mathbb{K})$
$\mathbb{Z}$ est un anneau intègre. $\mathcal{M}_n(\mathbb{K})$ n'est pas intègre ($n\geqslant 2$)

Savoir faire - Exploiter l'intégrité
On exploite l'intégrité dans son sens contraposée : $a\neq 0$ et $b\neq 0 \Longrightarrow ab\neq 0$.
En particulier, si on sait qu'un ensemble est un corps (comme $\frac{\mathbb{Z}}{p\mathbb{Z}}$, alors il est intègre.

Règles fréquentes

Proposition - Quelques règles de calcul
Les règles de calculs fréquentes :
- $(a_i)_{1\leqslant i\leqslant n}$ et $(b_j)_{1\leqslant j\leqslant p}$ deux familles d'éléments de A. Alors on peut écrire :
$$\Big(\sum_{i=1}^{n} a_i\Big)\Big(\sum_{j=1}^{p} b_j\Big) = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_i b_j$$
- formule du binôme : si a et b **commutent pour** $\star$ alors
$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$
- factorisation : si a et b **commutent pour** $\star$ alors
$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-k-1}b^k$$

en notant $xy = x\star y$ et les puissances étant au sens de la loi $\star$.

Remarque - Démonstration?
Il s'agit exactement des mêmes démonstrations que celles vues pour les nombres réels en début d'année.
En effet, les seules hypothèses qui ont été mobilisées étaient celles de commutativité des nombres (objets).

Un groupe pour $\star$: le groupe des inversibles

Proposition - Groupe des inversibles
L'ensemble des éléments inversibles de $(A,\star)$ est un groupe pour la loi $\star$.
Classiquement, ce groupe est noté $A^\times$.

Démonstration
A est non vide et possède au moins 1.
Soient $x,y\in A$, inversibles,

$$(yx^{-1})\star(xy^{-1}) = yx^{-1}xy^{-1} = yy^{-1} = 1 \qquad (xy^{-1})\star(yx^{-1}) = \cdots = 1$$

Donc xy^{-1} est inversible et donc $xy^{-1}\in A^*$.
Dans A^*, $\times$ est associatif.
L'ensemble des inversibles de A est un groupe. □

Exemple - $\mathbb{Z}^*$
$\mathbb{Z}^* = \{-1,1\}$
Exemple - $(\mathcal{M}_n(\mathbb{K}))^*$
L'ensemble des matrices inversibles se note : $\mathcal{M}_n(\mathbb{K})^* = GL_n(\mathbb{K})$.
On parle du groupe linéaire des matrices inversibles (à coefficients dans le corps $\mathbb{K}$.

2.2. Construction d'anneaux

Sous-anneaux

Définition - Sous-anneau
Soit $(A,+,\star)$ un anneau. $B\subset A$ est un *sous-anneau* de A si B est stable pour les lois internes + et $\star$ et si ces lois induites munissent B d'une structure d'anneau, donc, avec $1\in B$.

$(B,+)$ est nécessairement un groupe, stable également pour $\star$: la réciproque est suffisante :

Savoir faire - Caractérisation des sous-anneaux

Soit B une partie de A. B est un sous-anneau de A si et seulement si il vérifie :

- $1 \in B$
- $\forall (x,y) \in B^2,\ x-y \in B$
- $\forall (x,y) \in B^2,\ x \star y \in B$

Démontrons que ce savoir-faire est juste.

Démonstration

Soit B une partie de A. Supposons que $(B,+,\star)$ (lois induites donc stabilités...) soit un sous-anneau

Par hypothèse (définition de sous-anneau) : $1 \in B$.

Alors $(B,+)$ est un sous-groupe de $(A,+)$ et donc on la caracrétisation 2 du sous-groupe :

$\forall (x,y) \in B^2,\ x-y \in B$. Puisque $\star_B = \star$ est une loi interne sur B : $\forall (x,y) \in B^2,\ x \star y \in B$.

Réciproquement supposons que les trois points caractéristiques du savoir-faire sont vérifiés.

Alors B est stable par $\star$ d'après le point 3 respectivement,

il est également stable par $+$ car $0_A = 0_B$, puis si $y \in B$, $-y = 0_B - y \in B$ et $x+y = x-(-y) \in B$ pour $x, y \in B$.

Puis $(B,+_B,\star_B) = (B,+,\star)$ est bien un anneau car :

$(B,+)$ est un groupe avec la caractérisation du point 2.

$\star_B = \star$ reste associatif et distributif par rapport à $+_B = +$.

$(B,\star)$ possède l'élément neutre $1_B = 1$. □

Exercice

Montrer que l'intersection de deux sous-anneaux de A est un sous-anneau de A.
(On pourrait étendre à une intersection d'une famille de sous-anneaux

Correction

Notons les B_1 et B_2. Alors • $1 \in B_1$ et $1 \in B_2$, donc $1 \in B_1 \cap B_2$.

• Si $x, y \in B_1 \cap B_2$, alors $x, y \in B_1$ donc $x-y \in B_1$ et $x, y \in B_2$ donc $x-y \in B_2$.
Donc $x-y \in B_1 \cap B_2$.

• Si $x, y \in B_1 \cap B_2$, alors $x, y \in B_1$ donc $x \star y \in B_1$ et $x, y \in B_2$ donc $x \star y \in B_2$.
Donc $x \star y \in B_1 \cap B_2$.

Exemple - $2\cdot\mathbb{Z}$ est-il un sous-anneau de $(\mathbb{Z},+,\times)$

Si $a, b \in 2\mathbb{Z}$, alors $2|a-b$ et $2|a \times b$ mais $1 \notin 2\cdot\mathbb{Z}$, ce n'est pas un sous-anneau.
En fait un s'agit d'un idéal, on en reparlera avec les anneaux euclidiens $\mathbb{Z}$ et $\mathbb{K}[X]$.

Pour aller plus loin - Idéal

On dit que I ($\subset A$) est un idéal de A, si $(I,+) < (A,+)$ et $\forall\, x \in I, y \in A,\ x \star y \in I$ et $y \star x \in I$ (propriété d'absorbance. Voir plus loin...

Morphisme (et image) d'anneaux

Définition - Morphisme d'anneaux

Soient $(A,+_A,\star_A)$ et $(A',+_{A'},\star_{A'})$ deux anneaux. Un morphisme d'anneaux de A dans A' est une application f de A dans A' vérifiant :

- $\forall (x,y) \in A^2,\ f(x+_A y) = f(x) +_{A'} f(y)$
- $\forall (x,y) \in A^2,\ f(x \star_A y) = f(x) \star_{A'} f(y)$
- $f(1_A) = 1_{A'}$

Exemple - Projection canonique

Soit $F : \mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}},\ m \mapsto \overline{m}$.
Alors $F(m_1+m_2) = \overline{m_1+m_2} = \overline{m_1} + \overline{m_2}$ (on fera une vraie démonstration plus loin).
Alors $F(m_1 \times m_2) = \overline{m_1 \times m_2} = \overline{m_1} \times \overline{m_2}$.

Exemple - Sur $\mathbb{C}$

L'application $z \mapsto \overline{z}$ est également un morphisme d'anneaux (de corps ici).
Avec l'identité, ce sont les seuls morphismes d'anneaux surjectifs de $\mathbb{C}$ sur $\mathbb{C}$.

Exemple - Morphisme de Fröbenius

Nous verrons, dans l'une des démonstrations du petit théorème de Fermat que si p est premier, alors p divise $\binom{k}{p}$, pour tout $k \notin \{0,p\}$.

Alors $\dfrac{\mathbb{Z}}{p\mathbb{Z}} \to \dfrac{\mathbb{Z}}{p\mathbb{Z}},\ m \mapsto m^p$ (p premier) est un morphisme d'anneaux.

On le démontre à l'aide du binôme de Newton.

Proposition - Transfert par morphisme d'anneaux

Soit $f : A \to A'$ un morphisme d'anneaux. Alors

- $f(0_A) = 0_{A'}$
- $\forall\, x \in A,\ f(-x) = -f(x)$ et $\forall\, x \in A^*\ f(x^{-1}) = f(x)^{-1}$.

Démonstration

C'est un morphisme de groupe, donc $f(0) = 0$ ($f(x) = f(x+0) = f(x) + f(0)$. Donc $f(0) = 0$).
De même $0 = f(0) = f(x+(-x)) = f(x) + f(-x)$. Donc $f(-x) = -f(x)$.
$(A^*,\times)$ est un groupe. On applique exactement la même démonstration. □

Proposition - Morphisme du groupe $(A^\times,\star)$

Soit $f : A \to A'$ un morphisme d'anneaux. Alors $f^\times : A^\times \to A'^\times,\ x \mapsto f(x)$ est un morphisme de groupes.

Démonstration

$f(1_A) = 1_{A'}$.
Soient $x, y \in A^\times$.
$1_{A'} = f(1_A) = f(y \star_A y^{-1}) = f(y) \star_{A'} f(y^{-1}1)$, donc $f(y^{-1}) = \big(f(y)\big)^{-1}$. Puis

$$f(x \star_A y^{-1}) = f(x) \star_{A'} f(y^{-1}) = f(x) \star_{A'} \big(f(y)\big)^{-1}$$

A noter que f n'est ni nécessairement surjectif, ni injectif... □

Exercice

On dit que $I \subset A$ est un idéal de l'anneau A, si

- $(I,+)$ est un sous-groupe de $(A,+)$.
- $\forall\, x \in I, y \in A,\ x \star y \in I$ et $y \star x \in I$

Soit $f : A \to A'$ un morphisme d'anneaux. Montrer que $\mathrm{Ker}\, f$ est un idéal de A.

Correction

f est également un morphisme de groupes. Donc $(\mathrm{Ker}\, f,+)$ est un sous-groupe de $(A,+)$.
Soient $x \in \mathrm{Ker}\, f$ et $y \in A$.
Alors $f(x \star y) = f(x) \star f(y) = 0 \star f(y) = 0$, donc $x \star y \in \mathrm{Ker}\, f$. De même pour $y \star x$.
Donc $\mathrm{Ker}\, f$ est bien un idéal de A.

2.3. Idéaux

Dans la suite les anneaux sont considérés commutatifs.

Extension de la congruence

on étend à tous les anneaux, la notion de congruence vu dans $\mathbb{Z}$.

Pour aller plus loin - Cas A non commutatif

Si A n'est pas commutatif, il faut étudier les multiples à droite et les multiples à gauche...

Définition - Multiple dans un anneau

Soit a un élément d'un anneau A. On appelle multiple de a, les éléments de l'ensemble $(a) = \{a \times d, d \in A\}$, (parfois noté aA).
On dit que a divise b (noté $a|b$ si b est un multiple de a.

Définition - Congruence dans un anneau

Soit m un éléments d'un anneau A. Soient a, b deux éléments de A.
On dit que a est congru à b modulo m, noté $a \equiv b[m]$ ssi $b-a \in (m)$ (ou $m|b-a$).

Remarque - Notation multiple
On peut écrire au choix : $m|n$ ou $n \in (m)$ ou encore $(n) \subset (m)$.

Proposition - Relation d'équivalence
Dans un anneau, la relation de congruence modulo m est une relation d'équivalence

Exercice
Faire la démonstration

Correction
- $0 \in (m)$, donc $\equiv [m]$ est réflexif.
- si $k \in (m)$ alors $-k \in (m)$ donc $\equiv [m]$ est symétrique.
- si $k_1, k_2 \in (m)$ alors $k_1 + k_2 \in (m)$ donc $\equiv [m]$ est transitif.

Compatibilité

Théorème - Compatibilité
Si A est un anneau (commutatif) et $m \in A$.
Alors l'addition et la multiplication sont compatibles pour la relation d'équivalence $\equiv [m]$.
Autrement écrit, l'addition et la multiplication sont indépendants du choix du représentant de la classe d'équivalence ; on peut donc définir une addition et une multiplication sur les classes d'équivalence :

$$\overline{x}+\overline{x'} = \overline{x+x'} \qquad \overline{x}\times\overline{x'} = \overline{x\times x'}$$

Démonstration
Supposons que $x \equiv y[m]$ et $x' \equiv y'[m]$.
On peut note $x - y = mk$ et $x' - y' = mk'$, alors

$$x + x' = y + y' + m(k + k') \Longrightarrow x + x' \equiv y + y'$$

Donc la relation de congruence est compatible avec l'addition.

$$x \times x' = (y + mk) \times (y' + mk') = y \times y' + m(ky' + k'y + mkk')$$

Donc la relation de congruence est compatible avec la multiplication.
□

Idéaux

Analyse - Ce qui a marché
Si l'on relit la démonstration, la réussite de compatibilité es lié aux faits que :
— Si $a, a' \in (m)$ alors $a + a' \in (m)$.
Ici $a = x - y$ et $a' = x' - y'$
— Si $a \in (m)$ et $b \in A$ alors $a + b \in (m)$
Ici $a = mk$ et $b = y'$, puis $a = mk'$ et $b = y$

Définition - Idéal de A
Soit A un anneau.
On appelle idéal de A, toute partie I de A tel que :
— $0 \in I$
— $(I, +)$ est un sous-groupe de $(A, +)$ (noté $I < A$)
— $\forall\, a \in I, \forall\, b \in A, ab \in I$

Pour aller plus loin - Cas A non commutatif
Si A n'est pas commutatif, il faut étudier les idéaux à droite ($ba \in I$ si $a \in I$) et les idéaux à gauche ($ab \in I$ si $a \in I$)…

On se souvient que l'on a déjà rencontré $2 \cdot \mathbb{Z}$ qui est un idéal mais pas un sous-anneau de $\mathbb{Z}$. Exercice
Quels sont les idéaux de $\mathbb{Z}$?

Correction
Exactement les ensembles $a\mathbb{Z}$, pour $a \in \mathbb{Z}$

Remarque - Idéal engendré
Comme pour les sous-groupes engendrés (et plus tard les sous-espaces vectoriels engendrés), on définit les idéaux engendrés par une partie B de l'anneau $(A, +, \times)$ comme le plus petit des idéaux contenant B.
On l'obtient comme intersection (décroissante) des tous les idéaux contenant B.
Mais c'est aussi l'ensemble obtenu en faisant agir les éléments de B le plus largement possible… Exercice
Montrer que si I et J sont deux idéaux de $(A, +\times)$, alors $I \cap J$ et $I + J (:= \{a + b \mid a \in I, b \in J\})$ sont des idéaux de A.

Correction
- $I \cap J$.
$0 \in I$, $0 \in J$, donc à $\in I \cap J$.
$(I, +) < (A, +)$, $(J, +) < (A, +)$ donc $(I \cap J, +) < (A, +)$ par propriété des sous-groupes.
Soient $a \in I \cap J$ et $b \in A$, alors $a \in I$, donc $ab \in I$ et $a \in J$ donc $ab \in J$ donc $ab \in I \cap J$.
- $I + J$.
$0 = 0 + 0 \in I + J$, car $0 \in I$ et $0 \in J$
Soient $x, y \in I + J$, il existe $a, c \in I$, $b, d \in J$ tel que $x = a + b$ et $y = c + d$.
Puis $x - y = (a - b) + (c - d) \in I + J$. Donc $I + J < A$.
Soient $x = a + b \in I + J$ et $y \in A$, alors $x \times y = ay + by \in I + J$.

Sous-anneaux quotients

Heuristique - Quotientage d'un anneau par un idéal
Parmi les sous-groupes, les sous-groupes distingués permettaient de prolonger la loi interne (par compatibilité) à la structure quotiente qui devenait ainsi un groupe (quotient).
Formellement : si $(H, +) \lhd (G, +)$, alors $\left(\frac{G}{H}, \overline{+}\right)$ est un groupe.
Il en est de même pour le quotient d'un anneau par un idéal

Proposition - Anneau quotient
Soit $(A, +, \star)$ un anneau (commutatif) et I un idéal.
Alors $\left(\frac{A}{I}, \overline{+}, \overline{\star}\right)$ est un anneau (quotient).

Rappelons que $\frac{A}{I}$ désigne l'ensemble des classes d'équivalence de A pour la relation $a \equiv b \Longleftrightarrow a - b \in I$.

Démonstration
Le plus dur est de montrer la comptabilité des règles opératoires. Mais I étant idéal, tout va bien.
En effet, par construction :

$$\overline{a}\overline{+}\overline{b} = \overline{a+b} \qquad \overline{a}\overline{\star}\overline{b} = \overline{a\star b}$$

Puis l'élément neutre pour $\overline{+}$ est $\overline{0}$, celui pour $\overline{\star}$ est $\overline{1}$.
Plus précisément encore, $\frac{A}{I}$ est un anneau en tant qu'image de A par la projection (surjection) canonique $a \mapsto \overline{a}$. □

Exercice
Montrer que si f est un morphisme d'anneaux A sur B.
Alors $\operatorname{Ker} f = \{x \in A \mid f(x) = 0_B\}$ est un idéal de A.
Puis en déduire que $\frac{A}{\operatorname{Ker} f}$ est un anneau

Correction
C'est comme pour les groupes distingués.
Si $x, y \in \operatorname{Ker} f$, alors $f(x - y) = f(x) - f(y) = 0 - 0 = 0$ car f est un morphisme.
Donc $x - y \in \operatorname{Ker} f$.
Si $x \in \operatorname{Ker} f$ et $a \in A$, alors $f(xa) = f(x)f(a) = 0 \times f(a) = 0$.
Donc $xa \in \operatorname{Ker} f$.
Nous avons enfin une définition propre d'un ensemble dont on a beaucoup parlé.
Puis, comme $a\mathbb{Z}$ est un idéal :

Corollaire - Anneau quotient de $\mathbb{Z}$
Soit $a \in \mathbb{Z}$, l'ensemble $\left(\frac{\mathbb{Z}}{a\mathbb{Z}}, \overline{+}, \overline{\times}\right)$ des classes d'équivalence de $\mathbb{Z}$ est un anneau

2.4. Anneau euclidien. Anneau principal

Proposition - Anneau principal
Soit A un anneau.
On dit qu'un idéal I de A est principal si il existe $a \in I$ tel que $I = (a) (= aA)$.
On dit qu'un anneau est principal s'il est intègre et que tous ses idéaux sont principaux.

Pour aller plus loin - Anneau non principal
L'anneau des polynômes à coefficients entiers $\mathbb{Z}[X]$ n'est pas prinicipal.
En effet, l'idéal engendré dans $\mathbb{Z}[X]$ par $< 2, X >$ n'est pas principal.

Exemple - $\mathbb{Z}$ est principal
Les idéaux de $\mathbb{Z}$ sont les sous-groupes de $(\mathbb{Z}, +)$ donc de la forme $a\mathbb{Z}$.

Savoir faire - Montrer qu'un anneau est principal
Une méthode qui ne marche pas toujours est de montrer qu'un tel anneau est d'abord euclidien.

Définition - Anneau euclidien
Soit A un anneau intègre. On dit que A est euclidien s'il existe une application $\varphi : A \setminus \{0\} \to \mathbb{N}$ (appelé **stathme** euclidien) telle que :

$\forall\ (a,b) \in A \times A \setminus \{0\}, \exists\ (q,r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$

Notons que l'unicité n'est pas demandé.

Proposition - Anneau euclidien $\Rightarrow$ Anneau principal
Si A est euclidien, alors A est principal

Démonstration
Soit I un idéal de A euclidien.

$$\{\varphi(r), r \in I \setminus \{0\}\} \subset \mathbb{N}$$

Cet ensemble est non vide, inclus dans $\mathbb{N}$ donc admet un plus petit élément $s = \varphi(m)$.
Soit $a \in I$. Faisons la division euclidienne de a par m.
Il existe donc $q, r \in A$ tel que $a = mq + r$, avec $\varphi(r) < \varphi(m)$ ou $\varphi(r) = 0$.
Or I est un idéal, donc $mq \in I$ puis $a - mq \in I$, donc $r \in I$.
Comme $s = \varphi(m)$ est minimal, nécessairement, $r = 0$, et donc $m|a$.
Réciproquement, comme $(m) \subset I$.
On a donc $I = (m)$. I est principal.
Ainsi A est un anneau principal □

Exemple - Nombreux
$\mathbb{Z}$ et $\mathbb{K}[X]$ sont euclidiens donc principaux.
Exercice
On note $\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}$, l'ensemble des entiers de Gauss.

1. Trouver une division euclidienne sur $\mathbb{Z}[i]$
   On prendra, le carré de la fonction module comme stathme
2. En déduire que $\mathbb{Z}[i]$ est principal

Correction

1. Supposons que $a = u + iv$ et $b = x + iy$, alors $\frac{a}{b} = \frac{(ux - vy) + i(uy + vx)}{x^2 + y^2}$.
   Notons $m = \begin{cases} \lfloor \frac{ux-vy}{x^2+y^2} \rfloor & \text{si } \theta(\frac{ux-vy}{x^2+y^2}) \leqslant \frac{1}{2} \\ \lfloor \frac{ux-vy}{x^2+y^2} \rfloor + 1 & \text{si } \theta(\frac{ux-vy}{x^2+y^2}) > \frac{1}{2} \end{cases}$ et $n = \begin{cases} \lfloor \frac{uy+vx}{x^2+y^2} \rfloor & \text{si } \theta(\frac{uy+vx}{x^2+y^2}) \leqslant \frac{1}{2} \\ \lfloor \frac{uy+vx}{x^2+y^2} \rfloor + 1 & \text{si } \theta(\frac{uy+vx}{x^2+y^2}) > \frac{1}{2} \end{cases}$,
   puis $s = \frac{a}{b} - (m + in)$.
   Alors $a = bq + r$ (avec $q = m + in \in \mathbb{Z}[i]$) et $r = sb$.
   Puis $|r|^2 = (sb)\overline{(sb)} = |s|^2|b|^2$.
   Or $|s|^2 = \mathrm{Re}^2(s) + \mathrm{Im}^2(s) = \theta_1^2 + \theta_2^2 \leqslant 2 \times \frac{1}{2^2} = \frac{1}{2} < 1$ donc $|r|^2 < |b|^2$.
2. $\mathbb{Z}[i]$ est eucliden donc principal.

3. Structures de corps

3.1. Corps

Définition - Corps
Un corps est un anneau commutatif $(K, +, \times)$ dans lequel tous les éléments autres que 0 sont inversibles pour $\times$ c'est-à-dire que :
$(K, +, \times)$ est un corps si :
— $(K, +)$ est un groupe commutatif;
— $(K^*, \times)$ est un groupe commutatif, où 0 désigne l'élément neutre de K pour + et $K^* = K \setminus \{0\}$.
— la loi $\times$ est distributive par rapport à la loi +;

Exemple - Nombreux
Le corps $\mathbb{Q}$ est créé à partir de $\mathbb{Z}$, qui n'admet pas d'inverse, dans le but de rendre tous les éléments (sauf 0) inversibles.
De même, le corps $\mathbb{K}(X)$ des fractions rationnelles a le même rôle pour l'ensemble des polynômes $\mathbb{K}[X]$ que Q pour $\mathbb{Z}$.

Proposition - Tout élément est régulier
Un corps n'a pas de diviseurs de 0. Tout élément autre que 0 est donc régulier (on peut simplifier).

Démonstration
Si $ab = 0$, alors si $a \neq 0$, donc inversible : $b = a^{-1}ab = a^{-1}0 = 0$.
Et donc $b = 0$.
Ainsi aucun corps n'a de diviseurs de 0. □

3.2. Idéaux maximaux

Analyse - A quel condition un anneau quotient est-il un corps?
Il faut que tout élément $\overline{x}$ soit inversible. Donc qu'il existe $y \in A$ tel que $xy - 1 \in I$.
On a donc $1 \in I + (x)$ et ainsi $A = (1) \subset I + (x)$.
Nécessairement, il faut donc, pour que tout $\overline{x}$ soit inversible, que (x) ne contienne par I (sinon $I + (x) = (x) \neq A$).

Définition - Idéal maximal
Soit I un idéal de A.
On dit que I est maximal s'il $I \neq A$ et A est le seul idéal distinct de I, contenant I

Pour aller plus loin - Idéal engendré
Si I_1 et I_2 sont deux idéaux, alors $I_1 + I_2 = \{a_1 + a_2; a_1 \in I_1, a_2 \in I_2\}$ est un idéal; c'est le plus petit des idéaux qui contient à la fois I_1 et I_2.

Proposition - Corps

Soit I un idéal maximal de A. Alors $\left(\frac{A}{I}, \overline{+}, \overline{\times}\right)$ est un corps.

Remarque - Réciproque

Comme le montre l'analyse la réciproque est vrai.

Exemple - $6\mathbb{Z}$ n'est pas maximal

Les multiples de 6 sont des multiples de 3 : $6\mathbb{Z} \subset 3\mathbb{Z} \neq \mathbb{Z}$. Donc $6\mathbb{Z}$ n'est pas maximal.

D'après la réciproque : $\frac{\mathbb{Z}}{6\mathbb{Z}}$ n'est pas un corps.

Démonstration

Supposons que I est maximal.
Soit $\overline{x} \in \frac{A}{I}$.
Soit $J = I + (x)$ (plus petit idéal contenant I et (x)). Alors J est un idéal de A contenant I et différent de I (si $x \notin I$).
Or I est maximal, $J = A$ et donc $1 \in I + (x)$. Et donc il existe $a \in I$, $u \in A$ tel que $1 = a + ux$ et donc $1 = \overline{u \times x}$.
Donc $\overline{x}$ est inversible.
□

Exemple - $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec p premier

Dernier exemple et non des moindres : $\frac{\mathbb{Z}}{p\mathbb{Z}}$, avec p premier.

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \{0, 1, 2, \dots p-1\} \qquad \text{avec } u + v \equiv u + v\,[p] \text{ et } u \times v \equiv u \times v\,[p].$$

On a bien : Tout élément est inversible :
Soit $u \in \{0, 1, 2, \dots p-1\}$, et p premier, donc $u \wedge p = 1$.
D'après Bézout : il existe $a, b \in \mathbb{Z}$ tels que $au + bp = 1$, donc $au \equiv 1\,[p]$
Et donc u est inversible d'inverse a (ou son congru dans $\{0, 1, 2, \dots p-1\}$

Pour aller plus loin - Idéal premier

On dit que I est premier ssi $x \notin I$ et $y \notin I \Rightarrow xy \notin I$.
On a, par exemple, $n\mathbb{Z}$ est premier ssi n est premier.
Et plus généralement, $\frac{A}{I}$ est un anneau intègre ssi I idéal premier.
Dans le cadre de $A = \mathbb{Z}$, $\frac{A}{n\mathbb{Z}}$ est intègre ssi $\frac{A}{n\mathbb{Z}}$ est un corps…

3.3. Sous-corps. Morphisme (de corps)

Définition - Sous-corps, morphisme

On peut généraliser les définitions précédentes.
- Un sous-corps est un sous-anneau muni d'une structure de corps.
- Un morphisme de corps est un morphisme d'anneaux.
- L'image d'un corps par un morphisme de corps est un corps.

Le dernier point est un exercice à démontrer.

4. Bilan

Synthèse

⇝ Les anneaux sont les structures naturelles pour deux lois internes (addition, et multiplication, ou composition). Nous avons de nombreux exemples : $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathcal{M}_n(\mathbb{K})$…
Avec l'inversibilité de tous les éléments non nuls, la structure est encore plus riche, elle s'appelle un corps. Les exemples classiques sont $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, voire $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (p premier)

⇝ Mais pour ce dernier exemple, il faut commencer par s'assurer de la bonne définition des lois $\overline{+}$ et $\overline{\times}$, lorsqu'on passe de $\mathbb{Z}$ à $\frac{\mathbb{Z}}{n\mathbb{Z}}$.
Nous avons vu qu'il fallait que l'ensemble $n\mathbb{Z}$, soit un d'abord un idéal pour que le calcul ait un sens.
Mieux pour que $\frac{\mathbb{Z}}{n\mathbb{Z}}$ soit un corps, (il faut et)il suffit que $n\mathbb{Z}$ soit un idéal maximal (équivalent à idéal premier, dans ce contexte)

⇝ Les structures d'anneaux ou de corps, se transfère par morphisme (d'anneaux) ou par restriction.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Caractérisation des sous-anneaux
— Savoir-faire - Montrer qu'un anneau est principal

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$(A, +, \star)$ parfois A	Anneau	$(A, +)$ groupe ; $\star$ l.c.i. associative et unifère ; distributivité	Exemples courants : $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathcal{M}_n(\mathbb{K})$, $\frac{\mathbb{Z}}{n\mathbb{Z}}$
I	Idéal de A	$(I, +) < (A, +)$ & $\forall\, a \in A, x \in I,\ ax \in I$	
$(\mathbb{K}, +, \star)$ parfois $\mathbb{K}$	Corps	$(\mathbb{K}, +, \star)$ anneau, tout élément non nul inversible	Exemples courants : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $F_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$

Retour sur les problèmes

75. Cours
76. Bézout : $(a) + (b) = A$ et lemme de Gauss : $bc \in (a)$ et $(b) + (a) = A$ (a et b étrangers) alors $c \in (a)$.
77. Cours

Quatrième partie

Analyse réelle

Chapitre 18

Suites numériques

Résumé -

Les suites sont au coeur des mathématiques : il s'agit souvent d'étudier des valeurs numériques successives (i.e. dans une temporalité discrète ou paramétrée par $\mathbb{N}$). Ce sont donc des applications de $\mathbb{N}$ dans $\mathbb{C}$ (ou un sous-corps de $\mathbb{C}$).
Certaines sont classiques : les suites arithmétiques, géométriques, arithmético-géométriques, récurrentes à deux termes (par lesquelles on commence ici) ou définies implicitement, définies par une relation de récurrence (par lesquelles on termine ici). Entre ces deux types, on se concentre sur la question de la limite d'une suite. C'est un cas simple : un seule est possible et c'est toujours pour n tendant vers l'infini. On termine par étudier les propriétés topologiques de $\mathbb{R}$ (et $\mathbb{C}$) avec le langage des suites.
Quelques liens (inégaux) sur youtube :
- *netprof - Suites numériques réelles, définition. https://www.youtube.com/watch?v=Dvo4vgjRS7g*
- *[[UT#23]] - Calcul de limite - développement asymptotique. https://www.youtube.com/watch?v=T8kkTBTpM8Y*
- *Science4all - 1+2+3+4+5+... = −1/12 - https://www.youtube.com/watch?v=vMnkmBCvGQc*

Sommaire

1. Problèmes 338
2. Exemples fondamentaux 339
2.1. Suites arithmético-géométriques 339
2.2. Suites récurrentes linéaires homogène d'ordre 2 . . . 339
3. Suites extraites 340
3.1. Rappels 340
3.2. Valeur d'adhérence d'une suite 341
3.3. Application 1 : Contraire de « à partir d'un certain rang » 342
3.4. Application 2. Lemme des pics 343
4. Limite d'une suite réelle 343
4.1. Suite convergente 343
4.2. Suites divergentes 345
4.3. Opérations sur les suites/les limites et relation d'ordre 346
4.4. Extension aux suites à valeurs complexes 351
4.5. Bilan sur les théorèmes d'existence de limites 353
5. Analyse asymptotique 355
5.1. Hiérarchie de suites 355
5.2. Suites équivalentes 357
5.3. Suites dominées 363
6. Bilan 366

1. Problèmes

Problème 79 - Suite de Fibonacci

Le mathématicien italien du XIV-ième, Leonardo FIBONACCI a introduit la suite suivante définie par une double récurrence pour modéliser la reproduction des lapins :
$F_0 = F_1 = 1$ et pour tout entier $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$.
Comment calculer F_{100} ?
Il semble qu'il faut calculer tous les termes précédents, on peut exploiter un programme informatique.
Existe-t-il une formule fermée de F_n (expression directe et calculatoire de F_n directement en fonction de n) ?

Problème 80 - Forme fermée (ou forme close)

Au problème précédent, la réponse est affirmative, nous la verrons dans le cours.
De manière générale, quelles sont les types de suites pour lesquelles on peut trouver une forme fermée (expression directe en fonction de n) ?
Souvenons-nous que la définition naturelle d'une suite est plutôt sous forme d'une récurrence.
(Nous verrons une autre famille de suites importantes : celles pour lesquelles chaque terme est la solution d'une équation dépendant de n).

Problème 81 - Suites convergentes

Dans beaucoup de problèmes (au concours par exemple), il faut démontrer qu'une certaine suite converge.
Il est bon de faire la liste des méthodes. Quelles sont toutes les méthodes pour montrer qu'une suite converge ?
On se rend compte qu'il existe deux grandes familles de réponses à cette question : les méthodes qui donne également la limite et celle qui montre la convergence sans donner vraiment d'information quant à la valeur de la limite.

Problème 82 - Suite divergente vers l'infini

La somme de deux suites convergentes est une suite convergente dont la limite est la somme des deux suites qui la constituent.
Il existe également une règle avec l'une, voir les deux suites divergentes vers $+\infty$.
On peut multiplier les études en sous-cas (avec $+\infty$, avec $-\infty$, avec, avec...). Est-il possible de réunir en une seule formulation ?
On se rend compte dans ces cas là que la divergence vers l'infini est en fait plus proche de la convergence vers a que d'une divergence par absence de limite...

Problème 83 - Suite qui ne ... pas à partir d'un certain rang

Quelle stratégie mettre en place pour manipuler des suites qui ne font pas telle ou telle chose à partir d'un certain rang ?

2. Exemples fondamentaux

2.1. Suites arithmético-géométriques

On verra plus loin (lorsque nous disposerons d'autres outils) le cas des suites définies par une relation de récurrence du type $u_{n+1} = f(u_n)$.
En dehors des suites géométriques et arithmétiques, il y a quelques autres types de suites à savoir étudier.

Définition - Suites arithmético-géométrique
Une suite (u_n) (réelle ou complexe) est dite arithmético-géométrique si elle est définie par une relation de récurrence du type $u_{n+1} = au_n + b$ avec $a \neq 0, a \neq 1, b \neq 0$.

Savoir faire - Etudier une suite arithmético-géométrique
Pour étudier une telle suite,

1. on cherche un point fixe c : tel que $c = ac + b$
2. on introduit la suite $(v_n) = (u_n - c)$. Elle est géométrique de raison a.

On a donc $u_n = a^n(u_0 - c) + c$

Exercice
Etudier la suite définie par $u_0 = 1$ et $u_{n+1} = \frac{1}{2}u_n - \frac{2}{3}$.

Correction
Soit c tel que $c = \frac{1}{2}c - \frac{2}{3}$, donc $c = -\frac{4}{3}$.
Puis $v_n = u_n - c$, donc $v_{n+1} = u_{n+1} - c = \frac{1}{2}u_n - \frac{2}{3} - \frac{1}{2}c + \frac{2}{3} = \frac{1}{2}v_n$.
Par conséquent $v_n = \frac{1}{2^n}v_0 = \frac{1}{2^n}(1 + \frac{4}{3}) - \frac{4}{3} = \frac{1}{3}(\frac{2}{2^n} - 4)$

2.2. Suites récurrentes linéaires homogène d'ordre 2

Définition - Suites récurrentes linéaires homogène d'ordre 2
On appelle suite récurrente linéaire homogène d'ordre 2 toute suite $(u_n) \in \mathbb{K}^{\mathbb{N}}$ ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) définie par

$$u_0, u_1 \in \mathbb{K} \quad \text{et} \quad \forall n \in \mathbb{N}, \quad au_{n+2} + bu_{n+1} + cu_n = 0$$

où $(a, b, c) \in \mathbb{K}^3$, $a \neq 0, c \neq 0$.
On lui associe une équation dite caractéristique : $ax^2 + bx + c = 0$

Théorème - Etude des suites récurrentes linéaires d'ordre 2
Notons $\Delta = b^2 - 4ac$, le discriminant de l'équation caractéristique.
Pour $\mathbb{K} = \mathbb{C}$ (a, b, c complexes) :

— si $\Delta \neq 0$ et r_1, r_2 racines de l'équation caractéristique,

$$E = \{\lambda(r_1^n)_{n\in\mathbb{N}} + \mu(r_2^n)_{n\in\mathbb{N}}; (\lambda, \mu) \in \mathbb{C}^2\}$$

— si $\Delta = 0$ et r unique racine,

$$E = \{\lambda(r^n)_{n\in\mathbb{N}} + \mu(nr^n)_{n\in\mathbb{N}}; (\lambda, \mu) \in \mathbb{C}^2\}$$

Pour $\mathbb{K} = \mathbb{R}$ (a, b, c réels) :

— si $\Delta > 0$ et r_1, r_2 racines de l'équation caractéristique,

$$E = \{\lambda(r_1^n)_{n\in\mathbb{N}} + \mu(r_2^n)_{n\in\mathbb{N}}; (\lambda, \mu) \in \mathbb{R}^2\}$$

— si $\Delta = 0$ et r unique racine,

$$E = \{\lambda(r^n)_{n\in\mathbb{N}} + \mu(nr^n)_{n\in\mathbb{N}}; (\lambda, \mu) \in \mathbb{R}^2\}$$

— si $\Delta < 0$ et $r = \rho e^{i\theta}, \bar{r}$ racines complexes,

$$E = \{\lambda(\mathrm{Re}(r^n))_{n\in\mathbb{N}} + \mu(\mathrm{Im}(r^n))_{n\in\mathbb{N}}; (\lambda, \mu) \in \mathbb{C}^2\}$$

$$= \{\lambda(\rho^n \cos n\theta)_{n\in\mathbb{N}} + \mu(\rho^n \sin n\theta)_{n\in\mathbb{N}}; (\lambda, \mu) \in \mathbb{R}^2\}$$

Pour aller plus loin - Méthode américaine
Si on note r_1 et r_2 les racines de l'équation caractéristique.

1. *On considère $f(x) = \sum_{n=0}^{+\infty} u_n x^n$, alors $(a+bx+cx^2)f(x) = a(u_0+u_1x)+bu_0x+\sum_{n=0}^{+\infty}(au_{n+2} + bu_{n+1} + cu_n)x^{n+2} = a(u_0 + u_1x) + bu_0x$.*
2. *On pratique une décomposition en élément simple : $f(x) = \frac{au_0+(au_1+bu_0)x}{a(1+r_1x)(1+r_2x)} = \frac{A}{1+r_1x} + \frac{B}{1+r_2x} = \sum_{n=0}^{+\infty}(Ar_1^n + Br_2^n)x^n$.*
3. *Puis on peut identifier $u_n = Ar_1^n + Br_2^n$*

Savoir faire - Etudier une suite récurrente linéaire d'ordre 2
Pour étudier une telle suite,

1. on définit l'équation caractéristique associée
2. on calcule le discriminant :
   — Si $\Delta > 0$, les racines sont r_1 et r_2,
   $\exists A_1, A_2 \in \mathbb{R}$ tels que $\forall n \in \mathbb{N}$, $u_n = A_1 r_1^n + A_2 r_2^n$.
   — Si $\Delta = 0$, la racine double est r
   $\exists A_1, A_2 \in \mathbb{R}$ tels que $\forall n \in \mathbb{N}$, $u_n = (A_1 + A_2 n)r^n$.
   — Si $\Delta < 0$, les racines sont $r_1 = \rho e^{i\theta}$ et $r_2 = \rho e^{-i\theta}$,
   $\exists A \in \mathbb{C}$ tels que $\forall n \in \mathbb{N}$, $u_n = Ar_1^n + \overline{A}r_2^n$. $\exists A_1, A_2 \in \mathbb{R}$ tels que $\forall n \in \mathbb{N}$, $u_n = \rho^n(A_1\cos(n\theta) + A_2\sin(n\theta))$.

Savoir faire - Et s'il y a un second membre?
La résolution se fait comme pour les EDL2 à coefficients constants.

1. On cherche une solution particulière (de la même forme que le second membre et par tâtonnement)
2. On cherche l'ensemble des solutions du problème homogène

L'ensemble des solutions est la somme (affine) de la solution particulière et de l'espace des solutions du problème homogène (ce qui forme un espace affine).

Remarque - Démonstrations
Il existe au moins trois démonstrations classiques de ce résultat :
— par récurrence. On peut le faire (mais attention à la question de l'unicité de la suite)
— par la force de l'algèbre linéaire. Nous ferrons cette démonstration dans le cours d'algèbre linéaire (second semestre)
— par les séries géométriques (voir plus loin)

3. Suites extraites

3.1. Rappels

La définition a déjà été donnée, il s'agit de considérer seulement certains éléments (mais en nombre inifini) de (u_n), une suite donnée.

Définition - Suite extraite
On dit que (v_n) est une suite extraite de (u_n) (ou une sous-suite),
si $\exists \varphi : \mathbb{N} \to \mathbb{N}$, strictement croissante telle que $\forall n \in \mathbb{N}$, $v_n = u_{\varphi(n)}$.

Exemple - Extraction paire
Avec $\varphi : n \mapsto 2n$, strictement croissante, on trouve que le k-ième terme de (v_n) est $v_k = u_{2k} = u_{2k}$, le 2k-ième terme de (u_n).

Attention - Double extraction
Si (w_n) est une extraction de (v_n), elle-même une extraction de u_n,
$\exists\, \varphi_1, \varphi_2$ tel que $\forall\ n \in \mathbb{N}$, $w_n = v_{\varphi_2(n)}$ et $v_n = u_{\varphi_1(n)}$,
et donc $\forall\ n \in \mathbb{N}$, $w_n = v_{\varphi_2(n)} = u_{\varphi_1(\varphi_2(n))}$, l'extractrice est donc $\varphi_1 \circ \varphi_2$.

On a vu également (élargi ici) :

Proposition - Sous-ensemble infini et suite extraite
Soit $A \subset \mathbb{R}$, on a les équivalences :

i. $\{n \in \mathbb{N} \mid u_n \in A\}$ est infini

ii. $\{n \in \mathbb{N} \mid u_n \in A\}$ n'est pas majoré

iii. $\exists\, (v_n)$ extraite de (u_n) telle que $\forall\ n \in \mathbb{N}$, $v_n \in A$

iv. $\exists\, \varphi : \mathbb{N} \to \mathbb{N}$ ↗↗ telle que pour tout $n \in \mathbb{N}$, $u_{\varphi(n)} \in A$

On dit (en probabilité, en particulier) que $u_n \in A$ infiniment souvent, écris : $(u_n) \in Ai.s.$ (ou $(u_n) \in Ai.o.$ (infinitely often)).

Démonstration
Clairement, on a $[i.] \Leftrightarrow [ii.]$ et $[iii.] \Leftrightarrow [iv.]$.
$[iv.] \Rightarrow [i.]$ car si $[iv.]$ est vraie alors $\{\varphi(n), n \in \mathbb{N}\} \subset A$ et $\{\varphi(n), n \in \mathbb{N}\}$ est infini. Donc A également.
Réciproquement, supposons que $N := \{n \in \mathbb{N} \mid u_n \in A\}$ est infini.
Notons $i_0 = \min N$, car N est non vide. $v_0 = u_{i_0} \in A$.
Définissons par récurrence (au rang $k \in \mathbb{N}$), le nombres entiers $i_0, i_1, \dots i_k$ définis dans N est formant une suite croissante,
$N_k = N \setminus \{i_0, i_1, \dots i_k\}$, est infini (sinon N serait fini) et $i_{k+1} = \min(N_k)$.
La suite (i_k) ainsi obtenue est croissante, car $N_k = N_{k+1} \uplus \{i_k\}$ et que $i_k = \min N_k$, donc $\forall\ h \in N_{k+1}$, $i_k < h$.
Or $i_{k+1} \in N_{k+1}$ donc avec $h \leftarrow i_{k+1}$, on a donc $i_k < i_{k+1}$.
On peut prendre pour extraction : $\varphi : \mathbb{N} \to \mathbb{N}$, $k \mapsto i_k$, strictement croissante et $u_{\varphi(k)} = u_{i_k} \in A$ car $i_k \in N$. □

Remarque - Dans la démonstration…
Pour l'implication $[i.] \Rightarrow [iv.]$, on a refusé d'écrire : « A est infini, inclus dans $\mathbb{N}$, donc dénombrable ou énumérable.

$$A = \{i_0, i_1, i_2, i_3 \dots\}$$

Et il suffit de prendre $\varphi : n \mapsto i_n$. » Pour deux raisons, rien ne prouve que l'énumération est croissante (pour $\mathbb{Q}$ dénombrable, c'est par exemple compliqué) et ensuite, cela serait une tautologie : il faudrait bien démontrer ce résultat une fois pour toute. La démonstration proposée donne donc cette démonstration « une fois pour toute ».

3.2. Valeur d'adhérence d'une suite

Définition - Valeur d'adhérence (d'une suite)
Si a est limite d'une suite extraite de (u_n), alors, on dit que a est une valeur d'adherence de la suite (u_n).

Théorème - Limite d'une suite extraite
Toute suite extraite d'une suite tendant vers $\ell \in \overline{\mathbb{R}}$ est une suite tendant vers $\ell \in \overline{\mathbb{R}}$.
Autrement écrit : si $(u_n) \to \ell$, alors (u_n) n'admet qu'une seule valeur d'adhérence : ℓ.

Démonstration
Si (u_n) est proche de ℓ à ϵ près à partir d'un certain rang N,
il en est de même de $(u_{\varphi(n)})$ à partir du rang $\min\{n \mid \varphi(n) \geqslant N\} \in \mathbb{N}$, non vide. □

3.3. Application 1 : Contraire de « à partir d'un certain rang »

Analyse - Contraire de : « A partir d'un certain rang »
Souvent, pour B un ensemble donné, on rencontre la négation de :

$$\exists\, N \in \mathbb{N} \text{ tel que } \forall\ n \geqslant N, u_n \in B$$

on a donc :

$$\forall\ N \in \mathbb{N}, \exists\, n \geqslant N, u_n \notin B$$

On peut alors exploiter les suites extraites, car on a : $\exists\, \varphi$ ↗↗ telle que $\forall\ n \in \mathbb{N}$, $\varphi(n) \notin B$.

Théorème - Suite extraite
Soit (u_n) une suite numérique et $B \subset \mathbb{R}$.
Si on n'a pas : $\exists\, N \in \mathbb{N}$ tel que pour tout $n \in \mathbb{N}$, $u_n \in B$,
i.e. on a : $\forall\ N \in \mathbb{N}, \exists\, n \geqslant N, u_n \notin B$
Alors, il existe une sous-suite (v_n) de (u_n) tel que pour tout $n \in \mathbb{N}$, $v_n \notin B$

Démonstration
On note $A = \overline{B}$, le complémentaire de B.
Alors si on a $\forall\ N \in \mathbb{N}, \exists\, n \geqslant N$, tel que $u_n \notin B$, i.e. $u_n \in A$.
Alors $N := \{n \in \mathbb{N} \mid u_n \in A\}$ n'est pas majoré et on applique le théorème précédent. □

Exemple - Non suite nulle à partir d'un certain rang
On note $B = \{0\}$.
On n'a pas : (u_n) nulle à partir d'un certain rang :
Donc régulièrement (infiniment souvent) : u_n est non nul.
Formellement : $\forall\ N \in \mathbb{N}, \exists\, n \geqslant N$ tel que $u_n \neq 0$.
Avec le théorème, il existe φ ↗↗ tel que $\forall\ n \in \mathbb{N}$, $u_{\varphi(n)} \neq 0$.
Il ne faut pas confondre avec :
(u_n) non nulle à partir d'un certain rang, i.e. $\exists\, N \in \mathbb{N}, \forall\ n \geqslant N, u_n \neq 0$.

On exploite aussi des suites extraites pour étudier des suites non majorées :

Proposition - Suite non majorée
(u_n) n'est pas majorée ssi il existe une suite extraite de (u_n) tendant vers $+\infty$.
i.e. il existe $\varphi : \mathbb{N} \to \mathbb{N}$, ↗↗ telle que $(u_{\varphi(n)}) \to +\infty$

Démonstration
S'il existe une suite extraite tendant vers l'infini, alors nécessairement (u_n) ne peut pas être bornée.
Réciproquement, si (u_n) n'est pas majorée, elle n'est pas majorée à partir d'un certain rang.
$\forall\ M \in \mathbb{N}, \forall\ N \in \mathbb{N} \exists\, n \geqslant N$ tel que $u_n \geqslant M$.
En notant $B = [M, +\infty[$, il existe une suite φ ↗↗ tel que $(u_{\varphi(n)}) \geqslant M$.
Pour tout $M \in \mathbb{R}$, il existe une suite φ ↗↗ tel que $(u_{\varphi(n)}) \geqslant M$.
C'est la même chose, que (u_n) admet une suite extraite tendant vers $+\infty$. □

Exercice
Soit (u_n) une suite à valeurs dans $[a, b]$.
Soient $\epsilon > 0$ et $n = \left\lfloor \dfrac{b-a}{\epsilon} \right\rfloor$

1. $[a, b]$ peut s'écrire comme une réunion de n intervalles de taille inférieur à $\epsilon > 0$.

2. Montrer qu'il existe un ensemble $A \subset [a,b]$, de taille inférieur à ϵ et une suite extraite de (u_n) tel que pour tout $n \in \mathbb{N}$, $u_{\varphi(n)} \in A$

Correction

1. On note pour tout $k \in \mathbb{N}_n$, $I_k = [a+(k-1)\epsilon, a+k\epsilon]$.
   Alors I_k est de taille égale à ϵ. Il y a n intervalles I_k. Et $\bigcup_{k\in\mathbb{N}_n} I_k = [a, a+n\epsilon]$.
   Or $n\epsilon \geqslant \dfrac{b-a}{\epsilon}\epsilon = b-a$.
2. Si pour tout $k \in \mathbb{N}$, il existe $N_k \in \mathbb{N}$ tel que $\forall\, n \geqslant N_k$, $u_n \notin I_k$,
   Alors en prenant $N = \max N_k$, on a pour tout $n \geqslant N$, $u_n \notin I_k$, donc $u_n \notin \bigcup I_k = [a,b]$.
   Impossible.
   Ainsi, par l'absurde, il existe $k \in \mathbb{N}$ tel que $\forall\, N \in \mathbb{N}$, $\exists\, n \geqslant N$, tel que $u_n \in I_k$.
   Donc il existe $\varphi \nearrow\nearrow$ tel que $(u_{\varphi(n)}) \in I_k =: A$.

3.4. Application 2. Lemme des pics

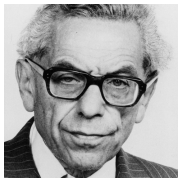
Proposition - Lemme des pics
Soit E, un ensemble totalement ordonné.
Toute suite de E admet une sous-suite croissante ou une sous-suite décroissante.

C'est encore plus fin ici, car l'ensemble A n'est pas fixe, d'une certaine façon… On travaille donc sur N directement et on doit adapter la démonstration.

Démonstration
On note $N = \{n \in \mathbb{N} \mid \forall\, m > n, u_n \leqslant u_m\}$.
• Ou bien N est fini, et donc est majoré par n_0.
Ainsi pour tout $n \geqslant n_0$, $n \notin N$, i.e. : $\exists\, m > n$, $u_n \geqslant u_m$.
Considérons $\psi : n \mapsto \min\{m > n \mid u_n \geqslant u_m\}$, bien définie.
Puis $j_k = \underbrace{\psi \circ \cdots \psi}_{k \text{ fois}}(n_0)$.
Donc la suite $(u_{j_k})_k$ est décroissante.
• Ou bien N est infini, et donc on construit une suite (i_k) strictement croissante d'éléments de N par récurrence :
$i_0 = \min N$ et $i_{k+1} = \min(N \setminus \{i_0, i_1, \dots i_k\})$, non vide (sinon N fini).
$I_k = I_{k+1} \uplus \{i_k\}$ et donc $i_{k+1} \geqslant i_k$ et par construction $u_{i_k} \leqslant u_{i_{k+1}}$.
Donc $(u_{i_k})_k$ est une suite croissante. □

Remarque - Le lemme de Erdös-Szekeres
LE DS10 2020-2021 donne un algorithme pour trouver, à partir d'une suite finie de $pq+1$ éléments ou bien une suite extraite croissante de $p+1$ éléments ou une suite décroissante de $q+1$ éléments.
Une forme d'optimalité finie.

Histoire - Paul Erdös



Paul Erdös (1913-1996) est un mathématicien hongrois en exil permanent. Très prolifique, il s'intéresse à l'arithmétique, théorie des graphes et probabilités ou encore l'analyse. Un de ses leitmotivs : « Another roof, another proof ». Il campait chez l'un ou l'autre des mathématiciens quelques jours pour trouver des résultats intéressants, puis il s'en allait.
Une autre citation intéressante : « Il faut parfois compliquer un problème pour en simplifier la solution. »
On peut lire : Erdös, l'homme qui n'aimait que les nombres.

4. Limite d'une suite réelle

4.1. Suite convergente

Heuristique - Expression en français
On dit qu'une suite (u_n) converge vers ℓ,
si à toute précision fixée a priori et notée ϵ,
la suite u_n est proche de ℓ à ϵ près, à partir d'un certain rang…

Définition - Limite (réelle)
Soit (u_n) une suite réelle et $\ell \in \mathbb{R}$. On dit que la suite (u_n) converge vers ℓ

lorsque
$$\forall \epsilon > 0, \exists N \in \mathbb{N} \mid \forall\, n \geqslant N, |u_n - \ell| \leqslant \epsilon$$

Remarque - Suite convergente vers 0
On a $(u_n) \underset{n\to+\infty}{\longrightarrow} \ell \iff (u_n - \ell) \underset{n\to+\infty}{\longrightarrow} 0$.
On pourrait donc restreindre notre cours à l'étude des suites convergentes vers 0.

Remarque - Strict ou non
On a aussi $(u_n) \underset{n\to+\infty}{\longrightarrow} \ell$ si et seulement si
$$\forall \epsilon > 0, \exists N \in \mathbb{N} \mid \forall\, n \geqslant N, |u_n - \ell| < \epsilon$$

Exercice

Soit $\alpha > 0$. Montrer à l'aide de la définition que la suite $\left(\dfrac{1}{n^\alpha}\right)$ converge vers 0.

Correction
Soit $\epsilon > 0$.
$$\left|\frac{1}{n^\alpha} - 0\right| < \epsilon \longleftarrow n > \epsilon^{-1/\alpha}$$
Et donc en prenant $N = \lfloor \epsilon^{-1/\alpha} \rfloor + 1$, on voit que la suite vérifie le critère de convergence vers 0.

Attention - Dépendance de N à ϵ
On remarquera bien sur cet exercice le fait important et fréquent :
N dépend de la valeur de ϵ choisie a priori.
On pourrait noter à la physicienne : $N(\epsilon)$

Proposition - Unicité de la limite
Soit (u_n) une suite réelle. Si (u_n) converge vers ℓ et vers ℓ', alors $\ell = \ell'$.
On note alors $(u_n) \underset{n\to+\infty}{\longrightarrow} \ell$ ou $\lim_{n\to+\infty} u_n = \ell$.

Démonstration
Soit $\epsilon > 0$.
$$\exists\, N_1, N_2 \mid \forall\, n \geqslant N_1, |u_n - \ell| < \frac{\epsilon}{2} \text{ et } \forall\, n \geqslant N_2, |u_n - \ell'| < \frac{\epsilon}{2}$$
Soit $N = \max(N_1, N_2)$, donc par inégalité triangulaire :
$$|\ell - \ell'| = |(\ell - u_N) + (u_N - \ell')| \leqslant |\ell - u_N| + |u_N - \ell'| \leqslant \epsilon$$
Ceci est vrai pour tout ϵ, donc $|\ell - \ell'| = 0$ i.e. $\ell = \ell'$. □

Définition - Suites convergente, divergente
Soit (u_n) une suite réelle.
S'il existe un réel ℓ tel que la suite converge vers ℓ, on dit que (u_n) est convergente.
ℓ (unique d'après ce qui précède) est appelé la limite de la suite.

Proposition - Suite convergente donc bornée
Toute suite convergente est bornée.

Démonstration
Si (u_n) converge vers ℓ.
Alors (u_n) est majorée par $\ell+1$ à partir d'un certain rang et minorée par $\ell-1$ à partir d'un certain rang.
Donc (u_n) est bornée. □

4.2. Suites divergentes

Il y a deux types de non convergence (=divergence) :
- les suites tendant vers ∞ (premier type de divergence - en fait convergence dans $\overline{\mathbb{R}}$).
- les suites ne tendant vers rien (deuxième type de divergence).

Définition - divergente
Si la suite n'est pas convergente on dit qu'elle est divergente.

On peut étendre la notion de limite d'une suite à $\overline{\mathbb{R}}$ ce qui donne la définition suivante.

Définition - Limite infinie
On dit que la suite réelle (u_n) tend vers $+\infty$ et on note $u_n \underset{n\to+\infty}{\longrightarrow} +\infty$, si

$$\forall A \in \mathbb{R}, \exists N \in \mathbb{N} \,|\, \forall n \geqslant N,\ u_n \geqslant A.$$

On dit que la suite réelle (u_n) tend vers $-\infty$ et on note $u_n \underset{n\to+\infty}{\longrightarrow} -\infty$, si

$$\forall A \in \mathbb{R}, \exists N \in \mathbb{N} \,|\, \forall n \geqslant N,\ u_n \leqslant A.$$

Remarque - Limite infinie et suite divergente
- Une suite admettant une limite infinie est une suite divergente. On ecrit toutefois $\lim\limits_{n\to+\infty} u_n = +\infty(-\infty)$ lorsque $(u_n) \underset{n\to+\infty}{\longrightarrow} +\infty(-\infty)$ et on dit que la suite diverge vers $+\infty$ $(-\infty)$.
- Si (u_n) tend vers $+\infty$ ou $-\infty$, alors $(|u_n|)$ tend vers $+\infty$.

Exercice
Soit $\alpha > 0$. Montrer à l'aide de la définition que la suite (n^α) diverge vers $+\infty$.

Correction
Soit $A > 0$.

$$n^\alpha > A \longleftrightarrow n > A^{1/\alpha}$$

Et donc en prenant $N = \lfloor A^{1/\alpha} \rfloor + 1$, on voit que la suite vérifie le critère de divergence vers $+\infty$.

Attention - Dépendance de N à A
On remarquera bien sur cet exercice le fait important et fréquent :
N dépend de la valeur de A choisie a priori.
On pourrait noter à la physicienne : $N(A)$

Attention - Cas pathologiques
Il existe
- des suites divergentes qui ne tendent pas vers $+\infty$ (ni vers $-\infty$) ;
- des suites non bornées qui ne divergent pas vers $+(-)\infty$.
- des suites convergentes non monotones.

Savoir faire - Montrer la divergence (deuxième type) d'une suite, par suites extraites
Soit (u_n) une suite réelle.
On suppose qu'il existe deux suites extraites $(u_{\varphi(n)})$ et $(u_{\psi(n)})$ convergeant respectivement vers ℓ et ℓ', avec $\ell \neq \ell'$. Alors la suite (u_n) est divergente.

Exercice
Donner des exemples de telles suites

Correction
Premier contre-exemple : $\left((-1)^n\right)$.
Deuxième contre-exemple : $\left((-1)^n n\right)$.
Premier contre-exemple : $\left(\frac{(-1)^n}{n}\right)$.

Exercice
Rappeler et démontrer les résultats sur la convergence des suites arithmétiques ou géométriques en fonction de leur raison.

Correction
Sauf si la raison vaut r, la suite arithmétique diverge vers $+\infty$ (si $r > 0$ et vers $-\infty$ (si $r < 0$).
La suite géométrique de raison q :
- converge vers 0 ssi $q \in]-1, 1[$ ou $u_0 = 0$
- est constant égale à u_0 si $q = 1$
- diverge vers $+\infty$ si $q > 1$ et $u_0 > 0$, et vers $-\infty$ si $q > 1$ et $u_0 < 0$,
- diverge (vers rien) si $q < -1$.

4.3. Opérations sur les suites/les limites et relation d'ordre

Ordre et limites

Proposition - Convergence et signe de la suite
Soit (u_n) une suite réelle qui tend vers $\ell \in \overline{\mathbb{R}}$. On suppose $\ell > 0$ (resp. $\ell < 0$). Alors la suite est strictement positive (resp. strictement négative) à partir d'un certain rang.

Démonstration
On suppose $\ell > 0$, on considère $\epsilon = \frac{\ell}{2}$.
A partir d'un certain rang : $|u_n - \ell| < \frac{\ell}{2}$, donc $\ell - \frac{\ell}{2} < u_n < \ell + \frac{\ell}{2}$.
Donc à partir d'un certain rang : $u_n > \frac{\ell}{2} > 0$. □

Et réciproquement, si $u_n > 0$, a-t-on $\lim(u_n) > 0$?

Attention - Les inégalités sont élargies!
Les inégalités strictes ne passent pas à la limite, elles se transforment en inégalités larges.
Par exemple $u_n = \frac{1}{n} > 0 = v_n$ et pourtant $\lim(u_n) = \lim(v_n) = 0$

Théorème - Passage à la limite dans les inégalités
Soient (u_n) et (v_n) deux suites réelles qui convergent respectivement vers les réels ℓ et ℓ'. On suppose qu'à partir d'un certain rang on a $u_n \leqslant v_n$. Alors $\ell \leqslant \ell'$.

Remarque - Dans $\overline{\mathbb{R}}$
Le résultat reste vrai avec des suites ayant des limites dans $\overline{\mathbb{R}}$.

Démonstration
$\ell' - \ell = (\ell' - v_n) + (v_n - u_n) + (u_n - \ell)$.
Pour tout $\epsilon > 0$, il existe $N \in \mathbb{N}$ (max) tel que $\forall\ n \geqslant N$:
$\ell - v_n > -\epsilon$, $v_n - u_n \geqslant 0$ et $u_n - \ell > -\epsilon$.
Donc (pour tout $n \geqslant N$) $\ell' - \ell \geqslant -2\epsilon$.
Ceci est vrai pour tout $\epsilon > 0$: $\ell' - \ell \geqslant 0$. □

Heuristique - Petit bilan… et mieux!
Dans le cadre des suites convergentes dans $\overline{R}$, on peut résumer d'une certaine façon, ce qu'on a vu en :
- Le passage à la limite conserve l'ordre large.
- Réciproquement (strict) : si $\lim u_n < \lim v_n$, alors $u_n < v_n$ à partir d'une certain rang.

, Le théorème d'encadrement est un peu plus fort : il assure aussi la convergence.

Théorème - Théorème de convergence par encadrement, dit "des gendarmes"
Soient $(u_n),(v_n),(w_n)$ trois suites réelles et $\ell\in\mathbb{R}$. On suppose que

$$\forall n\geqslant n_0, u_n\leqslant v_n\leqslant w_n, \text{ et que } \lim_{n\to+\infty}u_n=\lim_{n\to+\infty}w_n=\ell$$

alors la suite (v_n) converge vers ℓ.

Avec $(u_n)=(-w_n)$:

Corollaire - Encadrement en valeur absolue
Soit (u_n) une suite réelle. On suppose que l'on a (α_n) une suite de réels positifs qui converge vers 0 et un réel ℓ tels qu'à partir d'un certain rang $|u_n-\ell|\leqslant\alpha_n$. Alors (u_n) converge vers ℓ.

Démonstration
Soit $\epsilon>0$.
A partir d'un certain rang :

$$\ell-\epsilon<u_n<v_n<w_n<\ell+\epsilon$$

donc $|v_n-\ell|<\epsilon$ □

Savoir faire - A partir de deux certains rangs
Si on a, à partir d'un certain premier rang une propriété vraie : $\exists\, n_1\in\mathbb{N}$ tel que $\forall\ n\geqslant n_1, \mathscr{P}_n$.
Et à partir d'un certain second rang une propriété vraie : $\exists\, n_2\in\mathbb{N}$ tel que $\forall\ n\geqslant n_1, \mathscr{P}'_n$.
Alors, à partir d'un certain (autre) rang : $n_3=\max(n_1,n_2)$, $\forall\ n\geqslant n_3$, $\mathscr{P}_n$ et $\mathscr{P}'_n$ sont vraies.

Exercice

Montrer que la suite $\left(\frac{2^n}{n!}\right)$ converge vers 0.

Correction

Pour $n\geqslant 4$, $0\leqslant\frac{2^n}{n!}=\frac{2}{n}\frac{2}{n-1}\times\cdots\frac{2}{4}\frac{2}{3}\frac{2}{2}\frac{2}{1}\leqslant\frac{4}{3n}$.
Donc par encadrement, la suite considérée converge ers 0.

On a un résultat analogue au théorème précédent pour les limites infinies.

Théorème - Théorème de divergence (vers $\pm\infty$) par encadrement
Soient (u_n) et (v_n) deux suites réelles telles qu'à partir d'un certain rang $u_n\leqslant v_n$. Alors

$$(u_n)\underset{n\to+\infty}{\longrightarrow}+\infty\Rightarrow(v_n)\underset{n\to+\infty}{\longrightarrow}+\infty \tag{18.1}$$

$$(v_n)\underset{n\to+\infty}{\longrightarrow}-\infty\Rightarrow(u_n)\underset{n\to+\infty}{\longrightarrow}-\infty \tag{18.2}$$

Exercice

Soit (S_n) la suite définie par $S_n=\sum_{k=2}^{n}\frac{1}{k}$.

1. Pour $k\in\mathbb{N}^*$, comparez $\frac{1}{k}$ avec $\int_k^{k+1}\frac{\mathrm{d}t}{t}$ et $\int_{k-1}^{k}\frac{\mathrm{d}t}{t}$. En déduire que (S_n) diverge.
2. Prouver que $\left(\frac{S_n}{\ln n}\right)$ converge et donner sa limite.

Correction
C'est un résultat classique, à connaître.

1. La fonction $t\mapsto\frac{1}{t}$ est décroissante, donc pour tout $t\in[\![k,k+1]\!]$, $\frac{1}{k+1}\leqslant\frac{1}{t}\leqslant\frac{1}{k}$.
Puis on intègre pour t entre k et $k+1$, aux extrémités il s'agit de constante :

$$\frac{1}{k+1}\leqslant\int_k^{k+1}\frac{\mathrm{d}t}{t}\leqslant\frac{1}{k}$$

Un changement d'indice permet d'affirmer : $\int_k^{k+1}\frac{\mathrm{d}t}{t}\leqslant\frac{1}{k}\leqslant\int_{k-1}^{k}\frac{\mathrm{d}t}{t}$.
On peut alors sommer ces inégalités pour k de 2 à n et appliquer la formule de Chasles :

$$\ln(n+1)-\ln 2=\int_2^{n+1}\frac{\mathrm{d}t}{t}\leqslant S_n\leqslant\int_1^n\frac{\mathrm{d}t}{t}=\ln n$$

La minoration de S_n par une suite divergente vers $+\infty$ permet d'affirmer la divergence de (S_n).

2. On divise donc par $\ln n$: mais après avoir noté : $\ln(n+1)=\ln(n(1+\frac{1}{n}))=\ln n+\ln(1+\frac{1}{n})$:

$$1+\frac{\ln(\frac{1}{2}+\frac{1}{2n})}{\ln n}\frac{S_n}{\ln n}\leqslant 1$$

Et comme : $\lim\ln(\frac{1}{2}+\frac{1}{2n})=0$, alors $\lim 1+\frac{\ln(\frac{1}{2}+\frac{1}{2n})}{\ln n}=1$ et par encadrement : $\left(\frac{S_n}{\ln n}\right)$ converge vers 1.

Savoir faire - Convergence par encadrement/Divergence par minoration (majoration)
L'encadrement est souvent à la base de toute démonstration d'analyse.
Pour démontrer que $u_n\to\ell$, on démontre qu'à partir d'un certain rang
$v_n\leqslant u_n\leqslant w_n$ avec $\lim(v_n)=\lim(w_n)=\ell$.
ou $|u_n-\ell|\leqslant\alpha_n$ avec $\lim(\alpha_n)=0$.
Pour démontrer que $u_n\to+\infty$, on démontre qu'à partir d'un certain rang, $u_n\geqslant v_n$ et $v_n\to+\infty$.
Pour $u_n\to-\infty$, on démontre qu'à partir d'un certain rang, $u_n\leqslant w_n$ et $w_n\to-\infty$.

Opérations sur les limites

Définition - $\mathbb{R}^{\mathbb{N}}$ comme une algèbre
On définit les opérations suivantes sur l'ensemble des suites réelles :
• Addition : $(u_n)+(v_n)=(u_n+v_n)$
• Multiplication par un réel : $\lambda(u_n)=(\lambda u_n)$
• Multiplication de deux suites : $(u_n)\times(v_n)=(u_n\times v_n)$
Addition et multiplication de deux suites sont des "lois internes" sur $\mathbb{R}^{\mathbb{N}}$, la multiplication est une "loi externe".

On commence par deux lemmes qui simplifieront les démonstrations

Lemme -
Soient (u_n) et (v_n) deux suites numériques.
— Si $(u_n)\to 0$ et (v_n) est bornée, alors $(u_n\times v_n)\to 0$.
— Si $(u_n)\to+\infty$ et (v_n) est minorée, alors $(u_n+v_n)\to+\infty$

Démonstration
• Soit $\epsilon > 0$.
(v_n) est bornée, donc il existe $M \in \mathbb{R}_+$ tel que $\forall\ n \in \mathbb{N}, |v_n| \leqslant M$.
(u_n) converge vers 0, donc il existe N tel que, pour tout $n \geqslant N$, $|u_n| \leqslant \frac{\epsilon}{M}$.
Ainsi pour tout $n \geqslant N$, $|u_n \times v_n| \leqslant \frac{\epsilon}{M} M = \epsilon$.
Donc $(u_n v_n) \to 0$ • Soit $A > 0$ (v_n) est minorée, donc il existe $A' \in \mathbb{R}$ tel que $\forall\ n \in \mathbb{N}$, $v_n \geqslant A'$.
(u_n) diverge vers $+\infty$, donc il existe N tel que, pour tout $n \geqslant N$, $u_n \geqslant A - A'$.
Ainsi pour tout $n \geqslant N$, $u_n + v_n \geqslant (A - A') + A' = A$.
Donc $(u_n + v_n) \to +\infty$ □

Théorème - Opérations sur les limites
Soit (u_n) une suite tendant vers $\ell \in \overline{\mathbb{R}}$ et (v_n)une suite tendant vers $\ell' \in \overline{\mathbb{R}}$.
Alors, lorsque le calcul dans $\overline{\mathbb{R}}$ a du sens :
• la suite $(|u_n|)$ tend vers $|\ell|$;
• la suite $(u_n + v_n)$ tend vers $\ell + \ell'$;
• pour $\lambda \in \mathbb{R}$, la suite (λu_n) tend vers $\lambda \ell$;
• la suite $(u_n v_n)$ tend vers $\ell \ell'$;
• si $\ell' \neq 0$, la suite $(\frac{u_n}{v_n})$ tend vers $\frac{\ell}{\ell'}$

Savoir faire - A savoir compléter
Plus généralement les tableaux suivants, complétés, permettent de connaître les limites des suites $(u_n + v_n)$, $(u_n v_n)$, $(\frac{1}{u_n})$, $(\frac{u_n}{v_n})$ connaissant les limites, éventuellement infinies, des suites (u_n) et (v_n).
ℓ et ℓ' sont des réels.

1. **Limite d'une somme**

(u_n) a pour limite	ℓ	ℓ	ℓ	$+\infty$	$-\infty$	$+\infty$
(v_n) a pour limite	ℓ'	$+\infty$	$-\infty$	$+\infty$	$-\infty$	$-\infty$
alors $(u_n + v_n)$ a pour limite						

2. **Limite d'un produit**

(u_n) a pour limite	ℓ	$\ell \neq 0$	0	∞
(v_n) a pour limite	ℓ'	∞	∞	∞
alors $(u_n v_n)$ a pour limite				

Pour déterminer s'il s'agit de $+\infty$ ou de $-\infty$ on applique la règle des signes.

3. **Limite de l'inverse**

(u_n) a pour limite	$\ell \neq 0$	0 avec $u_n > 0$	0 avec $u_n < 0$	∞
alors $(\frac{1}{u_n})$ a pour limite				

4. **Limite d'un quotient**

(u_n) a pour limite	ℓ	0	$\ell \neq 0$	ℓ
(v_n) a pour limite	$\ell' \neq 0$	0	0 en restant de signe constant	∞
alors $(\frac{u_n}{v_n})$ a pour limite				

(u_n) a pour limite	∞	∞	∞
(v_n) a pour limite	0 en restant	∞	$\ell \neq 0$
alors $(\frac{u_n}{v_n})$ a pour limite			

Démonstration
• Supposons que $(u_n) \to \ell$.
Si $\ell \in \overline{\mathbb{R}_+^*}$, alors (u_n) est positive à partir d'un certain rang.
Et à partir de ce rang, $|u_n| = u_n$, $|\ell| = \ell$, donc $(|u_n|) \to |\ell|$.
Si $\ell \in \overline{\mathbb{R}_-^*}$, alors (u_n) est négative à partir d'un certain rang.
Et à partir de ce rang, $|u_n| = -u_n$, $|\ell| = -\ell$, donc $(|u_n|) \to |\ell|$ car $(-u_n)$ converge vers $-\ell$.
Si $\ell = 0$, alors $(u_n) \to 0$ et $(|u_n|) \to 0$ (il suffit d'écrire).
• Supposons $(u_n) \to \ell$ et $(v_n) \to \ell'$.
Si $\ell, \ell' \in \mathbb{R}$ (pas d'infini). Soit $\epsilon > 0$.
$\exists\ N_1 \in \mathbb{N}$ tel que $\forall\ n \geqslant N_1$, $|u_n - \ell| \leqslant \frac{\epsilon}{2}$ i.e. $-\frac{\epsilon}{2} \leqslant u_n - \ell \leqslant \frac{\epsilon}{2}$.
$\exists\ N_2 \in \mathbb{N}$ tel que $\forall\ n \geqslant N_2$, $|v_n - \ell'| \leqslant \frac{\epsilon}{2}$ i.e. $-\frac{\epsilon}{2} \leqslant v_n - \ell' \leqslant \frac{\epsilon}{2}$.
$\forall\ n \geqslant N := \max(N_1, N_2)$, $\epsilon \leqslant (u_n + v_n) - (\ell + \ell') \leqslant \epsilon$.
Donc $(u_n + v_n) \to \ell + \ell'$ Si $\ell = +\infty$ et $\ell' \in \mathbb{R} \cup \{+\infty\}$.
(v_n) converge donc est minorée.
D'après le lemme $(u_n + v_n) \to +\infty = \ell + \ell'$. Si $\ell = -\infty$ et $\ell' \in \mathbb{R} \cup \{-\infty\}$.
On considère les suites opposées.
D'après le lemme $(-u_n - v_n) \to +\infty$ donc $(u_n + v_n) \to -\infty = \ell + \ell'$.
• Supposons $(u_n) \to \ell$ et $\lambda \in \mathbb{R}$.
Si $\lambda = 0$, alors $\lambda u_n = 0 \to 0 = \lambda \ell$.
Si $\ell \in \mathbb{R}^*$ (pas d'infini). Soit $\epsilon > 0$.
$\exists\ N \in \mathbb{N}$ tel que $\forall\ n \geqslant N$, $|u_n - \ell| \leqslant \frac{\epsilon}{\lambda}$ i.e. $-\frac{\epsilon}{\lambda} \leqslant u_n - \ell \leqslant \frac{\epsilon}{\lambda}$.
$\forall\ n \geqslant N$, $\epsilon \leqslant \lambda u_n - \lambda \ell \leqslant \epsilon$.
Donc $(\lambda u_n) \to \lambda \ell$ Si $\ell = +\infty$ et $\lambda > 0$.
Soit $A > 0$, $\exists\ N$ tel que $u_n \geqslant \frac{A}{\lambda}$ et donc $\lambda u_n \geqslant A$.
Donc $(\lambda u_n) \to +\infty = \lambda \ell$. (de même pour $-\infty$)
Si $\ell = +\infty$ et $\lambda < 0$.
Soit $A < 0$, $\exists\ N$ tel que $u_n \geqslant \frac{A}{\lambda} (> 0)$ et donc $\lambda u_n \leqslant A$ $(\lambda < 0)$.
Donc $(\lambda u_n) \to -\infty = \lambda \ell$. (de même pour $-\infty$)
• Supposons $(u_n) \to \ell$ et $(v_n) \to \ell'$.
Si $\ell, \ell' \in \mathbb{R}$ (pas d'infini).
Alors $(u_n - \ell)$ converge vers 0, $(v_n - \ell')$ converge vers 0.
D'après le lemme : $(u_n - \ell) \times (v_n - \ell')$ converge vers 0 (elles sont bornées).
Donc $(u_n v_n + \ell\ell' - v_n \ell - u_n \ell')$ converge vers 0.
Par addition : $(u_n v_n) = (u_n v_n + \ell\ell' - v_n \ell - u_n \ell') - \ell\ell' + v_n \ell + u_n \ell' \to 0 - \ell\ell' + \ell\ell' + \ell\ell' = \ell\ell'$
Si $\ell = +\infty$ et $\ell' > 0$.
Alors à partir d'un certain rang, $v_n \geqslant \frac{\ell'}{2} > 0$.
Donc à partir d'un certain rang : $u_n v_n \geqslant \frac{\ell'}{2} u_n \to +\infty$ (de même en $-\infty$)
Si $\ell = +\infty$ et $\ell' < 0$.
Alors à partir d'un certain rang, $v_n \leqslant \frac{\ell'}{2} < 0$.
Donc à partir d'un certain rang : $u_n v_n \leqslant \frac{\ell'}{2} u_n \to -\infty$ (de même en $-\infty$)
• On commence par $\frac{1}{v_n} \to \frac{1}{\ell'}$.
Si $\ell \in \mathbb{R}^*$,
Notons que $\frac{1}{v_n} - \frac{1}{\ell'} = \frac{\ell' - v_n}{v_n \ell'}$.
A partir d'un certain rang $|v_n| \geqslant \frac{|\ell'|}{2} > 0$, donc $\frac{1}{|v_n \ell'|} \leqslant \frac{2}{|\ell'|^2}$.
Donc $(\frac{1}{v_n - \ell'})$ est bornée, alors que $(\ell' - v_n)$ converge vers 0.
Ainsi $\left(\frac{1}{v_n} - \frac{1}{\ell'}\right) \to 0$, i.e. $(\frac{1}{v_n}) \to \frac{1}{\ell'}$.
Si $\ell = +\infty$.
Soit $\epsilon > 0$, $A := \frac{1}{\epsilon} > 0$. A partir d'un certain rang, $v_n \geqslant A$.
Et ensuite, $0 < \frac{1}{v_n} \leqslant \frac{1}{A} = \epsilon$ et donc $(\frac{1}{v_n}) \to 0$. (de même en $-\infty$).
• Par produit, $\frac{u_n}{v_n} = u_n \times \frac{1}{v_n} \to \ell \frac{1}{\ell'} = \frac{\ell}{\ell'}$. □

Savoir faire - Gérer ϵ
Il faut bien différencier un « montrer que $\forall\ \epsilon$ » et « exploiter un $\forall\ \epsilon$ ».

1. S'il s'agit de **montrer** que $\forall\ \epsilon > 0 \ldots$
   a. On prend $\epsilon > 0$, fixé et quelconque
   b. et on agit avec lui. …
2. S'il s'agit de **exploiter** que $\forall\ \epsilon > 0 \ldots$
   On considère arbitrairement un $\epsilon > 0$, fixé et quelconque, *bien choisi.*

Application - Lemme de Cesaro
Soit (u_n) une suite telle que $(u_n) \to \ell$.
On note, pour tout entier $n \in \mathbb{N}$, $v_n = \frac{1}{n+1} \sum_{k=0}^{n} u_k$. Alors $(v_n) \to \ell$

Pour aller plus loin - Convergence au sens de Cesaro
Si (u_n) converge vers ℓ, alors $\mathscr{C}(u_n) \to \ell$ également.
Et si (u_n) ne converge pas, comme $u_n = (-1)^n$?
$\mathscr{C}(u_n) = \frac{1}{n+1}[n,\ pair] \to 0$.
Donc si $(-1)^n$ converge, sa limite serait 0 (au sens de Cesaro)

• Si $\ell = 0$.
Soit $\epsilon > 0$, il existe $N > 0$ tel que $\forall\ n \geqslant N, |u_n| \leqslant \epsilon$.
Pour tout $n > N$,

$$v_n = \underbrace{\overbrace{\frac{1}{n+1}}^{\to_n 0}\ \overbrace{\sum_{k=0}^{N-1} u_k}^{\text{Constante}}}_{\to_n 0} + \underbrace{\overbrace{\frac{1}{n+1}\sum_{k=N}^{n} u_k}^{\in\left[-\frac{n-N+1}{n+1}\epsilon, \frac{n-N+1}{n+1}\epsilon\right]}}_{\to 0}$$

Donc, par addition, $(v_n) \to 0$.
• Si $\ell \neq 0$. On note $w_n = u_n - \ell \to 0$.
Alors $x_n = \frac{1}{n+1}\sum_{k=0}^{n} w_n = \frac{1}{n+1}\sum_{k=0}^{n} u_n - \ell = \left(\frac{1}{n+1}\sum_{k=0}^{n} u_n\right) - \ell = v_n - \ell \to 0$.
Donc $v_n \to \ell$.
• Si $\ell = +\infty$. Soit $A > 0$, $\exists\ N \in \mathbb{N}$ tel que $\forall\ n \geqslant N$, $u_n > A + 1$.

$$v_n = \underbrace{\overbrace{\frac{1}{n+1}}^{\to_n 0}\ \overbrace{\sum_{k=0}^{N-1} u_k}^{\text{Constante}}}_{\to_n 0} + \underbrace{\overbrace{\frac{1}{n+1}\sum_{k=N}^{n} u_k}^{\geqslant \frac{n-N+1}{n+1} A}}_{\to A+1}$$

Donc pour tout A, il existe N' tel que pour tout $n \geqslant N'$, $v_n \geqslant A$.

4.4. Extension aux suites à valeurs complexes

Définition - Cas des suites complexes (bornées...)
Soit (u_n) une suite de complexes.
— On dit que la suite (u_n) est bornée si la suite réelle des modules $(|u_n|)$ est majorée.
— Soit $\ell \in \mathbb{C}$. On dit que la suite (u_n) converge vers ℓ si la suite réelle $(|u_n - \ell|)$ converge vers 0. On note $u_n \underset{n\to+\infty}{\longrightarrow} \ell$.

Définition - Convergence
La suite complexe (u_n) converge vers le complexe ℓ si et seulement si

$$\forall \epsilon > 0, \exists N \in \mathbb{N} | \forall n \geqslant N, |u_n - \ell| \leqslant \epsilon$$

Attention $|u_n - \ell|$ désigne ici le module du complexe $u_n - \ell$.

A partir de cette définition, on voit que bon nombre de résultats subsistent pour les suites complexes :

Proposition - Généralisation
• la limite, lorsqu'elle existe, est unique ;
• si $|u_n - \ell| \leqslant \alpha_n$ où (α_n) est une suite réelle qui converge vers 0, alors (u_n) converge vers ℓ ;
• les opérations (somme, produit, inverse, quotient) sur les limites restent valables ;
• toute suite extraite d'une suite convergente converge vers la même limite ;
• si les suites (u_{2n}) et (u_{2n+1}) convergent vers une même limite, alors la suite (u_n) converge.

Attention - Relation d'ordre dans $\mathbb{C}$?
En revanche les résultats liés à la relation d'ordre dans $\mathbb{R}$ n'ont plus de sens ici (inégalités).

Savoir faire - Souvent pour l'étude de suites complexes
On peut également, pour étudier une suite complexe, se ramener à deux suites réelles, selon la proposition qui suit...
Et si on veut raisonner pour la convergence par encadrement (vers 0), on note que :

$$|\mathrm{Re}(u_n)| \leqslant |u_n| \quad \text{et} \quad |\mathrm{Im}(u_n)| \leqslant |u_n|$$

$$|u_n| = \sqrt{|\mathrm{Re}(u_n)|^2 + |\mathrm{Im}(u_n)|^2} \leqslant |\mathrm{Re}(u_n)| + |\mathrm{Im}(u_n)|$$

On notera qu'il s'agit du module de u_n mais de la valeur absolue de $\mathrm{Re}(u_n)$ ou de $\mathrm{Im}(u_n)$.

Proposition - Utilisation de deux suites complexes
Soit (u_n) une suite complexe.
(u_n) est convergente (respectivement bornée) si et seulement les suites réelles $(\mathrm{Re}(u_n))$ et $(\mathrm{Im}(u_n))$ le sont toutes les deux.
En cas de convergence on a

$$\lim_{n\to+\infty} u_n = (\lim_{n\to+\infty} \mathrm{Re}(u_n)) + i(\lim_{n\to+\infty} \mathrm{Im}(u_n)).$$

Exercice
Montrer par deux méthodes que la suite complexe $(\overline{u_n})$ converge si et seulement si la suite (u_n) converge et donner alors une relation entre les limites.

Correction
Pour la correction, nous utiliserons que l'équivalence avec les suites réelles et imaginaires.
Comme $\mathrm{Re}(u_n) = \mathrm{Re}(\overline{u_n})$ et $\mathrm{Im}(u_n) = -\mathrm{Im}(\overline{u_n})$, on en déduit :

$$(u_n) \text{ converge} \longleftrightarrow (\mathrm{Re}(u_n)) \text{ et } (\mathrm{Im}(u_n)) \text{ convergent} \longleftrightarrow (\overline{u_n}) \text{ converge}$$

Dans ce cas $\lim(\overline{u_n}) = \overline{\lim(u_n)}$.

Démonstration
Notons les inégalités importantes, pour $z \in \mathbb{C}$:

$$\left.\begin{matrix}|\mathrm{Re}(z)| \\ |\mathrm{Im}(z)|\end{matrix}\right\} \leqslant |z| \leqslant |\mathrm{Re}(z)| + |\mathrm{Im}(z)|$$

Si u_n converge vers ℓ.
Soit $\epsilon > 0$, il existe $N \in \mathbb{N}$ tel que $\forall\ n \in \mathbb{N}$, $n \geqslant N$
$|\mathrm{Re}(u_n - \ell)| = |\mathrm{Re}(u_n) - \mathrm{Re}(\ell)| \leqslant |u_n - \ell| \leqslant \epsilon$ et $|\mathrm{Im}(u_n - \ell)| = |\mathrm{Im}(u_n) - \mathrm{Im}(\ell)| \leqslant |u_n - \ell| \leqslant \epsilon$.
Donc $(\mathrm{Re}(u_n))$ converge vers $\mathrm{Re}(\ell)$ et $(\mathrm{Im}(u_n))$ converge vers $\mathrm{Im}(\ell)$.
Réciproquement, si $(\mathrm{Re}(u_n))$ converge vers ℓ_1 et $(\mathrm{Im}(u_n))$ converge vers ℓ_2.
Soit $\epsilon > 0$, il existe $N_1, N_2 \in \mathbb{N}$ tel que $\forall\ n \in \mathbb{N}$,
si $n \geqslant N_1$, alors $|\mathrm{Re}(z) - \ell_1| \leqslant \frac{\epsilon}{2}$ et si $n \geqslant N_2$, alors $|\mathrm{Im}(z) - \ell_2| \leqslant \frac{\epsilon}{2}$
Donc pour $n \geqslant \max(N_1, N_2)$
$|z - (\ell_1 + i\ell_2)| \leqslant |\mathrm{Re}(z) - \ell_1| + |\mathrm{Im}(z) - \ell_2| \leqslant \epsilon$.
Donc (u_n) converge vers $\ell_1 + i\ell_2$ □

Exercice
Soit $z \in \mathbb{C}$.
1. Montrer que la suite géométrique (z^n) est convergente si et seulement si $|z| < 1$ ou $z = 1$.
2. Montrer que la suite (S_n) définie par $S_n = 1 + z + \cdots + z^n = \sum_{k=0}^{n} z^k$ (on dit que (S_n) est une série géométrique) converge si et seulement si $|z| < 1$ et que la limite vaut alors $\frac{1}{1-z}$.

Correction

1. Si $|z|<1$, $|z^n|=|z|^n\to 0$, donc par encadrement, (z^n) converge vers 0.
   Si $|z|>1$, alors $(|z|^n)=(|z^n|)$ est une suite numérique divergente.
   Or si (z^n) converge, nécessairement $(|z^n|)$ converge aussi. Par l'absurde : (z^n) ne peut pas converger.
   Si $|z|=1$, alors $z=e^{i\theta}$ et donc $\dfrac{z^{n+1}}{z^n}=e^{i\theta}$.
   Or si (z^n) converge, elle converge vers un nombre de module 1 donc différent de 0.
   Et par conséquent, $\dfrac{z^{n+1}}{z^n}\to 1=e^{i\theta}$, par unicité et nécessairement $\theta\equiv 0[2\pi]$, donc $z=1$.
   La réciproque est immédiate.
2. $T_n=(1-z)S_n=(1-z)\sum_{k=0}^{n}z^k=1-z^{n+1}$ (Télescopage).
   Si $z\neq 1$, (S_n) converge ssi (T_n) converge ssi $|z|<1$.
   Dans ce cas la limite vaut $\dfrac{1}{1-z}\lim(T_n)=\dfrac{1}{1-z}$.
   Si $z=1$, alors $S_n=n$ et la suite (S_n) diverge.

4.5. Bilan sur les théorèmes d'existence de limites

Convergence par encadrement

Rappelons le résultat suivant. C'est le plus naturel lorsqu'il faut démontrer la convergence ET donner la limite.

Proposition - Convergence par encadrement (ou gendarme)
Si pour tout entier n, $u_n\leqslant v_n\leqslant w_n$
et pour (u_n) et (w_n) converge vers la même limite ℓ.
Alors (v_n) converge et $\lim(v_n)=\ell$

Proposition - Divergence par minoration
Si pour tout entier n, $u_n\leqslant v_n$
et pour (u_n) diverge vers $+\infty$.
Alors (v_n) diverge et $\lim(v_n)=+\infty$

Proposition - Divergence par majoration
Si pour tout entier n, $v_n\leqslant w_n$
et pour (w_n) diverge vers $-\infty$.
Alors (v_n) diverge et $\lim(v_n)=-\infty$

Exploitation des suites extraites

Théorème - Convergence par suites extraites totales
Soit (u_n) une suite réelle.
On suppose que les suites extraites (u_{2n}) et (u_{2n+1}) convergent vers ℓ. Alors (u_n) converge vers ℓ

Pour aller plus loin - Suites extraites totales
On peut démontrer mieux :
(u_n) converge vers ℓ ssi toute suite extraite de (u_n) convergent vers ℓ

Remarque - Si $\ell=\infty$
Le résultat est encore valable pour les suites admettant une limite infinie.

Démonstration
Soit $\epsilon>0$. Il existe N_1 et $N_2\in\mathbb{N}$ tels que :

$$\forall\, n\geqslant N_1,|u_{2n}-\ell|<\epsilon \qquad \forall\, n\geqslant N_2,|u_{2n+1}-\ell|<\epsilon$$

Avec $N=\max(2N_1,2N_2+1)$, on a pour $n\geqslant N$: si $n=2p$: $|u_n-\ell|=|u_{2p}-\ell|<\epsilon$ car $p\geqslant N_1$
si $n=2p+1$: $|u_n-\ell|=|u_{2p+1}-\ell|<\epsilon$ car $p\geqslant N_2$
Donc (u_n) converge vers ℓ. □

Exercice
On considère une suite réelle (u_n) telle que les suites $(u_{2n}),(u_{2n+1}),(u_{3n})$ convergent. Montrer que la suite (u_n) est convergente.

Correction
Notons ℓ_1, ℓ_2 et ℓ_3, les limites de (u_{2n}), de (u_{2n+1}) et de (u_{3n}) respectivement.
La suite (u_{6n}) est une suite extraite de (u_{2n}) et de (u_{3n}) ; elle converge vers ℓ_1 et vers ℓ_3.
Mais elle n'admet qu'une limite, donc nécessairement $\ell_1=\ell_3$.
La suite (u_{6n+3}) est une suite extraite de (u_{2n+1}) et de (u_{3n}) ; elle converge vers ℓ_2 et vers ℓ_3.
Mais elle n'admet qu'une limite, donc nécessairement $\ell_2=\ell_3$.
Finalement $\ell_1=\ell_2(=\ell_3)$ et donc d'après le théorème précédent, (u_n) converge.

Suites monotones

Théorème - Théorème de la limite monotone
Soit (u_n) une suite croissante. On a les deux possibilités suivantes :
1. Si (u_n) est majorée, alors (u_n) est convergente (et $\lim\limits_{n\to+\infty}u_n=\sup\limits_{n\in\mathbb{N}}u_n$).
2. Si (u_n) n'est pas majorée, alors (u_n) diverge vers $+\infty$.

Démonstration
On considère que u_n est croissante et majorée.
Donc l'ensemble $\{u_n,n\in\mathbb{N}\}$ est une partie majorée de $\mathbb{R}$, elle admet une borne supérieure ℓ.
On a donc $\forall\, n\in\mathbb{N}$, $u_n\leqslant\ell$ et pour tout $\epsilon>0$, il existe $n_0\in\mathbb{N}$ tel que $\ell-\epsilon<u_{n_0}$.
Donc pour tout $\epsilon>0$, il existe $n_0\in\mathbb{N}$ tel que pour tout $n\geqslant n_0$:

$$0\leqslant\ell-u_n\leqslant\ell-u_{n_0}\leqslant\epsilon$$

par croissance de (u_n),
on peut donc affirmer par encadrement que (u_n) converge et $\lim(u_n)=\sup\{u_n,n\in\mathbb{N}\}$ □

Exercice
Démontrer directement le théorème de la limite monotone, avec les coupures de Dedekind

Correction
On note $X=\{a\in\mathbb{Q}\mid\exists\, n\in\mathbb{N}$ tel que $a\leqslant u_n\}$ et $Y=\{b\in\mathbb{Q}\mid\forall\, n\in\mathbb{N},b\geqslant u_n\}$.
• La suite (u_n) est croissante, donc $u_0\in X$, donc $X\neq\emptyset$.
• (u_n) est majorée par M, donc $M\in Y$, donc $Y\neq\emptyset$.
• La propriété caractéristique de X est exactement le contraire de celle de Y. Donc $X=\overline{Y}$ (complémentaire).
• $\forall\, a\in X$, $\forall\, b\in Y$, $\exists\, n_0\in\mathbb{N}$ tel que $a\leqslant u_{n_0}\leqslant b$, donc $X\leq Y$
La frontière entre X et Y donne la limite de (u_n).

Corollaire - Version décroissante
Soit (u_n) une suite décroissante. On a les deux possibilités suivantes :
1. Si (u_n) est minorée, alors (u_n) est convergente (et $\lim\limits_{n\to+\infty}u_n=\inf\limits_{n\in\mathbb{N}}u_n$).
2. Si (u_n) n'est pas minorée, alors (u_n) diverge vers $-\infty$.

Suites adjacentes

Définition - Suites adjacentes
Deux suites réelles (u_n) et (v_n) sont dites adjacentes si
— les deux suites sont monotones de sens contraire ;
— la suite (u_n-v_n) converge vers 0.

Théorème - Convergence pour suites adjacentes
Deux suites adjacentes convergent et ont même limite.

***Pour aller plus loin - Encadrement par les suites* sup *et* inf*. Définition de* limsup *et* liminf**
On exploite parfois aussi les suites suivantes associées à (u_n).
$M_n=\sup\{u_k,k\geqslant n\}$. M_n est bien définie si (u_n) majorée.
$m_n=\inf\{u_k,k\geqslant n\}$. M_n est bien définie si (u_n) minorée.
On démontre (M_n) est décroissante et (m_n) est croissante.
Or elles sont bornées, donc convergentes
On note : $\limsup(u_n)=\lim(M_n)$ et $\liminf(u_n)=\lim(m_n)$.
Il est possible d'extraire de (u_n) des suites qui convergent l'une vers $\limsup(u_n)$ et l'autre vers $\liminf(u_n)$… Ce sont donc des valeurs

Démonstration
On supposera que (u_n) est croissante et (v_n) décroissante.
Alors $(u_n - v_n)$ est croissante, de limite nulle, donc pour tout $n \in \mathbb{N}$, $u_n - v_n \leqslant 0$ et donc $u_n \leqslant v_n$.
Et par conséquent : pour tout $n \in \mathbb{N}$: $u_0 \leqslant u_n \leqslant v_n \leqslant v_0$.
La suite (u_n) est croissante et majorée (par v_0) et la suite (u_n) est décroissante et minorée (par u_0).
Elles sont toutes les deux convergentes. Notons ℓ_1 la limite de (u_n) et ℓ_2 celle de (v_n).
On a alors $\lim(u_n - v_n) = \ell_1 - \ell_2 = 0$, donc $\ell_1 = \ell_2$. □

Exercice

Soit les suites de terme général $u_n = \sum_{k=0}^{n} \frac{1}{k!}$ et $v_n = u_n + \frac{1}{n!}$.

1. Montrer que les suites $(u_n)_{n\geqslant 1}$ et $(v_n)_{n\geqslant 1}$ sont adjacentes.
2. Montrer que leur limite commune est un irrationnel.

Correction

1. Soit $n \in \mathbb{N}^*$,
   — $u_{n+1} - u_n = \frac{1}{(n+1)!} > 0$, donc $(u_n)_{n\geqslant 1}$ est croissante.
   — $v_{n+1} - v_n = u_{n+1} - u_n + \frac{1}{(n+1)!} - \frac{1}{n!} = \frac{2-(n+1)}{(n+1)!} = \frac{-(n-1)}{(n+1)!} \leqslant 0$, donc $(v_n)_{n\geqslant 1}$ est décroissante.
   — $u_n - v_n = -\frac{1}{n!} \longrightarrow 0$
   Les suites (u_n) et (v_n) sont adjacentes.
2. Notons ℓ leur limite commune.
   Si ℓ était rationnel, on suppose $\ell = \frac{p}{q}$.
   Comme (u_n) est strictement croissante et (v_n) strictement décroissante : pour tout $n \in \mathbb{N}$: $u_n < \ell < v_n$.
   En particulier pour $n = q$, et en multipliant par $q!$: $u_q q! < p(q-1)! < v_q q! = u_q q! + 1$.
   Or $u_q q! = \sum_{k=0}^{q} q(q-1)\cdots(k+1) \in \mathbb{Z}$, de même pour $p(q-1)!$, ce qui est contradictoire !

Savoir faire - Montrer la convergence avec deux sous-suites adjacentes
Il arrive souvent que (u_{2n}) et (u_{2n+1}) soient adjacentes (dans ce cas il faut le démontrer), on en déduit alors la convergence de (u_n) d'après le critère de convergence par suites extraites totales. C'est le cas :
— si $u_{n+1} = f(u_n)$ avec f décroissante et $|f'| < 1$
— si $u_n = \sum_{k=0}^{n} (-1)^k u_k$ avec $(u_k) \searrow 0$ (critère de Leibniz)…

5. Analyse asymptotique

Dans cette partie, nous donnons un peu des vocabulaire.
La manipulations des suites équivalentes, négligeables… et des développements limités auront lieu plus tard…

5.1. Hiérarchie de suites

Remarque - Autant en emporte…
En terminale, une habitude est de dire qu'« une fonction l'emporte sur une autre ». Sans définition claire, cela n'a pas de sens; par ailleurs nous verrons plus tard, pour les fonctions qu'il est toujours nécessaire au voisinage de quel point. Ici nous nous concentrons sur des suites, le voisinage est toujours $n \to +\infty$.
L'idée est donc d'obtenir une relation d'ordre. Telle suite croit plus vite, vers l'infini, qu'une autre.

Définition et critère d'application

Définition - Suites négligeables
Soient (u_n) et (v_n) deux suites numériques (réelles ou complexes).
On dit que (u_n) est négligeable devant (v_n) si
$\forall\, \epsilon > 0, \exists\, N \in \mathbb{N}$ tel que $\forall\, n \geqslant N, |u_n| \leqslant \epsilon |v_n|$.
On note alors $u_n = o(v_n)$ (lu u_n est un petit o de v_n) ou parfois $(u_n) \ll (v_n)$.

Proposition - Comparaison à une constante
Soit (u_n) une suite numérique.
$\forall\, \lambda \in \mathbb{K}$, $u_n = o(\lambda)$ ssi $(u_n) \to 0$

Démonstration
On prend $\epsilon' = \epsilon\lambda$. Et on trouve l'équivalence par simple jeu d'écriture □

Définition - Suites régulièrement nulles
Soit (u_n) une suite numérique. On note $\mathcal{Z}_u = \{n \in \mathbb{N} \mid u_n = 0\} = u^{-1}(\{0\})$.

Attention - Cas d'étude
• Si $\mathcal{Z}_u$ est fini, alors (u_n) n'est jamais nulle à partir d'un certain rang. C'est pratique.
Il existe $n_0 \in \mathbb{Z}$ tel que $\mathcal{Z}_u \cap [n_0, +\infty[= \emptyset$.
• Si (u_n) est nulle à partir d'un certain rang. Cela n'est pas intéressant.
Il existe $n_0 \in \mathbb{Z}$ tel que $[\![n_0, +\infty[\![\subset \mathcal{Z}_u$.
Cela correspond à la situation où le complémentaire de $\mathcal{Z}_u$ est fini.
• Le cas pénible : $\mathcal{Z}_u$ est infini mais pas de la forme contenant $[\![n_0, +\infty[\![$.
$\mathcal{Z}_u$ et son complémentaire sont infinis

Proposition - Négligeabilité avec la limite
Soient (u_n) et (v_n) deux suites numériques. Alors

$$u_n = o(v_n) \iff \lim_{n \notin \mathcal{Z}_v} \frac{u_n}{v_n} = 0, \text{ et } \exists\, N \in \mathbb{N} \mid \mathcal{Z}_v \cap [N, +\infty[\subset \mathcal{Z}_u$$

Démonstration
Si $u_n = o(v_n)$. Soit $\epsilon > 0$.
Il existe $N \in \mathbb{N}$ tel que $\forall\, n \geqslant N, |u_n| < \epsilon |v_n|$.
donc pour tout $n \in \mathcal{Z}_v \cap [N, +\infty[$, $v_n = 0$ et donc $u_n = 0$ donc $n \in \mathcal{Z}_u$.
et pour tout $n \notin \mathcal{Z}_v$, $\left|\frac{u_n}{v_n}\right| < \epsilon$ donc $\lim_{n \notin \mathcal{Z}_v} \frac{u_n}{v_n} = 0$.
Réciproquement, considérons $\epsilon > 0$. $\lim_{n \notin \mathcal{Z}_v} \frac{u_n}{v_n} = 0$, donc $\exists\, N_1$ tel que $\forall\, n \geqslant N_1$ et $n \notin \mathcal{Z}_v$, $|u_n| \leqslant \epsilon |v_n|$.
Et par ailleurs, $\exists\, N_2 \in \mathbb{N} \mid \mathcal{Z}_v \cap [N_2, +\infty[\subset \mathcal{Z}_u$, donc $\forall\, n \geqslant N_2$, $u_n = 0 \leqslant \epsilon v_n = 0$.
Donc en prenant $N = \max(N_1, N_2)$, on a $\forall\, n \geqslant N, |u_n| \leqslant \epsilon |v_n|$ □

On a un critère (savoir-faire) assez simple lorsque (v_n) est non nulle à partir d'un certain rang.

Savoir faire - $u_n = o(v_n)$ avec la notation des limites
Si v_n est non nulle à partir d'un certain rang, alors on utilise l'une des deux implications suivantes :

$$u_n = o(v_n) \iff \left(\frac{u_n}{v_n}\right) \longrightarrow 0$$

Relation d'ordre

Proposition - Relation d'ordre strict
$o()$ ou $\ll$ est une relation d'ordre strict sur l'ensemble des suites non (totalement) nulles à partir d'un certain rang : elle est transitive et antiréflexive (pour tout x, on n'a jamais $x\mathscr{R}x$).

Démonstration
On a jamais $(u_n) \ll (u_n)$ avec $\epsilon = \frac{1}{2}$ (par exemple), alors $u_n \neq 0 \Longrightarrow |u_n| > \epsilon |u_n|$.
Par ailleurs, elle est transitive. Supposons que $u_n = o(v_n)$ et $v_n = o(w_n)$.
Soit $\epsilon > 0$, $\exists\, N_1, N_2$ tel que $\forall\ n \geqslant N_1, |u_n| \leqslant \sqrt{\epsilon}|v_n|$ et $\forall\ n \geqslant N_2, |v_n| \leqslant \sqrt{\epsilon}|w_n|$.
alors pour tout $n \geqslant N = \max(N_1, N_2)$, $|u_n| \leqslant (\sqrt{\epsilon})^2 |w_n| = \epsilon |w_n|$ □

Remarque - Notations
Pour une relation d'ordre, il est peu malin d'exploiter une notation avec un signe d'égalité…
Nous verrons plus loin en quel sens cette notation peut néanmoins être pratique. En attendant, on peut préférer la notation $\ll$.
On peut aussi penser qu'il s'agit d'une relation d'appartenance : $u_n = o(v_n)$ signifie :

$$u_n \in \{(a_n) \in \mathbb{K}^{\mathbb{N}} \mid \frac{a_n}{v_n} \to 0\}$$

Pour aller plus loin - Ordre strict
Si $\mathscr{R}$ est une relation d'ordre strict, alors $\overline{\mathscr{R}}$ définie par $x\overline{\mathscr{R}}y$ ssi $x\mathscr{R}y$ ou $x = y$ est une relation d'ordre.
Et réciproquement, étant donnée une relation d'ordre, on peut définit une relation d'ordre strict en supprimant le cas d'égalité

Croissance comparée

Il s'agit simplement d'écrire avec la nouvelle notation des résultats déjà connus sur les fonctions de référence.

Proposition - Croissance comparée
Pour $\alpha > 0$, $\beta > 0$, $0 < p < q$, $a > 1$, on a

$$((\ln n)^\beta) \ll (n^\alpha)\,,\ (n^p) \ll (n^q)\,,\ (n^\alpha) \ll (a^n)\,,\ (a^n) \ll (n!)$$

5.2. Suites équivalentes

On cherche à définir ce que pourrait être deux suites égales à l'infini.

Définition et critère d'application

Définition - Suites équivalentes
Soient (u_n) et (v_n) deux suites numériques (réelles ou complexes).
On dit que (u_n) est équivalente à (v_n) si $u_n - v_n = o(v_n)$
On note alors $(u_n) \sim (v_n)$ (lu u_n est équivalente à v_n).

Proposition - Equivalence avec la limite
Soient (u_n) et (v_n) deux suites numériques. Alors

$$(u_n) \sim (v_n) \Longleftrightarrow \lim_{n \notin \mathscr{Z}_v} \frac{u_n}{v_n} = 1,\ \text{et } \exists\, N \in \mathbb{N} \mid \mathscr{Z}_v \cap [N, +\infty[\subset \mathscr{Z}_u$$

Démonstration
On a les équivalences :

$$\begin{aligned}(u_n) \sim (v_n) &\Longleftrightarrow (u_n - v_n) = o(v_n) \Longleftrightarrow \lim_{n \notin \mathscr{Z}_v} \frac{u_n - v_n}{v_n} = 0,\ \text{et } \exists\, N \in \mathbb{N} \mid \mathscr{Z}_v \cap [N, +\infty[\subset \mathscr{Z}_{u-v} \\ &\Longleftrightarrow \lim_{n \notin \mathscr{Z}_v} \frac{u_n}{v_n} - 1 = 0,\ \text{et } \exists\, N \in \mathbb{N} \mid \forall\ n \geqslant N, v_n = 0 \Rightarrow u_n + v_n = 0 \\ &\Longleftrightarrow \lim_{n \notin \mathscr{Z}_v} \frac{u_n}{v_n} = 1,\ \text{et } \exists\, N \in \mathbb{N} \mid \forall\ n \geqslant N, v_n = 0 \Rightarrow u_n = 0 \\ &\Longleftrightarrow \lim_{n \notin \mathscr{Z}_v} \frac{u_n}{v_n} = 1,\ \text{et } \exists\, N \in \mathbb{N} \mid \mathscr{Z}_v \cap [N, +\infty[\subset \mathscr{Z}_u\end{aligned}$$

□

Si v_n est constante (différente de 0) et donc jamais nulle

Proposition - Comparaison à une constante
Soit (u_n) une suite numérique.
$\forall\ \lambda \in \mathbb{K}^*$ (non nul!), $u_n \sim \lambda$ ssi $(u_n) \to \lambda$

Démonstration
On trouve $\frac{u_n}{\lambda} \to 1$. □

On a un critère (savoir-faire) assez simple lorsque (v_n) est non nulle à partir d'un certain rang.

Savoir faire - $(u_n) \sim (v_n)$ avec la notation des limites
Si v_n est non nulle à partir d'un certain rang, alors on utilise l'une des deux implications suivantes :

$$(u_n) \sim (v_n) \Longleftrightarrow \left(\frac{u_n}{v_n}\right) \longrightarrow 1$$

Relation d'équivalence

Proposition - Relation d'équivalence
$\sim$ est une relation d'équivalence sur l'ensemble des suites numériques.

Pour aller plus loin - Croissance à la même vitesse
On note parfois $u_n \asymp v_n$ pour signifier que $\frac{u_n}{v_n}$ est bornée.
On dit qu'elles croissent à la même vitesse.
C'est une notion importante dans l'étude asymptotique des suites, même si elle ne figure pas au programme.

Démonstration
- $u_n - u_n = 0 = o(u_n)$ donc $u_n \sim u_n$. Et $\sim$ est réflexive.
- Si $u_n \sim v_n$. Soit $\epsilon > 0$ et $\epsilon' = f(\epsilon)$.
  Il existe N tel que $\forall\ n \geqslant N : |u_n - v_n| \leqslant \epsilon' |v_n| = \epsilon |v_n - u_n + u_n| \leqslant \epsilon' |v_n - u_n| + \epsilon' |u_n|$.
  Donc $(1 - \epsilon')|u_n - v_n| \leqslant \epsilon' |u_n|$ et $|u_n - v_n| \leqslant f^{-1}(\epsilon')|u_n|$.
  avec $f^{-1} : x' \mapsto \frac{x'}{1-x'}$.
  Or $f^{-1}(0) = 0$ et f^{-1} est inversible au voisinage de 0 : $f : x \mapsto \frac{x}{1+x}$.
  Donc avec $\epsilon' = \frac{\epsilon}{1+\epsilon}$, on trouve $|u_n - v_n| \leqslant \epsilon |u_n|$.
  Donc $\sim$ est symétrique.
- . Si $u_n \sim v_n$ et $v_n \sim w_n$.
  Alors $u_n - v_n = o(v_n)$, $v_n - w_n = o(w_n)$.
  Soit $\epsilon > 0$ et $\epsilon' = f(\epsilon)$ avec f définie plus tard.
  Alors il existe $N \in \mathbb{N}$ tel que pour tout $n \in \geqslant N$, $|u_n - w_n| = |u_n - v_n + v_n - w_n| \leqslant \epsilon' |v_n| + \epsilon' |w_n|$.
  Or $|v_n| - |w_n| \leqslant |v_n - w_n| \leqslant \epsilon' |w_n|$, donc $\epsilon' |v_n| \leqslant \epsilon' (1 + \epsilon') |w_n|$.
  Ainsi, pour tout $n \geqslant N$, $|u_n - w_n| \leqslant (2\epsilon' + \epsilon'^2)|w_n| = \epsilon |w_n|$,
  avec $f^{-1} : x' \mapsto 2x' + x'^2$.
  Or $f^{-1}(0) = 0$ et f^{-1} est inversible au voisinage de 0 : $f : x \mapsto \sqrt{1+x} - 1$.
  Donc $\sim$ est transtive. □

Exercice
Refaire la démonstration en exploitant le savoir-faire précédent dans le cas où les suites sont non nulles à partir d'un certain rang.

Correction
Réflexivité : $\lim \frac{u_n}{u_n} = 1$
Symétrie : $\lim \frac{u_n}{v_n} = 1 \Longleftrightarrow \lim \frac{v_n}{u_n} = 1$.
Transitivité : $\lim \frac{u_n}{w_n} = \lim \frac{\frac{u_n}{v_n}}{\frac{w_n}{v_n}} = 1$

***Pour aller plus loin - Propriété de* HARDY**
HARDY a introduit la notion de classe des suites logarithmico-exponentielles que l'on peut définir comme la plus petite famille $\mathscr{L}$ de fonctions qui satisfont les propriétés suivantes :
— pour tout $\alpha \in \mathbb{R}$, la suite constante

Suites équivalentes

Analyse - Equivalence en action

On considère la suite définie par récurrence : $u_{n+1} = \sin(u_n)$ et $u_0 = 1$.
Un simple programme informatique Python, donne pour première valeur :

```
def suite(n):
    u=1
    s=10
    L=[u]
    for k in range(n):
        u=np.sin(u)
        if k==s:
```

Pour $n = 100$, on obtient la liste suivante (on ne donne que les derniers termes) :

$$[\dots 0.17303865584954667, 0.1721764163093636, 0.17132698944422506, 0.17049006030857783, 0.16966532470732423, 0.16885248872798114]$$

Le dernier terme ressemble à $\frac{1}{6}$. Mais est-ce satisfaisant ?
Le mieux est de calculer le résultat pour différentes valeurs de $n = 10^{-k}$ et différentes valeurs de k.
On trouve (on garde 4 chiffres significatifs) :

n	0	10	100	1 000	10 000	100 000
u_n	1	0.4465…	0.1680…	0.05456…	0.01731…	0.0054769…

On a le sentiment qu'un nombre sur 2, on trouve une division par 10.
Donc à une multiplication par 100, correspond une division par 10. On peut penser que $u_n \sim \dfrac{C}{\sqrt{n}}$.
De fait, le calcul de $\sqrt{n}u_n$, donne (on garde 4 chiffres significatifs) :

n	0	10	100	1 000	10 000	100 000
$\sqrt{n}u_n$	1	1.412…	1.680…	1.725…	1.731…	1.731…

Notons que $\sqrt{3} = 1,732\dots$. Reste **à démontrer** que $u_n \sim \sqrt{\dfrac{3}{n}}$. Mais si c'est bien vrai, alors c'est bien pratique…

Heuristique - Objectif premier

Dans de nombreuses situations, trouver un équivalent signifie trouver une expression fermée, analytique notée v_n (dépendant de n) et permettant de remplacer (car très proche) u_n et avantageusement (car plus simple à calculer).

Les résultats suivants sont spectaculaires. Ils ne doivent pas vous détourner de l'objectif principal…

Proposition - Equivalences classiques
On a les comparaisons classiques suivantes :

$$n^2 = o(n^3) \text{ et plus généralement } n^p = o(n^q) \text{ pour } 0 < p < q$$
$$\sum_{k=1}^{n} \frac{1}{k} \sim \ln n$$
$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \text{ formule de Stirling}$$

Démonstration
Si $q > p$, alors $q - p > 0$ et donc $\lim \dfrac{n^p}{n^q} = \lim \dfrac{1}{n^{q-p}} = 0$.
Nous avons montré (exercice classique de comparaison limite-intégrale) ($k \in \mathbb{N}^*$) :

$$\forall\, t \in [k, k+1] : \frac{1}{k+1} \leqslant \frac{1}{t} \leqslant \frac{1}{k} \Rightarrow \int_k^{k+1} \frac{1}{k+1}\mathrm{d}t \leqslant \int_k^{k+1} \frac{1}{t}\mathrm{d}t \leqslant \int_k^{k+1} \frac{1}{k}\mathrm{d}t$$

$$\forall\, k \in \mathbb{N}^* : \frac{1}{k+1} \leqslant \ln(k+1) - \ln k \leqslant \frac{1}{k} \Rightarrow \sum_{k=1}^{n-1} \frac{1}{k+1} \leqslant \ln n - \ln 1 \leqslant \sum_{k=1}^{n-1} \frac{1}{k}$$

En notant $S_n = \sum_{k=1}^{n} \frac{1}{k}$, on a donc

$$S_n - 1 \leqslant \ln n \leqslant S_n - \frac{1}{n} \Rightarrow 1 - \frac{1}{S_n} \leqslant \frac{\ln n}{S_n} \leqslant 1 - \frac{1}{nS_n}$$

Enfin, comme (S_n) diverge vers $+\infty$ (divergence par minoration : $S_n \leqslant \ln n$), on a donc $\lim \dfrac{\ln n}{S_n} = 1$.
La formule de Stirling est démontrée en exercice (avec les intégrales de Wallis). □

Exercice

$\ln(n!) = \sum_{k=1}^{n} \ln(k)$. Nous allons essayer de trouver un équivalent de série, pour avoir des idées pour trouver un équivalent de $n!$.

1. (a) Montrer que $1 \leqslant \sum_{k=1}^{n} \ln(k) - n\ln n - n \leqslant n\ln(1 + \frac{1}{n}) + \ln(n+1)$
   (b) En déduire $\ln(n!) \sim n\ln n - n$.
   On peut supposer que $n! = K_n \times n^n \times e^{-n}$, avec $\ln(K_n) = o(n \ln n)$.
   (c) Montrer que la fonction logarithme est concave. Calculer l'équation de la tangente à $y = \ln(x)$ en $x = k$.
   (d) En déduire que pour tout $x \in [k - \frac{1}{2}, k + \frac{1}{2}]$, $\ln(x) \leqslant \frac{1}{k}(x - k) + \ln k$ (on pourra faire un dessin).
   (e) Montrer alors que $\ln k \leqslant \int_{k-\frac{1}{2}}^{k+\frac{1}{2}} \ln t \mathrm{d}t$ (approximation du point milieu).
   Puis que $\ln(n!) \geqslant ln(n^n\sqrt{n}e^{-n}\sqrt{2})$
   (f) On note $u_n = \dfrac{n!}{n^n e^{-n}\sqrt{n}}$.
   Montrer que (u_n) est décroissante, puis convergente, on note K la limite de (u_n).
   (g) Donner un équivalent de $n!$ exploitant K.
2. Intégrale de Wallis.
   On définie les intégrales de Wallis $W_n = \int_0^{\pi/2} \cos^n(t)dt$ pour compléter le résultat précédent (i.e. trouver la valeur de la constante).
   (a) Calculer W_0 et W_1.
   (b) Donner relation de récurrence entre W_{n+2} et W_n.
   (c) En déduire une expression de W_{2n} et de W_{2n+1} en utilisant les factorielles.
   (d) Par ailleurs, montrer que W_n et W_{n+1} sont équivalentes.
   (e) En déduire la formule de Stirling (i.e. la valeur de K), en supposant que $n! \sim Kn^n e^{-n}\sqrt{n}$

Correction

1. (a) La fonction $f : x \mapsto \ln(x)$ est croissante positive sur $[1; +\infty[$
   Donc la série $\sum_{k\geqslant 1} \ln(k)$ a le même comportement que $\int_1^{+\infty} \ln t dt$. Ecrivons la suite des inégalités :
   $$\ln(k) \leqslant \int_k^{k+1} \ln(x)dx \leqslant \ln(k+1)$$
   $$\sum_{k=1}^{n} \ln(k) \leqslant \sum_{k=1}^{n} \int_k^{k+1} \ln(x)dx = \int_1^{n+1} \ln(x)dx \leqslant \sum_{k=1}^{n} \ln(k+1) = \sum_{k=1}^{n+1} \ln(k) \qquad (f(1) = \ln 1 = 0)$$
   Par conséquent (en $n-1$ et en n) :
   $$\int_1^n \ln(x)dx \leqslant \sum_{k=1}^{n} \ln(k) \leqslant \int_1^{n+1} \ln(x)dx$$
   Puisque une primitive de ln est $x \mapsto x\ln x - x$
   $$n\ln n - n + 1 \leqslant \sum_{k=1}^{n} \ln(k) \leqslant (n+1)\ln(n+1) - (n+1) + 1$$
   $$1 \leqslant \sum_{k=1}^{n} \ln(k) - (n\ln n - n) \leqslant (n+1)\ln(n+1) - n\ln n = n\ln(1 + \frac{1}{n}) + \ln(n+1)$$

(b) Puis $n\ln n - n = \ln(n^n e^{-n})$, donc

$$1 \leqslant \ln\left(\frac{n!}{n^n e^{-n}}\right) \leqslant n\ln(1+\frac{1}{n}) + \ln(n+1)$$

On ne peut pas en déduire un équivalent de $n!$, mais on a un équivalent de $\ln n!$:

$$\frac{1}{n\ln n - n} \leqslant \frac{\ln(n!)}{n\ln n - n} - 1 \leqslant \frac{n\ln(1+\frac{1}{n}) + \ln(n+1)}{n\ln n - n}$$

Les termes de gauche et de droite tendent vers 0, donc $\ln n! \sim \ln(n^n e^{-n}) = n\ln n - n$
On peut supposer que $n! = K_n \times n^n \times e^{-n}$, avec $\ln(K_n) = o(n\ln n)$.

(c) ln est de classe $\mathscr{C}^2$ et $\forall\, x > 0$, $\ln''(x) = \frac{-1}{x^2} < 0$, donc ln est concave.
Puis la tangente en k a pour équation $y = \frac{1}{k}(x-k) + \ln(k)$

(d) ln est concave, donc tous les points de la courbe sont les tangentes.
Donc pour tout $x \in [k-\frac{1}{2}, k+\frac{1}{2}]$, $\ln(x) \leqslant \frac{1}{k}(x-k) + \ln k$

(e) On intègre $\int_{k-\frac{1}{2}}^{k+\frac{1}{2}} \ln x dx \geqslant \frac{1}{2k}[(x-k)^2]_{k-\frac{1}{2}}^{k+\frac{1}{2}} + 1\ln k = \ln k$

$$\sum_{k=1}^{n} \ln k \geqslant \int_{1-\frac{1}{2}}^{n+\frac{1}{2}} \ln x dx = (n+\frac{1}{2})\ln(n+\frac{1}{2}) - (n+\frac{1}{2}) - (\frac{1}{2})\ln(\frac{1}{2}) + \frac{1}{2}$$

$$\ln(n!) \geqslant (n+\frac{1}{2})\ln(n) - n + \frac{1}{2}\ln 2 + (n+\frac{1}{2})\ln(1+\frac{1}{2n})$$

Comme $(n+\frac{1}{2})\ln(1+\frac{1}{2n})$ est positif (et tend vers 0, ce qui fait qu'on peut le supprimer sans grand risque) :

$$\ln(n!) \geqslant (n+\frac{1}{2})\ln(n) - n + \frac{1}{2}\ln 2 = \ln(n^n\sqrt{n}e^{-n}\sqrt{2})$$

(f) On note $u_n = \frac{n!}{n^n e^{-n}\sqrt{n}}$.
D'après la question précédente, en composant par l'exponentielle croissante, on voit que $u_n \geqslant \sqrt{2}$.
Par ailleurs, $\frac{u_{n+1}}{u_n} = \frac{(n+1)n^n e^{-n}\sqrt{n}}{(n+1)(n+1)^n e^{-n-1}\sqrt{n+1}} = \left(\frac{n}{n+1}\right)^{n+\frac{1}{2}} e$.
Puis $\frac{u_{n+1}}{u_n} \leqslant 1 \Leftrightarrow e \leqslant \left(\frac{n+1}{n}\right)^{n+\frac{1}{2}} \Leftrightarrow 1 \leqslant (n+\frac{1}{2})\ln(1+\frac{1}{n})$
$\Leftrightarrow \frac{2}{2n+1} \leqslant \ln(1+\frac{1}{n}) \Leftrightarrow \leqslant \ln(1+\frac{1}{n}) - \frac{2}{2n+1} \geqslant 0$.
Soit $\varphi : x \mapsto \ln(1+x) - \frac{2x}{2+x}$, de classe $\mathscr{C}^1$ sur $]-1,+\infty[$.
Et $\forall\, x > -1$, $\varphi'(x) = \frac{x^2}{(x+1)(x+2)^2} > 0$, donc φ est croissante et $\varphi(0) = 0$.
Donc pour tout n, $\varphi(\frac{1}{n}) \geqslant \varphi(0) = 0$.
La suite (u_n) est décroissante, minorée, elle converge.

(g) On a donc $\lim \frac{n!}{Kn^n e^{-n}\sqrt{n}} = 1$, donc $n! \sim Kn^n e^{-n}\sqrt{n}$.

2. Intégrale de Wallis

(a) $W_0 = \frac{\pi}{2}$ et $W_1 = 1$

(b) $W_{n+2} = \frac{n+1}{n+2} W_n$ (intégration par parties)

(c) $W_{2n} = \frac{(2n)!}{2^{2n}(n!)^2}\frac{\pi}{2}$ et $W_{2n+1} = \frac{2^{2n}(n!)^2}{(2n+1)!}$

(d) On a $W_{n+2} = \frac{n+1}{n+2} W_n \leqslant W_{n+1} \leqslant W_n$ donc $\frac{n+1}{n+2} \leqslant \frac{W_{n+1}}{W_n} \leqslant 1$, en passant à la limite on a l'équivalent recherché.

(e) Donc $W_{2n}^2 \sim W_{2n}W_{2n+1} \sim \frac{\pi}{2n}$ donc $W_n \sim \sqrt{\frac{\pi}{2n}}$.
En utilisant $n! \sim Kn^n e^{-n}\sqrt{n}$, on en déduit que $K = \sqrt{2\pi}$

Calculer avec des relations d'équivalence

Théorème - Signe d'une suite
Si la suite (u_n) est équivalente à (v_n), alors à partir d'un certain rang, les deux suites sont de même signe (strict).

Démonstration
$\lim \frac{u_n}{v_n} = 1$, donc (avec $\epsilon = \frac{1}{2}$),

$$\exists\, N \text{tel que} \qquad \forall\, n \geqslant N, |\frac{u_n}{v_n} - 1| \leqslant \frac{1}{2} \Rightarrow \forall\, n \geqslant N, \frac{1}{2} \leqslant \frac{u_n}{v_n} \leqslant \frac{3}{2}$$

Donc, nécessairement, pour tout $n \geqslant N$ u_n et v_n ont strictement le même signe. □

Attention - Evidemment si (u_n) tend vers 0...
... et que le signe de (u_n) n'est jamais stabilisé ; on ne peut rien dire

Théorème - Equivalents et limite
Soient (u_n) et (v_n) deux suites réelles.
- Si $u_n \sim v_n$ et $v_n \underset{n\to+\infty}{\longrightarrow} \ell \in \mathbb{R}$ alors $u_n \underset{n\to+\infty}{\longrightarrow} \ell$;
- Si $u_n \underset{n\to+\infty}{\longrightarrow} \ell$, $\ell \in \mathbb{R}$, $\ell \neq 0$, alors $u_n \sim \ell$.

Démonstration
Commençons par la seconde affirmation avec $\ell \in \mathbb{R}^*$.

$$\lim \frac{u_n}{\ell} = \frac{\ell}{\ell} = 1 \Longrightarrow u_n \sim \ell$$

Reprenons la première affirmation. Notons $\epsilon_n = \frac{u_n}{v_n}$.
On a donc $u_n = v_n \times \epsilon_n$, avec $(\epsilon_n) \to 1$.
Par produit des limites : $\lim(u_n) = \lim(v_n) \times 1 = \lim(v_n)$. □

Attention - Equivalence à 0
Ne pas écrire $u_n \sim 0$, cela n'a pas de sens avec la première définition et avec celle qui suit cela signifie que (u_n) est nulle à partir d'un certain rang (ce qui est bien rare...), usuellement ce genre d'écriture provient d'une somme (ou d'une soustraction) d'équivalents, ce qui n'est pas autorisé.
Ne pas confondre $u_n \sim v_n$ et $u_n - v_n \underset{n\to+\infty}{\longrightarrow} 0$.

Théorème - Opérations sur les équivalents
Soient $(u_n), (v_n), (x_n), (y_n)$ quatre suites telles que $u_n \sim x_n$ et $v_n \sim y_n$. Alors
- $u_n v_n \sim x_n y_n$;
- si (v_n) est non nulle à partir d'un certain rang, $\frac{u_n}{v_n} \sim \frac{x_n}{y_n}$;
- si les suites sont à valeurs strictement positives et $\alpha \in \mathbb{R}$ alors $u_n^\alpha \sim x_n^\alpha$.

Exercice
A démontrer.

Correction
On peut tout refaire, ou exploiter $u_n \sim v_n$ ssi $u_n - v_n = o(v_n)$...

Heuristique - Recherche des équivalents
Déterminer un équivalent d'une suite consiste à chercher un équivalent écrit comme produit ou quotient de suites de références (n^α, a^n, $(\ln(n))^\beta$, $n!$...) a priori sans somme (dans une somme, l'un des termes est négligeable devant l'autre et s'enlève de l'équivalent) en laissant les constantes multiplicatives (si on les supprime, la limite du quotient ne sera plus 1). Par exemple :

$2(n^3+n) \sim$; $\frac{\pi}{2n+1} \sim$; $e^{n^3+n+1/n} \sim$; $\ln(3n^5+n+2) \sim$.

Exemple - Problème d'addition…
$u_n = \frac{n+1}{n+2}$, $v_n = \frac{1-n^2}{n^2+n+1}$.
Donner un équivalent de $u_n + v_n$.
A priori : $u_n \sim 1$, $v_n \sim -1$, donc $u_n + v_n \sim 0$? Non

$$u_n + v_n = \frac{(n+1)(n^2+n+1)+(1-n^2)(n+2)}{(n+2)(n^2+n+1)} = \frac{3n+3}{n^3+3n^2+3n+2} \sim \frac{3}{n^2}$$

Attention - Ce qui ne marche pas
D'une manière générale, les équivalents ne passent ni aux sommes, ni aux exponentielles, ni aux logarithmes.

Savoir faire - Comment faire si on veut additionner des équivalents ?
Dans ces cas-là, et dans toute opération un peu compliquée,
on remplace $u_n \sim v_n$ par $u_n = v_n + o(v_n) = v_n(1+\epsilon_n)$ avec $\epsilon_n \to 0$,
comme il s'agit d'égalités (LA VRAIE !), on peut alors faire des opérations.
L'enjeu : que les parties principales de disparaissent pas comparativement à la suite de domination.

Pour aller plus loin - Erreur relative / erreur absolue
Lorsqu'on écrit : $u_n = v_n + o(w_n)$, on parle d'une erreur absolue en $o(w_n)$.
Lorsqu'on écrit : $u_n = v_n(1+o(w_n))$, on parle d'une erreur relative en $o(w_n)$ (absolue en $o(v_n w_n)$).

5.3. Suites dominées

Mais pour le calcul asymptotique, le notation vraiment pratique est la suivante. C'est avec elle que l'on fera les calculs.

Définition et critère d'application

Définition - Suite dominée
Soient (u_n) et (v_n) deux suites numériques (réelles ou complexes).
On dit que (u_n) est dominée par (v_n) si
$\exists\, C > 0, \exists\, N \in \mathbb{N}$ tel que $\forall\, n \geqslant N$, $|u_n| \leqslant C|v_n|$.
On note $(u_n) = O\big((v_n)\big)$ qui se lit « u_n est un grand O de v_n ».
On dit aussi parfois que (v_n) est prépondérante à (ou domine) (u_n).

Exemple - Relations avec les notations précédentes
Si $u_n = o(v_n)$, alors $(u_n) = O\big((v_n)\big)$.
Si $u_n \sim v_n$ alors $(u_n) = O\big((v_n)\big)$ et $(v_n) = O\big((u_n)\big)$ On n'a pas les implications réciproques.

Proposition - Domination avec la limite
Soient (u_n) et (v_n) deux suites numériques. Alors

$$(u_n) = O(v_n) \iff \left(\frac{u_n}{v_n}\right)_{n \in \mathcal{Z}_v} \text{ bornée, et } \exists\, N \in \mathbb{N} \mid \mathcal{Z}_v \cap [N, +\infty[\subset \mathcal{Z}_u$$

Exercice
Faire la démonstration

Correction
La même que celle avec la négligeabilité

On a un critère (savoir-faire) assez simple lorsque (v_n) est non nulle à partir d'un certain rang.

Histoire - Edmund Landau

Toutes ces notations : o, O et ∼ ont été popularisées par Edmund LANDAU. *Edmund* LANDAU *(1877-1938) est un mathématicien allemand passionné de théorie des nombres. C'est dans ce cadre de réflexion qui développe ses notations O et o.*
Cette approche est finalement assez récente dans l'histoire des mathématiques

Savoir faire - $u_n = O(v_n)$ avec la notation des limites
Si v_n est non nulle à partir d'un certain rang, alors on utilise l'une des deux implications suivantes ($\Rightarrow$ ou $\Leftarrow$) :

$$(u_n) = O(v_n) \iff \left(\frac{u_n}{v_n}\right) \text{ est bornée}$$

Proposition - Implication sur les limites
Soit (u_n) une suite réelle. On a
$u_n = O(1) \iff (u_n)$ est bornée

Pour aller plus loin - Croissance à la même vitesse
En revanche on a l'équivalence :
$[(u_n) = O\big((v_n)\big)$ *et* $(v_n) = O\big((u_n)\big)]$
$\iff$
$(u_n) \asymp (v_n)$

Relation de préordre

Proposition - Relation de préordre
O est une relation de préordre (réflexive et transitive) sur l'ensemble des suites numériques.

Exercice
Faire la démonstration

Correction

Remarque - La relation d'équivalence naturelle à associer à $O(\cdot)$
Pour que cela soit une relation d'ordre, il faudrait que l'égalité des suites correspondent à la notation $\asymp$, c'est-à-dire l'égalité des vitesses de croissance, ou au fait que (u_n) et (v_n) soit d'ordre comparable.
Autrement écrit : cela signifie que dans le cadre de l'analyse asymptotique, si la relation d'ordre intéressante est celle de la domination $\big(O()\big)$, alors la relation d'équivalence intéressante est celle de $\asymp$.

Manipuler $O(\cdot)$

Heuristique - Une première formule commentée
On note pour tout $n \in \mathbb{N}$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$.
On a alors $H_n = \ln n + \gamma + O\left(\frac{1}{n}\right)$.
Cela signifie que le n-ieme nombre harmonique est égal à $\ln n$ additionné de la constante $\gamma \approx 0,577\,215\,664\,9$ d'Euler et d'un terme d'une autre suite, inconnue, mais dont on sait que divisé par $\frac{1}{n}$ (c'est-à-dire multiplié par n) elle reste bornée ou encore une suite que ne dépasse pas un nombre constant de fois $\frac{1}{n}$.

Remarque - Addition, multiplication
Même si on ignore toujours qui est précisément (a_n) caché derrière un $O(v_n)$. On peut néanmoins faire des calculs avec des O…
Il faut alors se rappeler que $O(v_n)$ n'est pas forcément optimal (par exemple : $n^2 = O(n^{10\,000})$).

Analyse - Que signifie $O(\frac{1}{n}) + O(\frac{1}{n^2})$?
Si l'on rencontre une opération du type : $O(\frac{1}{n}) + O(\frac{1}{n^2})$, cela signifie qu'on est en présence de deux suites (u_n) et (v_n) cachées et dont on connait des dominants.
Ces deux suites peuvent évidemment s'additionner et donner une nouvelle suite (w_n). Peut-on trouver un dominant de (w_n) ?
Oui !

$$\frac{w_n}{\frac{1}{n}} = n w_n = n u_n + n v_n = \frac{u_n}{\frac{1}{n}} + \frac{1}{n} \times \frac{v_n}{\frac{1}{n}} \to 0 + 0 \times$$

Donc $w_n = O\left(\frac{1}{n}\right)$ En revanche, on ne peut savoir si $w_n = O\left(\frac{1}{n^2}\right)$. On se trouve en présence d'une forme indéterminée.

On peut donc affirmer que $O(\frac{1}{n}) + O(\frac{1}{n^2}) = O(\frac{1}{n})$
Avant de passer aux théorèmes et démonstrations, deux petites remarques complémentaires :

Truc & Astuce pour le calcul - Pour manipuler une opération avec $O(a_n)$
Lorsque vous rencontrer $O(a_n)$ (avec (a_n) non nulle à partir d'un certain rang), vous pouvez le remplacer par $(u_n) = (a_n \times \epsilon_n)$ avec ϵ_n bornée.

Attention - Rappel : il ne s'agit pas d'une relation d'équivalence
Rappelons que même s'il y a une égalité : il n'y a pas de symétrie.
On a $O(\frac{1}{n^2}) = O(\frac{1}{n})$, mais on n'a pas $O(\frac{1}{n}) = O(\frac{1}{n^2})$.
Toute suite dominée par $(\frac{1}{n^2})$ est dominée par $\frac{1}{n}$ mais la réciproque est fausse.
Ce symbole = $O()$ est plutôt à voir comme une relation d'ordre, voir une inclusion d'ensemble.
L'ensemble des suites dominées par $(\frac{1}{n^2})$ est inclus dans l'ensemble des suites dominées par $(\frac{1}{n})$.

Proposition - Opérations entre les relations
Soient $(u_n), (v_n), (w_n), (x_n)$ quatre suites réelles.
- Si $u_n = o(v_n)$ alors $u_n = O(v_n)$
- Si $u_n \sim v_n$ alors $u_n = O(v_n)$ et $v_n = O(u_n)$.
- Si $u_n \sim v_n$ alors $w_n = O(u_n) \Leftrightarrow w_n = O(v_n)$.
- Si $u_n = O(w_n)$ et $v_n = O(w_n)$ alors $u_n + v_n = O(w_n)$.
  Autrement écrit : $O(w_n) + O(w_n) = O(w_n)$
- Si $u_n = O(v_n)$, $\lambda \in \mathbb{R}$ alors $\lambda u_n = O(v_n)$
  Autrement écrit : $\lambda \times O(v_n) = O(v_n)$
- Si les termes u_n et v_n ne s'annulent pas et $u_n = O(v_n)$ alors $\frac{1}{v_n} = O(\frac{1}{u_n})$.
- Si $u_n = O(v_n)$ et alors $u_n \times x_n = O(v_n \times x_n)$.
- Si $u_n = O(v_n)$ et $w_n = O(x_n)$ alors $u_n \times w_n = O(v_n \times x_n)$.
- Si les termes u_n et v_n sont > 0 avec $u_n = O(v_n)$, alors pour $\alpha > 0$ on a $u_n^\alpha = O(v_n^\alpha)$.

Les propriétés sont encore vraies en remplaçant les « O » par des « o ».

Démonstration
- Le premier résultat découle du fait que toute suite qui converge vers 0 est bornée.
- On l'a déjà vu
- $\exists\, C > 0, N \in \mathbb{N}$ tels que $\forall\, n \geqslant N$, $|w_n| < C|u_n|$.
  $\exists\, N' \in \mathbb{N}$ tels que $\forall\, n \geqslant N'$, $|u_n| < (1 + \frac{1}{2})|v_n|$.
  Donc $\forall\, n \geqslant \max(N, N')$, $|w_n| < \frac{3}{2}C|v_n|$. Donc $w_n = O(v_n)$.
  L'autre implication est totalement symétrique.
- On note $M = \{n \in \mathbb{N} \mid w_n \neq 0\}$, il est infini dénombrable (sinon sans intérêt).
  Alors par définition, $\forall\, n \notin M$, $u_n = v_n = w_n = 0$.
  Et pour tout $n \in M$, $\frac{u_n}{w_n}$ et $\frac{v_n}{w_n}$ sont bornées. Donc $\frac{u_n + v_n}{w_n}$ bornée.
- On note $M = \{n \in \mathbb{N} \mid v_n \neq 0\}$, il est infini dénombrable (sinon sans intérêt).
  Alors par définition, $\forall\, n \notin M$, $u_n = v_n = 0$.
  Et pour tout $n \in M$, $\frac{u_n}{v_n}$ est bornée. Donc $\frac{\lambda u_n}{v_n}$ bornée.
- On note $M = \{n \in \mathbb{N} \mid v_n \neq 0\}$, il est infini dénombrable (sinon sans intérêt).
  Alors par définition, $\forall\, n \notin M$, $u_n = v_n = 0$.
  Et pour tout $n \in M$, $\frac{|u_n|}{|v_n|} = \left|\frac{\frac{1}{v_n}}{\frac{1}{u_n}}\right|$ est bornée.
- $\exists\, C > 0, N \in \mathbb{N}$ tels que $\forall\, n \geqslant N$, $|u_n| < C|v_n|$ Donc en multipliant par $|x_n| \geqslant 0$: $|u_n x_n| \leqslant C|v_n x_n|$
- $\exists\, C > 0, N \in \mathbb{N}$ tels que $\forall\, n \geqslant N$, $|u_n| < C|v_n|$ $\exists\, C' > 0, N' \in \mathbb{N}$ tels que $\forall\, n \geqslant N'$, $|w_n| < C'|x_n|$ Donc en multipliant par $|w_n| \geqslant 0$, puis $|x_n| \geqslant 0$:
  $\forall\, n \geqslant \max(N, N')$, $|u_n w_n| \leqslant C|v_n w_n| \leqslant CC'|v_n x_n|$

- On note $M = \{n \in \mathbb{N} \mid v_n \neq 0\}$, il est infini dénombrable (sinon sans intérêt).
  Alors par définition, $\forall\, n \notin M$, $u_n = v_n = 0$.
  Et pour tout $n \in M$, $\frac{|u_n|}{|v_n|}$ est majorée par une constante notée C, donc $\frac{|u_n^\alpha|}{|v_n^\alpha|}$ est majorée par $C^\alpha = f(C)$

□

Proposition - Comparaison logarithmique
Soient (u_n) et (v_n) sont deux suites à termes strictement positifs telles qu'à partir d'un certain rang on ait $\frac{u_{n+1}}{u_n} \leqslant \frac{v_{n+1}}{v_n}$.
Alors $u_n = O(v_n)$.

Corollaire - Demi-critère de D'Alembert
Soit (u_n) est une suite à termes positifs, alors

$$\frac{u_{n+1}}{u_n} \underset{n\to+\infty}{\longrightarrow} \ell < 1 \Longrightarrow u_n \underset{n\to+\infty}{\longrightarrow} 0$$

$$\frac{u_{n+1}}{u_n} \underset{n\to+\infty}{\longrightarrow} \ell > 1 \Longrightarrow u_n \underset{n\to+\infty}{\longrightarrow} +\infty$$

Démonstration
Proposition :
Par positivité des termes de la suite, on a pour tout $n \in \mathbb{N}$: $\frac{u_{n+1}}{v_{n+1}} \leqslant \frac{u_n}{v_n} \leqslant \ldots \frac{u_0}{v_0} = M$.
Donc pour tout $n \in \mathbb{N}$, $u_n \leqslant M v_n$ i.e. $u_n = O(v_n)$.
Corollaire :
Premier cas.
Considérons $m = \frac{\ell+1}{2}$, donc $\ell < m < 1$, puis $v_n = m^n$.
Alors à partir d'un certain rang : $\frac{u_{n+1}}{u_n} \leqslant m = \frac{v_{n+1}}{v_n}$.
D'après la question précédente : $u_n = O(v_n)$. Mais $(v_n) \to 0$ $(m < 1)$, donc $(u_n) \to 0$.
Second cas.
Considérons $m = \frac{\ell+1}{2}$, donc $\ell > m > 1$, puis $v_n = m^n$.
Alors à partir d'un certain rang : $\frac{u_{n+1}}{u_n} \geqslant m = \frac{v_{n+1}}{v_n}$.
D'après la question précédente : $v_n = O(u_n)$. Mais $(v_n) \to +\infty$ $(m < 1)$, donc $(u_n) \to +\infty$. □

6. Bilan

Synthèse

- Des phénomènes récurrent conduisent à des suites. Certaines se calculent explicitement : les suites arithmético-géométrique, récurrente d'ordre 2. Et d'autres non.
- On cherche alors des expressions approchantes et toujours explicites. Ces expressions se devinent à partir de la fin, donc de la limite. Ainsi, il nous faut réfléchir (beaucoup) à la limite de suites, à l'arithmétique associé, à truc et astuce pour déterminer ces limites.
- On est parfois malheureusement contraint d'étudier uniquement des suites extraites.
- Tout est maintenant en place pour pouvoir étudier deux familles de suites typiques (en TD-cours) : les suites définies implicitement (à partir d'une équation), ou les suites définies par une relation d'équivalence. Comme ailleurs, cela conduit à de nombreux savoir-faire à apprendre…

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Etudier une suite arithmético-géométrique
- Savoir-faire - Etudier une suite récurrente linéaire d'ordre 2
- Savoir-faire - Et s'il y a un second membre ?
- Savoir-faire - Montrer la divergence (deuxième type) d'une suite, par suites extraites
- Savoir-faire - A partir de deux certains rangs
- Savoir-faire - Convergence par encadrement/Divergence par minoration (majoration)
- Savoir-faire - A savoir compléter
- Savoir-faire - Gérer ϵ
- Savoir-faire - Souvent pour l'étude de suites complexes
- Savoir-faire - Montrer la convergence de deux sous-suites adjacentes
- Savoir-faire - $u_n = o(v_n)$ avec la notation des limites.
- Savoir-faire - $u_n \sim (v_n)$ avec la notation des limites.
- Savoir-faire - Comment faire si on veut additionner des équivalents ?
- Savoir-faire - $u_n = O(v_n)$ avec la notation des limites.
- Truc & Astuce pour le calcul - Pour manipuler une opération avec $O(a_n)$

Notations

ts	*Propriétés*	*Remarques*
:ge vers ℓ ou diverge vers $\ell = +\infty$	si $\ell \in \mathbb{R} : \forall\, \epsilon > 0, \exists\, N \in \mathbb{N} \mid \forall\, n \geqslant N, \lvert u_n - \ell \rvert \leqslant \epsilon$ si $\ell = +\infty : \forall\, A \in \mathbb{R}, \exists\, N \in \mathbb{N} \mid \forall\, n \geqslant N, u_n > A$	On accepte $u_n \to \ell$
rmation de Cesaro de (u_n)	$\forall\, n \in \mathbb{N}, \left(\mathscr{C}(u)\right)_n = \dfrac{1}{n+1}\displaystyle\sum_{k=0}^{n} u_k$	Si $\lim(u_n) = \ell$, alors $\lim(\mathscr{C}(u)) = \ell$

Retour sur les problèmes

78. Cours : $\forall\, n \in \mathbb{N}$, $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)$.
79. Si on savait répondre à ce genre de question, on serait heureux. Mais comme on n'y arrive pas, on cherche des développements limités explicites et exactes (à un certain ordre près).
80. Les théorème de simple existence de limite utilisent les théorème de convergence monotone, suites adjacentes et plus tard Bolzano-Weierstrass. Aussi les comparaisons de séries positives (plus tard)
Les théorème qui donne la limite exploite la convergence par encadrement, ou les suites extraites. Aussi les séries avec télescopage.
81. La formulation qui fusionne les convergences et divergences vers $\pm\infty$ sera étudiée au chapitre suivant.
82. On exploite les suites extraites. Il y a nécessairement une sous-suite qui ne vérifie pas la propriété en question.

Chapitre 19

Questions topologiques interprétées sur $\mathbb{R}$

Résumé -

Nous commençons par définir la notion de voisinage d'un point de $\overline{\mathbb{R}}$ afin de pouvoir offrir (au chapitre suivant) une définition unifié de la notion de limite de fonction.

Nous ouvrons la porte de la topologie à cette occasion. Nous nous contenterons d'une interprétation de ces idées (topologiques) dans $\mathbb{R}$, ce qui rend les choses assez simple : c'est une question d'intervalle, fermé si besoin. Nous reviendrons sur ces notions en fin d'année…

Sommaire

1. Problèmes 369
2. Halo autour de $a \in \mathbb{R}$ 370
2.1. Voisinages 370
2.2. Intérieur, adhérence 371
3. Intervalles et connexité 374
3.1. Connexité 374
3.2. Intervalle réel 375
3.3. Sur-ensemble : droite numérique achevée 376
4. Segments et compacités 376
4.1. Segments emboîtés 376
4.2. Fonctions d'intervalles et principe de dichotomie . . 377
4.3. Théorème de Bolzano-Weierstrass 379
4.4. Lemme de Cousin 380
5. Curiosité topologique : complétude 382
5.1. Suites de Cauchy 382
5.2. $\mathbb{R}$ est complet 382
6. Bilan 383

1. Problèmes

? Problème 84 - Extension aux suites de la propriété de la borne supérieure

On sait que toute partie majorée de $\mathbb{R}$ admet une borne supérieure. Mais comment « prendre » cette borne supérieure, qui par définition existe mais est insaisissable? Est-ce que les suites peuvent nous aider?

? Problème 85 - Voisinage

La continuité en un point signifie qu'on peut regarder au-delà (ou en-deça) de ce point mais pas nécessairement trop loin.
Si la notion de voisinage du point conceptualise cette idée, quelle définition formelle faut-il donner au voisinage d'un point?
Et si ce point était $+\infty$, est-ce très différent d'un nombre $a \in \mathbb{R}$, quelconque?

? Problème 86 - Pas de trou

Pour définir proprement la continuité de f, il faut qu'il n'y ait pas de trou dans l'ensemble de départ de f…
Comment formaliser/définir les ensembles qui sont en un seul tenant?

? Problème 87 - Principe de dichotomie

Pour construire $\mathbb{R}$, nous nous sommes inspirés de l'algorithme de dichotomie vu au lycée. On « piège » le nombre cherché entre deux nombres maitrisés, puis on réduit de moitié l'intervalle dans lequel il se trouve.
Comment généraliser ce principe pour étudier directement des problèmes. Nous pensons évidemment à la recherche d'une solution d'une équation (polynomiale ou autre) à l'aide du théorème des valeurs intermédiaires.
Quelle méthode générale peut-on tirer de ce principe? Que peut-on démontrer à l'aide de ce principe?

2. Halo autour de $a \in \mathbb{R}$

2.1. Voisinages

Voisinage

Heuristique - Exemple de limite de suites

On a vu que pour les suites il y a deux formalismes différents selon qu'elle converge vers un nombre ℓ ou diverge vers l'infini :

$$\forall\, \epsilon > 0, \exists\, N \in \mathbb{N} \mid \forall\, n \geqslant N, |u_n - \ell| < \epsilon$$

$$\forall\, A > 0, \exists\, N \in \mathbb{N} \mid \forall\, n \geqslant N, u_n > A$$

- $n \geqslant N$, correspond à l'ensemble des voisinages entiers de $+\infty$,
- $\forall\, A, \cdots > A$ à l'ensemble des voisinages réels de $+\infty$
- $\forall\, \epsilon > 0, |\cdots - \ell| < \epsilon$ à l'ensemble des voisinage de ℓ.

Il est préférable d'unifier en une notation ces différents types de voisinage.

Définition - Voisinage d'un point de $\overline{\mathbb{R}}$
Soit $a \in \mathbb{R}$.
$V \subset \mathbb{R}$ est un voisinage de a s'il existe $\epsilon > 0$ tel que $[a-\epsilon, a+\epsilon] \subset V$.
$V \subset \mathbb{R}$ est un voisinage de $+\infty$ s'il existe $A \in \mathbb{R}$ tel que $[A, +\infty[\subset V$
$V \subset \mathbb{R}$ est un voisinage de $-\infty$ s'il existe $B \in \mathbb{R}$ tel que $]-\infty, B] \subset V$
Une propriété est dite vraie au voisinage de $a \in \overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$
si elle est vraie sur un voisinage de a.
On note $\mathcal{V}_a$ l'ensemble des voisinages du point $a \in \overline{\mathbb{R}}$.

Exemple - $[2,3] \cup]4,6[$
est un voisinage de 5.

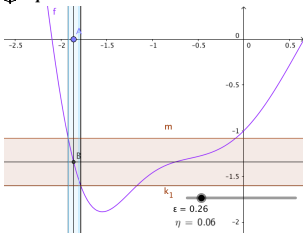
Remarque - Voisinage avec des ouverts
Dans la définition précédente, nous avons considéré des intervalles fermés ($[a-\epsilon, a+\epsilon]$ ou $[A, +\infty[$).
Les définitions restent vraies (et équivalentes) pour des intervalles ouverts car

$$]a - \frac{1}{2}\epsilon, a + \frac{1}{2}\epsilon[\subset [a-\epsilon, a+\epsilon] \subset]a-2\epsilon, a+2\epsilon[$$

Pour aller plus loin - Halo de a
En analyse non standard (cf. wikipedia), on parle de halo de a pour exprimer la même idée que celle de voisinage et on travaille directement avec…
C'est plus pratique lorsqu'il s'agit d'exploiter des infinitésimaux, comme Newton le faisait.

Proposition - Stabilité de voisinage par intersection
Soit $a \in \mathbb{R}$ ou $a \in \{-\infty, +\infty\}$ (i.e. $a \in \overline{\mathbb{R}}$).
- Pour tout voisinage V de a (i.e. $V \in \mathcal{V}_a$), $a \in V$.
- Si $V \in \mathcal{V}_a$ et $V \subset W$, alors $W \in \mathcal{V}_a$.
- L'intersection de deux voisinages de a est un voisinage de a (non vide) :
  $\forall\, V_1, V_2 \in \mathcal{V}_a$, $V_1 \cap V_2 \in \mathcal{V}_a$.
- $\bigcap_{V \in \mathcal{V}_a} = \{a\}$ (borne inférieure…) - *qui n'est pas un voisinage de a.*

Représentation - Illustration



Démonstration
- C'est une conséquence directe de la définition.

Notons que cela est également vrai, si l'on considère des intervalles ouverts (car $\epsilon > 0$)
- (Cas $a \in \mathbb{R}$) Il existe $\alpha > 0$, tel que $[a-\alpha, a+\alpha] \subset V$, donc $[a-\alpha, a+\alpha] \subset W$ et $W \in \mathcal{V}_a$.
  (Cas $a = \infty$) Il existe $A > 0$, tel que $[A, +\infty[\subset V$, donc $[A, +\infty[\subset W$ et $W \in \mathcal{V}_a$.
- Pour le cas $a \in \mathbb{R}$.
  Soient V_1 et V_2, deux voisinages de a.
  Il existe $\alpha_1, \alpha_2 > 0$ tels que $[a-\alpha_1, a+\alpha_1] \subset V_1$ et $[a-\alpha_2, a+\alpha_2] \subset V_2$.
  Considérons $\beta = \min(\alpha_1, \alpha_2)$, alors $[a-\beta, a+\beta] \subset [a-\alpha_1, a+\alpha_1] \subset V_1$ et $[a-\beta, a+\beta] \subset [a-\alpha_2, a+\alpha_2] \subset V_2$.
  Donc $[a-\beta, a+\beta] \subset V_1 \cap V_2$.
  Ainsi $V_1 \cap V_2$ est un voisinage de a.

Pour le cas $a = +\infty$. $[A, +\infty[$ et $[A', +\infty[$ deux voisinages de $+\infty$.
  Alors $[A, +\infty[\cap [A', +\infty[= [\max(A, A'), +\infty[$ est un voisinage de $+\infty$.

De même pour $a = -\infty$.
- D'après la première remarque $a \in \bigcap_{V \in \mathcal{V}_a} V$.

Réciproquement, si $x \in \bigcap_{V \in \mathcal{V}_a} V$ et $x \neq a$.
  (Pour $a \in \mathbb{R}$) On note $\alpha = \frac{a+x}{2}$ (si $a \in \mathbb{R}$), alors $x \notin [a-\alpha, a+\alpha]$, contradiction donc $x = a$.
  (Pour $a = +\infty$) On note $A = x+1$ si $a = +\infty$ et $B = x-1$ si $a = -\infty$… □

Exercice
Soient $\ell_1, \ell_2 \in \overline{\mathbb{R}}$. Montrer que :
Si $\forall\, V \in \mathcal{V}_{\ell_1}$, $\ell_2 \in V$ (i.e $V \in \mathcal{V}_{\ell_2}$), alors $\ell_1 = \ell_2$.

Correction
Directement $\ell_2 \in \bigcap_{V \in \mathcal{V}_{\ell_1}} V = \{\ell_1\}$.

2.2. Intérieur, adhérence

Intérieur

Pour nous, le but des définitions qui suivront est de donner le vocabulaire le plus adaptée aux questions qui se poseront pour définir avec précision la continuité (mais aussi la dérivabilité) des fonctions numériques.

Pour aller plus loin - Généralisation des définitions
Ici, on donne des définitions adaptées à $\mathbb{R}$, elles seront généralisés à tout espace normé en fin d'année.
Dans ce cadre là, nous raisonnerons sur les ensembles directement, et non sur les points comme ici.

Définition - Point intérieur à une partie de $\mathbb{R}$
Soit A une partie de $\mathbb{R}$.
On dit que a est un point intérieur de A, si il existe $\epsilon > 0$ tel que $[a-\epsilon, a+\epsilon] \subset A$.
Ou encore si A est un voisinage de a. On note alors $a \in \mathring{A}$.
$\mathring{A}$ est l'ensemble des points intérieurs de A.

Exemple - Cas d'un intervalle semi-ouvert
Les points intérieurs de $[a, b[$ sont tous les éléments de $]a, b[$.

Proposition - Stabilité
Soit A_1, A_2 deux parties de $\mathbb{R}$ telles que $A_1 \subset A_2$.
Alors $\mathring{A_1} \subset \mathring{A_2}$.

Démonstration
Soit $a \in \mathring{A_1}$.
Alors il existe $\epsilon > 0$ tel que $[a-\epsilon, a+\epsilon] \subset A_1 \subset A_2$.
Donc $a \in \mathring{A_2}$. □

Adhérence et point d'accumulation

Définition - Point adhérent à une partie de $\mathbb{R}$
Soit A une partie de $\mathbb{R}$.
On dit que a est un point adhérant de A, si $\forall\, \epsilon > 0$ tel que $[a-\epsilon, a+\epsilon] \cap A \neq \emptyset$.
On note alors $a \in \overline{A}$.
$\overline{A}$ est l'ensemble des points adhérents de A.

Attention - Ne pas confondre…
Point adhérent à une partie et valeur d'adhérence d'une suite.

Exemple - Cas d'un intervalle semi-ouvert
Les points adhérents de $[a, b[$ sont tous les éléments de $[a, b]$.

Pour aller plus loin - Ouverts et fermés de $\mathbb{R}$
Globalement, les ensembles ouverts sont les ensembles A qui vérifient $A = \mathring{A}$.
Les ensembles fermés sont les ensembles A qui vérifient $A = \overline{A}$.

Proposition - Stabilité
Soit A_1, A_2 deux parties de $\mathbb{R}$ telles que $A_1 \subset A_2$.
Alors $\overline{A_1} \subset \overline{A_2}$.

Démonstration
Soit $a \in \overline{A_1}$.
Alors pour tout $\epsilon > 0$, $[a-\epsilon, a+\epsilon] \cap A_1$ et non vide.
  Or $[a-\epsilon, a+\epsilon] \cap A_2$ contient celui-ci, il est donc également non vide.
Donc $a \in \overline{A_2}$. □

On a parfois besoin d'une suite convergente vers a, tout en étant différente de a.

Définition - Point d'accumulation
On dit que a est un point d'accumulation de A
  si $\forall\, \epsilon > 0$ tel que $\left[[a-\epsilon, a+\epsilon] \cap A\right] \setminus \{a\} \neq \emptyset$.
Autrement écrit a est un point d'accumulation ssi $a \in \overline{A \setminus \{a\}}$.

Remarque - Points isolés
Comme $\left[[a-\epsilon, a+\epsilon] \cap A\right] \setminus \{a\} \subset \left[[a-\epsilon, a+\epsilon] \cap A\right]$, tout point d'accumulation de A est un point adhérent de A.
Les points adhérents qui ne sont pas d'accumulation sont appelés points isolés.

Exemple - Point d'accumulation de $A = \{0\} \cup [1,4[$
$\overline{A} = \{0\} \cup [1,4]$.
Les points d'accumulation de A sont les points de $[1,4]$. 0 est un point isolé de A.
Exercice
Montrer que si a est un point d'accumulation, alors dans chaque voisinage de a, il existe une infinité de points de A.

Correction
Soit $\epsilon > 0$. Supposons que $[a-\epsilon, a+\epsilon] \cap A$ ne contient qu'un nombre fini de points distincts : $x_1, x_2, \dots x_r$ et distincts de a.
Notons $\delta = \min\{|a - x_i|, i \in \mathbb{N}_r\}$. Alors $[a - \frac{\delta}{2}, a + \frac{\delta}{2}] \cap A = \{a\}$. Impossible.

Les points adhérents sont les points que l'on peut approcher par des points de A, ou encore pour lesquels la question du calcul de $\lim_{x \to a, x \in A}$ a un sens.

Les points d'accumulation sont les points que l'on peut approcher par des points de $A \setminus \{a\}$, ou encore pour lesquels la question du calcul de $\lim_{x \to a, x \in A, x \neq a}$ a un sens.

Proposition - Suite convergente d'éléments de A
Soit A une partie de $\mathbb{R}$. Soit $a \in A$
a est adhérent à A si et seulement si il existe $(a_n) \in A^{\mathbb{N}}$ tel que $a = \lim(a_n)$.
Les points adhérents de A sont toutes les limites possibles d'éléments de A.

Démonstration
Supposons que $a \in \overline{A}$.
alors pour tout $n \in \mathbb{N}$, en prenant $\epsilon \to \frac{1}{n}$, il existe $a_n \in A \cap [a - \frac{1}{n}, a + \frac{1}{n}]$.
les points a_n sont à valeurs dans A et : $\forall \epsilon > 0$, i$\exists N = \lfloor \frac{1}{\epsilon} \rfloor + 1$ tel que $\forall n \geqslant N, |a - a_n| \leqslant \frac{1}{N} \leqslant \epsilon$.
Donc $(a_n) \to a$.
Réciproquement, supposons qu'il existe une suite $(a_n) \in A^{\mathbb{N}}$ convergente vers a.
alors pour tout $\epsilon > 0$, $\exists N \in \mathbb{N}$ tel que $|a - a_N| \leqslant \epsilon$,
Donc $\forall \epsilon > 0$, $[a-\epsilon, a+\epsilon] \cap A \neq \{0\}$. □

Complément sur la borne supérieure (inférieure)

Proposition - Borne supérieure
Soit X une partie non vide majorée de $\mathbb{R}$. Soit M un majorant de X.
$M \in \overline{X}$ (M est adhérent de X). Plus précisément, c'est le seul majorant adhérent à X : Alors $M = \sup X$ si et seulement si il existe une suite d'éléments de X qui converge vers M.

Exercice
Donner la caractérisation équivalente pour $m = \inf X$

Correction
m un minorant de X.
$m = \inf X$ si et seulement si il existe une suite d'éléments de X qui converge vers m

Démonstration
On considère $\epsilon = \frac{1}{n}$.
Si $M = \sup X$,
alors pour tout $\epsilon = \frac{1}{n}$, il existe $x_n \in X$ tel que $x_n \leqslant M < x_n + \epsilon = x_n - \frac{1}{n}$.
donc pour tout $n \in \mathbb{N}$, $0 \leqslant M - x_n < \frac{1}{n}$ et donc par comparaison : $(x_n) \to M$.
Réciproquement, s'il existe une suite (x_n) d'éléments de X qui converge vers M,
alors pour tout majorant Mm de X, on a $x_n \leqslant Mm$ et en passant à la limite $M \leqslant Mm$.
Donc, si en outre M majore X, c'est le plus petit des majorants, donc $M = \sup X$. □

Densité dans $\mathbb{R}$

Remarque - Rappel de la définition de la densité
On dit qu'une partie X est dense dans $\mathbb{R}$,
si pour tout $a \in \mathbb{R}$ et $\forall \epsilon > 0$, il existe $x \in X$ tel que $|a - x| < \epsilon$.
ssi pour tout $a \in \mathbb{R}$ et $\forall \epsilon > 0$, $]a-\epsilon, a+\epsilon[\cap X \neq \emptyset$

Proposition - Densité
Une partie X de $\mathbb{R}$ est dense dans $\mathbb{R}$
ssi $\overline{X} = \mathbb{R}$ ($\mathbb{R}$ est égal à l'adhérence de X.)
ssi pour tout a réel il existe $(x_n) \in X^{\mathbb{N}}$ telle que $(x_n) \to a$.

Démonstration
Supposons X dense dans $\mathbb{R}$,
Soit $a \in \mathbb{R}$, prenons $\epsilon = \frac{1}{n}$, puis $x_n \in X$ tel que $|a - x_n| < \epsilon = \frac{1}{n}$.
Alors $\lim(a - x_n) = 0$, donc $\lim(x_n) = a$.
Donc il existe une suite (x_n) d'éléments de X tel que $\lim(x_n) = a$, pour tout $a \in \mathbb{R}$.
Réciproquement, supposons que pour tout a réel il existe $(x_n) \in X^{\mathbb{N}}$ qui converge vers a.
Soit $\epsilon > 0$, alors il existe N tel que $\forall n \geqslant N$, $|a - x_n| < \epsilon$.
Ce $x_N \in X$ convient et permet d'affirmer la densité de X dans $\mathbb{R}$. □

Proposition - Densité des rationnels dans $\mathbb{R}$
La densité des rationnels dans $\mathbb{R}$ permet d'affirmer que :
tout nombre réel est limite d'une suite de rationnels.

Remarque - On a mieux encore...
Mieux encore : tout réel est limite d'une suite décroissante (resp. croissante) de rationnels.
Cette dernière affirmation est laissé en exercice, on peut reprendre le lemme des pics...

3. Intervalles et connexité

3.1. Connexité

Le but est donné un nom propre aux ensembles « continues », i.e. sans trou afin d'appliquer le théorème des valeurs intermédiaires.

Définition - Ensemble séparé
Soient A et B, deux parties de $\mathbb{R}$.
On dit A et B sont séparés si $A \cap \overline{B} = \emptyset$ et $\overline{A} \cap B = \emptyset$.
Aucun point de A n'est dans l'adhérence de B, aucun point de B n'est dans l'adhérence de A.

Exemple - Cas de $A =]0,1[$ et $B =]1,2]$ ou $B = [1,2]$
$]0,1[$ et $]1,2]$ sont bien séparés.
En revanche $]0,1[$ et $[1,2]$ ne sont pas bien séparés car $1 \in [1,2] \cap \overline{]0,1[}$.

Définition - Ensemble connexe
Soit E une partie de $\mathbb{R}$.
On dit que E est connexe, si on ne peut pas l'écrire comme réunion de deux sous-ensembles séparés non vide.

Exemple - Réunion d'intervalle
On voit bien que $[0,1]\cup[3,4]$ n'est pas connexe.
Et plus difficilement que $[0,4]$ est connexe.
Exercice
Faire la démonstration de $[0,4]$ est connexe.

Correction
Par l'absurde, si $[0,4]$ n'est pas connexe, il existe A et B tel que $A\cup B=[0,4]$ et $A\cap\overline{B}=\emptyset$ et $\overline{A}\cap B=\emptyset$.
SPDG, on peut supposer que $0\in A$ et il existe $b\in B$.
Notons $A'=\{s\in[0,4]\mid\forall\ u\in[0,s],u\in A\}$. $0\in A'$ donc $A'\neq\emptyset$.
A' est majoré par b, donc A' admet une borne supérieure a.
$a\in[0,4]=A\cup B$.
ou bien $a\in B$ et donc $a\notin A$, mais il existe $(s_n)\in A'(\subset A)$ tel que $a=\lim(s_n)$, donc $a\in\overline{A}$.
C'est impossible car $B\cap\overline{A}=\emptyset$.
ou bien $a\in A$. Pour tout $\epsilon>0$, il existe $t\in B\cap[a,a+\epsilon]$, sinon, $\sup A'\geqslant a+\epsilon$.
Donc $a\in\overline{B}$. Ce qui est tout autant impossible.
On a donc une contradiction : $[0,4]$ est connexe.

La méthode s'adapte à tout intervalle. Ainsi, dans $\mathbb{R}$, tous les intervalles (même ouverts) sont connexes.

Pour aller plus loin - Connexe par arcs
La stratégie classique dans les espaces plus grands que $\mathbb{R}$, pour démontrer qu'un ensemble A est connexe, est de montrer qu'il est « connexe par arcs », i.e. pour tout $a,b\in A$, il existe une application γ (dite chemin) continue de $[0,1]$ dans A tel que $\gamma(0)=a$ et $\gamma(1)=b$.

Savoir faire - Montrer qu'une partie de $\mathbb{R}$ est connexe
La méthode consiste souvent à faire un raisonnement par l'absurde et à travailler à partir du nombre x_0 qui est obtenu comme borne supérieure d'un ensemble A (à inventer) et élément de B ou bien élément de A et borne inférieure de B.
A partir de ce x_0, trouver une contradiction.

3.2. Intervalle réel

Intervalles

Définition - Caractérisation des intervalles de $\mathbb{R}$
Soit I une partie non vide de $\mathbb{R}$. On dit que I est un intervalle de $\mathbb{R}$ si il vérifie :
$$\forall\ x<y\in I,\qquad\{t\in\mathbb{R}\mid x\leqslant t\leqslant y\}\subset I$$
(I est une partie convexe de $\mathbb{R}$).
On notera, ensuite, plus simplement $[x,y]$ l'ensemble $\{t\in\mathbb{R}\mid x\leqslant t\leqslant y\}$ dont il est question dans la définition.

Exemple - Ensemble des majorants d'une partie majorée
Soit A une partie de $\mathbb{R}$, majorée.
On note I l'ensemble des majorants de A
Alors pour tout $x<y\in I$, $\forall\ t\in[x,y]$, $\forall\ a\in A$, $a\leqslant x\leqslant t$.
Donc $t\in I$ et donc $[x,y]\subset I$.
Ainsi I est un intervalle de $\mathbb{R}$.
Plus précisément, on montre que $I=[\sup A,+\infty[$.

Proposition - Intervalles de $\mathbb{R}$
Tout intervalle de $\mathbb{R}$ est de la forme (a,b), avec $a<b$ et $a,b\in\overline{\mathbb{R}}$.
Par notation "(","$)"\in\{"[","]"\}$.
Ce qui revient au même que de montrer qu'il existe $a,b\in\overline{\mathbb{R}}$ tel que $]a,b[\subset I\subset[a,b]$.

Démonstration
Sur $\overline{R}$, I est une partie de $\mathbb{R}$, donc admet une borne supérieure et inférieure dans $\overline{R}$.
Donc il existe $a,b\in\overline{R}$ tel que $I\subset[a,b]$.
Puis, comme il s'agit d'un intervalle, on a $\forall\ x\in]a,b[$, $\exists\ x_a\in]a,x[\cap I$ et $x_b\in]x,b[\cap I$ et donc $x\in[x_a,x_b]\subset I$.
Donc $]a,b[\subset I$. □

On a vu que dans $\mathbb{R}$, les intervalles étaient connexes. La réciproque est vraie .

Proposition - Les connexes de $\mathbb{R}$
Si X est un connexe de $\mathbb{R}$, alors X est un intervalle.

Démonstration
Soit $a,b\in X$. Soit $t\in[a,b]$.
Supposons, par l'absurde, que $t\notin X$.
Notons $A=X\cap]-\infty,t[$ et $B=X\cap]t,+\infty[$.
Alors $A\cup B=X\cap(]-\infty,t[\cup]t,+\infty[)=X\setminus\{t\}=X$ car $t\notin X$.
A est non vide car $a\in A$ et B est non vide car $b\in B$.
$A\subset]-\infty,t[$ donc $\overline{A}\subset]-\infty,t]$ et $B\subset]t,+\infty[$, donc $\overline{A}\cap B=\emptyset$.
$A\subset]-\infty,t[$ et $B\subset]t,+\infty[$ donc $\overline{B}\subset[t,+\infty[$, donc $A\cap\overline{B}=\emptyset$.
On a donc trouver de quoi séparer X, ce qui est impossible car X est connexe.
Par conséquent $t\in X$, et donc X est un intervalle de $\mathbb{R}$. □

3.3. Sur-ensemble : droite numérique achevée

Heuristique - Donner une borne supérieure à une partie non majorée
Cela correspond à donner une borne supérieure : $+\infty$ à une partie non majorée de $\mathbb{R}$ et une borne inférieure : $-\infty$ à une partie non minorée de $\mathbb{R}$.
Cela permet d'écrire certaines propriétés de manière plus simple en différenciant moins de cas.
Par exemple, le théorème fondamental n'est plus : *toute partie bornée de $\mathbb{R}$ admet une borne supérieure*, mais il devient *toute partie de $\overline{\mathbb{R}}$ admet une borne supérieure*

Définition - Droite numérique achevée $\overline{\mathbb{R}}$
On définit : $\overline{\mathbb{R}}=\mathbb{R}\cup\{-\infty,+\infty\}$ où $-\infty,+\infty\notin\mathbb{R}$
et on prolonge la relation d'ordre $\leqslant$ sur $\overline{\mathbb{R}}$ en posant
$$\forall x\in\overline{\mathbb{R}},\ x\leqslant+\infty\text{ et }x\geqslant-\infty.$$

Pour aller plus loin - $\overline{R}_+$
On verra dans le chapitre sur les séries (et d'une certaine façon sur l'intégrale), que l'ensemble $\overline{R}_+=\mathbb{R}\cup\{+\infty\}$ est intéressant pour construire certains objets : séries/intégrales. En effet, pour cet ensemble, toute suite croissante est nécessairement convergente…

Attention - Mais il y a un coût…
Il est difficile d'étendre les opérations + et × à $\overline{\mathbb{R}}$ sans aboutir à des incohérences ;
pour « $0\times+\infty$, $0\times-\infty$ et $(+\infty)+(-\infty)$ ».

Ce que l'on gagne :

Proposition - Existence de la borne supérieure
Dans $\overline{\mathbb{R}}$, toute partie de $\mathbb{R}$ admet une borne supérieure et une borne inférieure

Démonstration
Soit $A\subset\mathbb{R}$,
— ou bien A est majoré, et donc A admet une borne supérieure (dans $\mathbb{R}$)
— ou bien A n'est pas majoré et donc $\sup A=+\infty$.
□

4. Segments et compacités

4.1. Segments emboîtés

Segment

Définition - Segment
On appelle segment de $\mathbb{R}$, tout intervalle fermé et borné de $\mathbb{R}$.

Remarque - Listes
Les segments de $\mathbb{R}$ sont exactement les ensembles $[a,b]$, $[a,+\infty[$, $]-\infty,b]$ et $]-\infty,+\infty[$, où $a,b\in\mathbb{R}$ avec $a\leqslant b$.
En revanche $[a,b[$ n'est pas fermé donc n'est pas un segment.
Et $[a,b]\cup[c,d]$ avec $b<c$ n'est pas non plus un segment

Suite de segments emboités de limite nulle

En exploitant les suites adjacentes réelles :

Proposition - Théorème des segments emboîtés de longueur tendant vers 0
Soit $(I_n)_{n\in\mathbb{N}}$ une suite de segments emboîtés (i.e. $I_{n+1}\subset I_n$), de longueur tendant vers 0 (i.e. si $I_n=[a_n,b_n]$ alors $b_n-a_n\underset{n\to+\infty}{\longrightarrow}0$).
Alors leur intersection est un singleton :

$$\exists \ell\in\mathbb{R}\mid \bigcap_{n\in\mathbb{N}} I_n=\{\ell\}.$$

Démonstration
Existence :
Puisque les segments $([a_n,b_n])_n$ sont emboités : $a_n<a_{n+1}<b_{n+1}<b_n$.
Donc la suite (a_n) est croissante et la suite (b_n) est décroissante.
Et comme $(b_n-a_n)\to 0$, les suites (a_n) et (b_n) sont adjacentes.
On note ℓ, la limite commune de ces deux suites.
On a alors $\forall\, n\in\mathbb{N}: a_n\leqslant\ell\leqslant b_n$, donc $\ell\in[a_n,b_n]$, donc $\ell\in\bigcap_{n\in\mathbb{N}}I_n$.
Unicité :
Et si $x\in\bigcap_{n\in\mathbb{N}}I_n$, on a alors pour tout $n\in\mathbb{N}$, $a_n\leqslant x\leqslant b_n$,
puis en passant à la limite : $\ell\leqslant x\leqslant\ell$ et donc $x=\ell$.
Finalement : $\bigcap_{n\in\mathbb{N}}I_n=\{\ell\}$ □

4.2. Fonctions d'intervalles et principe de dichotomie

Fonctions d'intervalles

Définition - Fonctions d'intervalles. Sous-additivité
On appelle fonction d'intervalles de (a,b) une application F de l'ensemble des sous-intervalles de (a,b) dans $\mathbb{R}$.
On dit que F est sous-additive sur (a,b) si

$$\forall\ \alpha<\beta<\gamma\in[a,b],\qquad F(\alpha,\gamma)\leqslant F(\alpha,\beta)+F(\beta,\gamma)$$

Exemple - L'intégrale de f
$F_f:(\alpha,\beta)\mapsto\int_\alpha^\beta f(t)\mathrm{d}t$ est une fonction d'intervalles.
Elle est additive selon le théorème de Chasles : $F_f(\alpha,\beta)+F_f(\beta,\gamma)=F_f(\alpha,\gamma)$.
En particulier pour $f=1$: $F_1:(\alpha,\beta)\mapsto\beta-\alpha$ est une fonction d'intervalles

Définition - Fonction paramétrée par une famille de propositions
Soit $(\mathscr{P}_I)_{I\subset[a,b]}$, une famille de propositions sur les sous-intervalles de $[a,b]$.
L'application $f_{\mathscr{P}}:(\alpha,\beta)\mapsto[\mathscr{P}_{[\alpha,\beta]}]=\begin{cases}1 & \text{si } \mathscr{P}_{[\alpha,\beta]} \text{ vraie}\\ 0 & \text{si } \mathscr{P}_{[\alpha,\beta]} \text{ fausse}\end{cases}$ est une fonction d'intervalles.

Histoire - (Frigyes (Frederic) Riesz



Frigyes Riesz (1781-1848) est un mathématicien hongrois à l'origine d'une grande école de mathématiques hongroise (analyse et arithmétique et plus) qui a subit une forme de "dispora" entre les deux guerres mondiales.
Il formalise avec Nagy, la notion de fonctions d'intervalles dans l'ouvrage Leçons d'analyse fonctionnelle.

Savoir faire - Sous-additivité pour un fonction d'intervalle définie par une propriété
Dans ce cas, on doit vérifier :

$$\forall\ \alpha,\beta,\gamma\in[a,b],\qquad f_{\mathscr{P}}(\alpha,\gamma)\leqslant f_{\mathscr{P}}(\alpha,\beta)+f_{\mathscr{P}}(\beta,\gamma)$$

Or $f_{\mathscr{P}}$ est à valeurs dans $\{0,1\}$. Donc la sous-additivité est équivalente au fait que

$$f_{\mathscr{P}}(\alpha,\beta)=f_{\mathscr{P}}(\beta,\gamma)=0\Longrightarrow f_{\mathscr{P}}(\alpha,\gamma)=0$$

Principe de Dichotomie

Le principe suivant nous sera utile plusieurs fois par la suite, toujours à propos de résultats très fins sur $\mathbb{R}$ (Bolzano-Weierstrass, Cousin, valeurs intermédiaires…)

Pour aller plus loin - Récurrence
Il s'agit d'une sorte de raisonnement en descente infinie (donc non constructive…) basée sur une partie (fermé et bornée) de $\mathbb{R}$ et non sur $\mathbb{N}$ entier

Proposition - Processus de dichotomie
Soit $[a,b]$ un segment (intervalle fermé et borné) de $\mathbb{R}$.
Soit $(\mathscr{P}_I)$, une famille de propositions définie sur l'ensemble des sous-segments de $[a,b]$.
Supposons que $f_{\mathscr{P}}$ la fonction d'intervalles paramétrée par $(\mathscr{P}_I)$ est sous-additive.
Si $f_{\mathscr{P}}(a,b)=1$, il existe (a_n), (b_n) adjacentes dans $[a,b]$ (ou une suite de segments $([a_n,b_n])_{n\in\mathbb{N}}$ emboités de longueur tendant vers 0) tel que pour tout $n\in\mathbb{N}$, $f_{\mathscr{P}}(a_n,b_n)=1$.

Remarque - Simplification des notations
Souvent $\mathscr{P}$ n'apparaitra pas dans la notation. Voyons en action ce principe, même si les objets suivants ne sont pas encore bien définis.
La structure d'application est proche de celle de la récurrence ou plutôt de la méthode de la descente infinie de Fermat.

Application - Anticipation : TVI
Soit φ une application continue sur $[a,b]$ tel que $\varphi(a)\geqslant 0$ et $\varphi(b)\leqslant 0$.
alors il existe $x\in[a,b]$ tel que $\varphi(x)=0$.
On note $f(\alpha,\beta)=[\varphi(\alpha)\times\varphi(\beta)\leqslant 0]$ (i.e. $\varphi(\alpha)$ et $\varphi(\beta)$ de signes opposés).
• Soient $\alpha<\beta<\gamma\in[a,b]$

$$f(\alpha,\beta)=f(\beta,\gamma)=0\Rightarrow\varphi(\alpha)\varphi(\beta)>0\,\&\,\varphi(\beta)\varphi(\gamma)>0\Rightarrow\varphi(\alpha)\varphi(\beta)\varphi(\beta)\varphi(\gamma)>0\Rightarrow f(\alpha,\gamma)=0$$

Donc f est sous-additive.
• Or $f(a,b)=1$, donc il existe (a_n) et (b_n) adjacentes telles que $\forall\, n\in\mathbb{N}$, $f(a_n,b_n)=1$ est fausse.
On note $x=\lim(a_n)(=\lim(b_n))$. Pour tout $n\in\mathbb{N}$, $\varphi(a_n)\varphi(b_n)\leqslant 0$
Puis par continuité de φ : $0\leqslant\varphi(x)^2=\lim\varphi(a_n)\varphi(b_n)\leqslant 0$:
$\varphi(x)^2=0$. Donc $\varphi(x)=0$.

Démonstration
Supposons que $f_{\mathscr{P}}(a,b)=1$.
Alors en prenant $c=\frac{a+b}{2}$, on a nécessairement $f_{\mathscr{P}}(a,c)=1$ ou $f_{\mathscr{P}}(c,b)=1$.
sinon par hérédité, $f_{\mathscr{P}}(a,b)=0$.
On reprend cette même idée, pour créer par récurrence une suite $(I_n)=([a_n,b_n])$ telle que $f_{\mathscr{P}}(a_n,b_n)=1$. Puis on continue la construction de la même manière (récurrence) :

$$\exists\,(I_n)\qquad\text{telle que}\qquad\begin{cases}I_0=[a,b],\\ \forall\, n\in\mathbb{N}, b_n-a_n=\frac{b-a}{2^n}\\ \forall\, n\in\mathbb{N}, I_{n+1}\subset I_n\\ \forall\, n\in\mathbb{N}, f_{\mathscr{P}}(a_n,b_n)=1\end{cases}$$

En effet, si on note $I_n=[a_n,b_n]$, avec $f_{\mathscr{P}}(a_n,b_n)=1$,
alors avec $c_n=\frac{a_n+b_n}{2}$, on a alors $f_{\mathscr{P}}(a_n,c_n)=1$ (H_1) ou $f_{\mathscr{P}}(c_n,b_n)=1$ (H_2)(ou les deux).
On considère alors $I_{n+1}=[a_n,c_n]$ dans le cas (H_1) et $I_{n+1}=[c_n,b_n]$ dans le cas (H_2).
La construction de la suite (I_n), par récurrence, est alors assurée. □

Remarque - Longueur de I_n

On peut même affirmer, avec la même démonstration, que $b_n - a_n = \dfrac{b-a}{2^n}$.
Analysez bien les deux types d'applications du processus de dichotomie du savoir-faire. Dans quel cas se trouve l'application qui conduit au TVI?

Savoir faire - Comment exploiter le « processus de dichotomie ».

De manière générale, on exploite le processus de dichotomie de deux façons :

- Pour mettre en avant un objet x qui vérifie une propriété particulière. On le construit en tant que limite des suites adjacentes qui émergent. On suit un mouvement descendant.
  (C'est le cas de la démonstration du théorème de BOLZANO-WEIERSTRASSS).
- Pour montrer une propriété vraie sur un intervalle compact (global). On le couple à un raisonnement par l'absurde. On suit un mouvement ascendant.
  (C'est le cas de la démonstration du lemme de COUSIN).

4.3. Théorème de Bolzano-Weierstrass

Théorème - Théorème de Bolzano-Weierstrass
De toute suite réelle bornée on peut extraire une suite convergente.

On a le corollaire (équivalent) :

Corollaire - Suite de points d'un segment
Soit (u_n) une suite de points du segment $[a,b]$. Alors il existe une suite extraite convergente.

Démonstration
On considère une suite $(x_n) \in [a,b]$.
On note pour tout couple $(\alpha,\beta) \in [a,b]$, $f(\alpha,\beta) = \begin{cases} 1 & \text{si } \{n \in \mathbb{N} \mid x_n \in [\alpha,\beta]\} \text{ est infini} \\ 0 & \text{si } \{n \in \mathbb{N} \mid x_n \in [\alpha,\beta]\} \text{ est fini} \end{cases}$
Pour tout $\alpha < \beta < \gamma \in [a,b]$,

$$\{n \in \mathbb{N} \mid x_n \in [\alpha,\gamma]\} = \{n \in \mathbb{N} \mid x_n \in [\alpha,\beta]\} \cup \{n \in \mathbb{N} \mid x_n \in [\beta,\gamma]\}$$

Donc $f(\alpha,\gamma) \leqslant f(\alpha,\beta) + f(\beta,\gamma)$.
Par ailleurs $f(a,b) = 1$.
Ainsi, avec le processus de dichotomie :
il existe (a_n) et (b_n) adjacentes telles que $f(a_n,b_n) = 1$.
On note $x = \lim(a_n) (= \lim(b_n))$.
Comme, pour tout $k \in \mathbb{N}$, $N_k = \{n \in \mathbb{N} \mid x_n \in [a_k,b_k]\}$ est infini.
On construit alors par récurrence $(n_k)_{k\in\mathbb{N}}$ par

$$n_0 = \min N_0 \qquad n_{k+1} = \min\{N_{k+1} \cap [\![n_k+1, +\infty[\![\subset \mathbb{N}, \text{ non vide}\}$$

Et alors (x_{n_k}) est une suite extraite de (x_n) et $x_{n_k} \in [a_{n_k}, b_{n_k}]$ donc $\lim x_{n_k} = x$. □

On pourrait également exploiter le lemme des pics. Mais il est hors-programme, il faut donc d'abord commencer par le (re)démontrer.

Savoir faire - Suite-extraite dans N_k

Dans la démonstration, on a exploité une idée intéressante à savoir reformaliser.
S'il existe une suite (N_k) de sous-ensembles de $\mathbb{N}$, tel que pour tout k, N_k est infinie.
Alors, il existe une suite (v_k) strictement croissante telles que $\forall\, k \in \mathbb{N}$, $v_k \in N_k$.

Pour aller plus loin - Propriété de compacité

Un ensemble est compact, s'il est complet et précompact, c'est-à-dire ***fini à ϵ-près****.*
Une autre définition possible pour la compacité est celle de pouvoir vérifier le critère de Bolzano-Weierstrass…
Tout segment de $\mathbb{R}$ est compact (donc fini à ϵ-près - nous en reparlerons avec le lemme de Cousin).
Nous prendrons une définition générale en fin d'année lorsqu'on étudiera la topologie sur $\mathbb{R}^2$ voire $\mathbb{R}^n$. Il faudra alors généraliser ce que l'on voir ici…

Histoire - Bernard Bolzano



Bernard Bolzano (1781-1848) est un prêtre mathématicien tchèque.

, Il suffit de prendre $v_{k+1} := \min(N_{k+1} \cap [\![v_k+1, +\infty[\![)$.

Théorème - Théorème de Bolzano-Weierstrass
De toute suite complexe bornée on peut extraire une suite convergente.

Pour la démonstration, on exploite le critère précédent.
La subtilité : il y a deux suites extraites, a priori.

Démonstration
On considère une suite $(z_n) \in \mathbb{C}^{\mathbb{N}}$, bornée.
Notons (x_n), respectivement (y_n) la suite des parties réelles, resp. imaginaires de (z_n).
Pour tout $n \in \mathbb{N}$, $|x_n| \leqslant |z_n|$ et $|y_n| \leqslant |z_n|$. Donc ces deux suites sont bornées.
On exploite le TBW pour (x_n). Il existe $\varphi_1 : \mathbb{N} \to \mathbb{N}\nearrow$ tel que $x_{\varphi_1(n)}$ converge.
Puis la suite $(y_{\varphi(n)})$ est également bornée,
Il existe $\varphi_2 : \mathbb{N} \to \mathbb{N}\nearrow$ tel que $y_{\varphi_1(\varphi_2(n))}$ converge.
Alors $z_{\varphi_1\circ\varphi_2(n)} = x_{\varphi_1(\varphi_2(n))} + y_{\varphi_1(\varphi_2(n))}$ converge. □

4.4. Lemme de Cousin

Heuristique - Pourquoi le lemme de Cousin?

Le lemme de Cousin est une formulation particulièrement efficace des propriétés de compacité de $\mathbb{R}$.
Bien qu'il ne soit pas au programme officiel de la MPSI (ni de la MP), il figure dans ce cours car

- Il est vrai
- Il est commode. Nous l'exploiterons à quelques reprises dans le prochain chapitre de cours
- Il est nécessaire à la construction d'une intégrale robuste sur $\mathbb{R}$: l'intégrale de Kurzweil-Henstock que nous construirons au deuxième semestre.

Cela commence par deux définitions.

Définition - Subdivision pointée
Soit $I = [a,b]$, un segment de $\mathbb{R}$.
On appelle subdivision pointée de I la donnée

- d'une subdivision (finie!) $\sigma = (x_0, x_1, \dots x_n)$ de $[a,b]$,
  $\forall\, i \in \mathbb{N}_{n-2}$, $a = x_0 \leqslant x_i \leqslant x_{i+1} \leqslant x_n = b$
- un pointage de cette subdivision $t_1, t_2, \dots t_n \in I$ tels que
  $\forall\, i \in \mathbb{N}_n$, $t_i \in [x_{i-1}, x_i]$.

On la notera $\sigma_p = \{([x_0,x_1],t_1),([x_1,x_2],t_2),\dots([x_{n-1},x_n],t_n)\}$, on appelera les (t_i) les points de marquage de σ_p.

Histoire - Pierre Cousin

Pierre Cousin (1867-1933) est un mathématicien français.
Peu (re)connu, cet élève d'Henri Poincaré a pourtant eu des intuitions prémonitoires concernant le théorèmes de Borel et Lebesgue. Sa vie reste un mystère (pas de iconographie reconnue, par exemple)

Définition - Subdivision pointée adaptée à un jauge
Un pas ou une jauge est une application $\delta : [a,b] \to \mathbb{R}_+^*$.
Une subdivision $\sigma_p = \{([x_0,x_1],t_1),([x_1,x_2],t_2),\dots([x_{n-1},x_n],t_n)\}$ est dite adaptée au pas δ ou δ-fine, si

$$\forall\, k \in \mathbb{N}_n, \qquad [x_{k-1},x_k] \subset \left[t_k - \frac{\delta(t_k)}{2}, t_k + \frac{\delta(t_k)}{2}\right]$$

On remarquera que $0 \leqslant x_k - x_{k-1} \leqslant \delta(t_k)$

Attention - Strictement positif

Il est important que $\delta(\cdot) > 0$, comme on va le voir dans la démonstration du lemme de Cousin.
Par contre, il n'est pas nécessaire que δ soit continue

Remarque - Compacité

On voit bien sur ces définitions l'importance de voir I, comme une réunion finie de sous-ensemble défini à un pas (variable) près

Théorème - Lemme de COUSIN

Pour tout δ, jauge sur $[a,b]$, il existe une subdivision pointée
$\sigma_p = \{([x_0,x_1],t_1),([x_1,x_2],t_2),\dots([x_{n-1},x_n],t_n)\}$, adaptée à δ (δ-fine)

Remarque - Une question de recouvrement

Etant donné δ, l'existence d'une subdivision pointée δ-fine signifie que $[a,b]$ est recouvert par deux réunions finies :

— $[a,b] = \bigcup_{i\in\mathbb{N}_n} [x_{i-1},x_i]$, réunion disjointe (aux extrémités près)

— $[a,b] \subset \bigcup_{i\in\mathbb{N}_n} \left[t_i - \frac{\delta(t_i)}{2}, t_i + \frac{\delta(t_i)}{2}\right]$, réunion débordante mais bien résumée par δ en un nombre fini de points.

Exercice

Formaliser le lemme de COUSIN

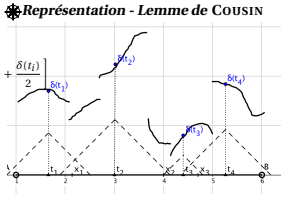
Correction

$\forall\, \delta : [a,b] \to \mathbb{R}_+^*, \exists\, n\in\mathbb{N}, \exists\, x_0(=a) \leqslant t_1 \leqslant x_1, \leqslant \dots \leqslant t_n \leqslant x_n(=b) \mid \forall\, i\in\mathbb{N}_n, [x_{i-1},x_i] \subset \left[t_i - \frac{\delta(t_i)}{2}, t_i + \frac{\delta(t_i)}{2}\right]$

Démonstration

Soit $\delta > 0$ une jauge sur $[a,b]$.
Notons pour tout $[\alpha,\beta] \subset [a,b]$, $f(\alpha,\beta)$: « il n'existe pas de subdivisions pointées $\delta_{|[\alpha,\beta]}$ fine de $[\alpha,\beta]$ ».
1. Montrons d'abord qu'on peut appliquer le processus de dichotomie.
Si $f(\alpha,\beta) = 0$ et $f(\beta,\gamma) = 0$ alors la simple concaténation des subdivision pointée $\delta_{|[\alpha,\beta]}$ et $\delta_{|[\beta,\gamma]}$ fines donne une subdivision $\delta_{|[\alpha,\beta]}$ fine. Donc $f(\alpha,\gamma) = 0$.
2. Raisonnons alors par l'absurde. Supposons donc que $f(a,b) = 1$.
Donc il existe (a_n), (b_n) adjacentes telles que $\forall\, n\in\mathbb{N}$, $f(a_n,b_n) = 1$.
Notons $x = \lim(a_n)(= \lim(b_n))$, et rappelons que $\delta(x) > 0$.
il existe m tel que si $x - a_m < \frac{\delta(x)}{2}$ et $b_m - x < \frac{\delta(x)}{2}$.
I_m admet alors une subdivision finie : $([a_m,b_m],x)$, donc $f(a_m,b_m) = 0$.
Cela nous donne une contradiction : $f(a,b) = 0$. □

Représentation - Lemme de COUSIN



Savoir faire - Exploiter le lemme de Cousin

Il y a deux façons d'exploiter le lemme de Cousin.
• On peut exploiter le lemme de Cousin par l'absurde.
On doit vérifier une certaine propriété $\mathscr{P}$.
On démontre alors que sa contradiction conduit à l'existence d'une jauge δ sur un segment fermé qui n'admet pas de subdivision δ-fine, ou une contradiction sur la finitude de la subdivision.
Trouver δ n'est pas toujours évident. (On a une application de cette méthode plus bas).
• Une jauge δ est naturellement donnée (exemple, la jauge de continuité).
Alors l'utilisation du lemme de Cousin conduit à couper l'intervalle en un nombre **fini** d'intervalles dont on maitrise le « centre » (t_i).
Il reste ensuite à considérer un max et non un sup. (On applique cette méthode pour démontrer le théorème de Heine).

Pour aller plus loin - Théorème de HEINE

Une application classique du lemme de COUSIN est la démonstration du théorème de HEINE.
Nous verrons également le théorème de HEINE-BOREL (ou Borel-Lebesgue) en exercice.
C'est dans ce même esprit que ce lemme est exploité pour construire l'intégrale de KURZWEIL-HENSTOCK…

Exemple - Nouvelle démonstration du théorème de Bolzano-Weierstrass

On considère une suite (u_n) bornée, par exemple à valeurs dans $[a,b]$.
Si on a :

$$\exists\, t\in[a,b], \qquad \forall\, \epsilon(=\frac{\delta(t)}{2}) > 0,]t-\epsilon, t+\epsilon[\text{ contient une infinité de termes de } (u_n)$$

Alors (u_n) admettrait une sous-suite convergente vers t.
Donc si on suppose que (u_n) n'admet pas de suite extraite convergente, alors

$\forall\, t\in[a,b], \exists\, \epsilon(t) > 0 \mid]t-\epsilon(t), t+\epsilon(t)[$ ne contienne qu'un nombre fini de termes de (u_n)

Prenons $\delta : [a,b] \to \mathbb{R}_+^*, t \mapsto \epsilon(t)$.
donc comme $[t - \frac{\delta(t)}{2}, t + \frac{\delta(t)}{2} \subset]t-\epsilon(t), t+\epsilon(t)[$, on a :

$$\forall\, t\in[a,b], \qquad [t - \frac{\delta(t)}{2}, t + \frac{\delta(t)}{2}] \text{ ne contienne qu'un nombre fini de termes de } (u_n)$$

A partir de la jauge δ ainsi définie par $(*)$, il existe une subdivision pointée δ-fine.
Comme cette subdivision est finie et que chacun de ces intervalles ne possède qu'un nombre fini de termes, alors (u_n) possède un nombre fini de termes.
Cela est évidemment faux.
Donc (u_n) admet une suite extraite convergente.

5. Curiosité topologique : complétude

5.1. Suites de Cauchy

Heuristique - Mise en place du concept

La difficulté avec les suites, c'est que pour démontrer leur convergence, on doit connaître la limite (la définition nécessite le calcul $|u_n - \ell|$).
Que peut-on dire si la suite ne « bouge » plus, visiblement après un certain nombre de calculs? CAUCHY propose de s'intéresser à ces suites là en particulier (on les appelle suite de CAUCHY). Sont-elles nécessairement convergentes? famille de suites
Autre définition avec u_N au lieu de u_q, plus naturelle. Puis équivalence des deux défintions.
Interprétation avec $\epsilon = 10^{-k}$

Pour aller plus loin - Notion hors-programme

… mais elle est vraie et elle est essentielle en mathématiques.
On dit qu'un ensemble (espace) E qui vérifie le principe suivant :
toute suite de E est convergente ssi elle est de Cauchy est un espace complet.
On va voir que $\mathbb{R}$ est complet

Définition - Suites de CAUCHY

On dit que la suite (u_n) vérifie le critère de CAUCHY si elle verifie l'un des deux critères suivants équivalents :

$$\forall\, \epsilon > 0, \exists\, n_0\in\mathbb{N} \mid \forall\, p \geqslant n_0, |u_p - u_{n_0}| < \epsilon$$

$$\forall\, \epsilon > 0, \exists\, N\in\mathbb{N} \mid \forall\, p,q \geqslant N, |u_p - u_q| < \epsilon$$

Montrons que les deux critères sont équivalents.

Démonstration

Si (u_n) vérifie le second critère, il vérifie le premier (il suffit de prendre $q = N$).
Réciproquement, supposons que (u_n) vérifie le premier critère.
Soit $\epsilon > 0, \exists\, n_0\in\mathbb{N} \mid \forall\, p \geqslant n_0, |u_p - u_{n_0}| < \frac{\epsilon}{2}$.
Donc pour tout $p,q \geqslant n_0, |u_p - u_q| \leqslant |u_p - u_{n_0}| + |u_{n_0} - u_q| \leqslant \epsilon$.
Ainsi (u_n) vérifie le premier critère. □

Pour aller plus loin - Construction de $\mathbb{R}$

La stratégie de Cauchy pour construire $\mathbb{R}$, formalisée par CANTOR, consiste à dire que $\mathbb{R}$ est l'ensemble obtenu à partir de $\mathbb{Q}$ et des limites des suites rationnelles vérifiant le critère de CAUCHY.
Nous avons choisi une technique plus proche de la méthode historique de BOLZANO.
Une troisième stratégie consiste à définir puis exploiter les coupures de DEDEKIND.
Une quatrième stratégie est d'étudier les développements décimaux…

Application - Suite, écrite décimalement

Supposons que $\epsilon = 10^{-k}$. Alors une suite de Cauchy vérifie à partir d'un certain rang n_0, $|u_n - u_{n_0}| < 10^{-k}$ i.e u_n garde toujours les mêmes k premières décimales à partir du rang n_0.
Elle semble donc invariante à partir d'un certain rang si nous ne pouvons en avoir qu'une connaissance à k décimales près.

5.2. $\mathbb{R}$ est complet

L'idée de CAUCHY est de trouver un critère de suite convergente sans avoir à connaître la limite.

Proposition - Condition nécessaire

Si $(u_n) \in \mathbb{R}^{\mathbb{N}}$ est convergente, alors elle vérifie le critère de Cauchy

Démonstration
Soit $\epsilon > 0$. Alors il existe n_0 tel que $\forall\ p \geqslant n_0, |u_p - \ell| < \frac{\epsilon}{2}$.
Et donc pour $p, q \geqslant n_0$,

$$|u_p - u_q| \leqslant |u_p - \ell| + |\ell - u_q| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

□

Proposition - Condition suffisante
Si $(u_n) \in \mathbb{R}^{\mathbb{N}}$ vérifie le critère de Cauchy, alors elle est convergente.

La démonstration de la proposition est faite dans l'exercice suivant
Exercice

1. Montrer que toute suite de Cauchy est bornée.
2. Montrer que toute suite de Cauchy qui admet une sous-suite convergente, converge vers cette même limite.
3. Conclure, en exploitant le théorème de Bolzano-Weiertrass.

Pour aller plus loin - Ensemble complet
Un ensemble dont les suites de Cauchy sont nécessairement convergentes s'appelle un espace complet.

Correction

1. Soit $\epsilon > 0$.
   Alors il existe $n_0 \in \mathbb{N}$ tel que $\forall\ p, q \geqslant n_0, |u_p - u_q| < \epsilon$.
   Donc $\forall\ p \geqslant n_0, |u_p - u_{n_0}| < \epsilon$, donc $|u_p| < \epsilon + |u_{n_0}|$. Ainsi toute suite de Cauchy est bornée à partir d'un certain rang, donc bornée.
2. Supposons que $(u_{\varphi(n)})$ converge vers ℓ.
   Soit $\epsilon > 0$.
   Il existe $n_0 \in \mathbb{N}$ tel que $\forall\ p, q \geqslant n_0, |u_p - u_q| < \frac{\epsilon}{2}$
   et $\exists\ m (= \varphi(k)) \geqslant n_0$ tel que $|u_m - \ell| < \frac{\epsilon}{2}$.
   Alors $\forall\ p \geqslant n_0, |u_p - \ell| < |u_p - u_m| + |u_m - \ell| < \epsilon$. Donc (u_n) converge vers ℓ.
3. (u_n) est bornée, donc d'après BW admet une sous-suite convergente vers ℓ.
   Et donc (u_n) converge vers ℓ d'après la seconde question.

6. Bilan

Synthèse

⇝ Nous abordons beaucoup de définition importante ici pour comprendre les passages à la limite dans $\mathbb{R}$: voisinage, puis intérieur ou adhérence.

⇝ On retrouve ensuite la notion de connexe : ensemble en un seul tenant. Dans $\mathbb{R}$, il s'agit des intervalles. Cela nous donnera une bonne base pour le TVI.

⇝ On parle ensuite des compacts : ensemble que l'on peut découper en un nombre fini de morceaux suffisamment grand (et choisi a priori). Dans $\mathbb{R}$, il s'agit des fermés bornés, donc en particulier des segments (=intervalle, fermé et borné).

⇝ Par curiosité, nous parlons ici de la notion de complétude qui permet d'assurer l'existence d'une limite d'une suite (ou de tout autre) car un critère qui ne nécessite pas de connaître a priori cette valeur de limite.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Montrer qu'une partie de $\mathbb{R}$ est conenxe
— Savoir-faire - Sous-additivité pour une fonction d'intervalle définie par une propriété
— Savoir-faire - Comment exploiter le « processus de dichotomie »
— Savoir-faire - Suite extraire dans N_k
— Savoir-faire - Exploiter le lemme de Cousin

Notations

Notations	*Définitions*	*Propriétés*
$\overline{\mathbb{R}}$	Droite réelle achevée	$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$
$\mathcal{V}_a$	Ensemble des voisinage de $a \in \overline{\mathbb{R}}$	Si $a = +\infty$. $V \in \mathcal{V}_a$ si $\exists\ A \in \mathbb{R}$ tel que $]A, +\infty[\subset V$ Si $a \in \mathbb{R}$. $V \in \mathcal{V}_a$ si $\exists\ \epsilon > 0$ tel que $]a-\epsilon, a+\epsilon[\subset V$
$\mathring{A}$	Intérieur de l'ensemble A	$\{a \in I \mid \exists\ \epsilon > 0 \mid]a-\epsilon, a+\epsilon[\subset A\}$
$\overline{A}$	Adhérence de l'ensemble A	$\{a \in I \mid \forall\ \epsilon > 0 \mid]a-\epsilon, a+\epsilon[\cap A \neq \emptyset$
$\sigma_p = ([x_{i-1}, x_i], t_i)_{i \in \mathbb{N}_n}$	Subdivision pointée du segment $I = [x_0, x_n]$	$\forall\ i \in \mathbb{N}_n, x_{i-1} \leqslant t_i \leqslant x_i$

Retour sur les problèmes

83. Voir cours
84. Voir définition de voisinage.
85. Voir définition de connexité.
86. Voir cours

Chapitre 20

Continuité

Résumé -

Nous formalisons ici la notion de continuité. Suivant Bolzano puis Weierstrass qui au XIX siècle ont défini proprement la continuité, il est nécessaire de suivre l'ordre suivant : 1. notion de limite de fonction ; 2. notion de continuité en un point ; 3. notion de continuité sur un intervalle.
Nous verrons qu'en considérant f continue globalement sur son ensemble de définition (intervalle voire segment), nous obtenons des résultats importants d'existence (théorèmes des valeurs intermédiaires, de Weierstrass, de Heine).
Le chapitre se termine par l'extension aux fonctions à valeurs complexes.
Des liens youtube :

- *Jaicompris Maths - fonctions continues : comprendre la définition - le cours et les propriétés. https ://www.youtube.com/watch ?v=uuwlDYw49h4*
- *Maths Adulte - Théorème des valeurs intermédiaires et applications. https ://www.youtube.com/watch ?v=xgENfRQvPrA*
- *Bibmaths.net - Théorème de Bolzano-Weierstrass. https ://www.youtube.com/watch ?v=5WqLT_J8T4s*

Sommaire

1. Problèmes 386
2. Limites (de fonctions) 386
2.1. Définitions 386
2.2. Ordre et limites 390
2.3. Opérations sur les limites 391
2.4. Cas des fonctions monotones 392
2.5. Continuité en un point 394
3. Fonction continue sur un ensemble (intervalle, segment...) 395
3.1. Fonctions continues sur I 395
3.2. Prolongement par continuité 396
3.3. Théorème des valeurs intermédiaires 397
3.4. Cas de l'image d'un segment par f continue 398
3.5. Théorème de la bijection (bis) 401
3.6. Continuité uniforme 402
4. Généralisation aux fonctions à valeurs dans $\mathbb{C}$ 405
4.1. Opérations classiques sur $\mathcal{F}(X,\mathbb{C})$ 405
4.2. Fonctions bornées 405
4.3. Limites 406
4.4. Opérations sur les limites 406
4.5. Continuité 407
5. Bilan 407

1. Problèmes

Problème 88 - Limite. Propriété algébrique.

Un célèbre ouvrage de mathématique (L'analyse au fil de l'histoire) commence par la citation : « *Qu'est-ce qu'une dérivée ? une limite. Qu'est-ce qu'une intégrale ? Une limite. Qu'est-ce qu'une limite ? Un nombre* »
La notion de limite (on pourrait ajouter de borne supérieure) est au coeur de l'analyse mathématique réelle ou complexe.
Que peut-on faire avec les limites ? En particulier quelles sont les propriétés algébriques du passage à la limite (passage à la limite d'une combinaison linéaire, par exemple) ?
De cette réponse découlera beaucoup de propriétés d'analyse.

Problème 89 - Qu'est-ce qu'une fonction continue ?

Le théorème des valeurs intermédiaires dont on parle au problème précédent, s'appuie sur l'hypothèse essentielle de continuité.
Mais qu'est-ce qu'une fonction continue ? Si l'on visualise bien la réponse : une fonction que l'on trace « sans lever le crayon », cette réponse ne semble pas passer les canons des définitions mathématiques en MPSI. On aimerait également une réponse que ne soit pas vraiment associé à une représentation graphique.
Comment formaliser la définition de la continuité d'une fonction ?

Problème 90 - Fonction nulle part continue.

Existe-t-il des fonctions définies en tout point, mais continue nulle part ?

Problème 91 - Image d'un intervalle par une fonction continue ?

Soit I un intervalle de $\mathbb{R}$ et f continue sur I.
Que peut-on dire de $f(I)$? En particulier, est-il borné ?
Si $f(I)$ est bornée, alors $\sup(f(I))$ existe. A-t-on nécessairement : $\exists\, x_0 \in I$ tel que $f(x_0) = \sup f(I)$?
Faut-il ajouter des conditions nécessaires, suffisantes supplémentaires ?

Problème 92 - Continuité prolongée

Qu'est-ce que la continuité pour des fonctions de $\mathbb{R}$ dans $\mathbb{C}$?

2. Limites (de fonctions)

Par la suite I est toujours un intervalle.

2.1. Définitions

Limite

Définition - Limite
Soient f une fonction définie sur $I \subset \mathbb{R}$, à valeurs dans $\mathbb{R}$ et a un élément d'accumulation ou adhérent de I.
On dit que f tend vers $\ell \in \overline{\mathbb{R}}$ quand x tend vers a si :

$$\forall W \in \mathcal{V}_\ell, \exists V \in \mathcal{V}_a \,|\, f(I \cap V) \subset W$$

ou de manière équivalente :

$$\forall W \in \mathcal{V}_\ell, f^{-1}(W) := [f \in W] \in \mathcal{V}_a$$

On note $f(x) \underset{x \to a}{\longrightarrow} \ell$.

L'avantage : on a créé une définition unifiée. Mais on peut la voir en 9 parties.

Remarque - Rappel sur les images réciproques
On note en réalité $f^{-1}(W)$ l'ensemble $\{x \in I \mid f(x) \in W\}$.
On peut aussi trouver la notation vue pour les variables aléatoires : $[f \in W]$ ou $[f = a] = \{x \in E \mid f(x) = a\} = f^{-1}(\{a\})$.
On a alors presque trivialement : $f(f^{-1}(B)) = f([f \in B]) \subset B$ et $B \subset [f \in f(B)] = f^{-1}(f(B))$.

Analyse - Pourquoi ces deux définitions sont équivalentes ?
Rappelons : $f^{-1}(W) = [f \in W] = \{x \in I \mid f(x) \in W\}$.
On a les équivalences (cas $a \in \mathbb{R}$) :

$$\begin{aligned} f^{-1}(W) \in \mathcal{V}_a &\iff \exists \epsilon > 0 \mid]a-\epsilon, a+\epsilon[\subset f^{-1}(W) \\ &\iff \exists \epsilon > 0 \mid f(]a-\epsilon, a+\epsilon[\cap I) \subset W \end{aligned}$$

De même pour les cas $a = +\infty$ et $a = -\infty$…

Exemple - $x \mapsto x \ln x$
On étudie la limite en 0.
Quelques informations : $f : \mathbb{R}_+^* \to \mathbb{R}, x \mapsto x \ln x$ est décroissante sur $]0, \frac{1}{e}]$ puis croissante sur $[\frac{1}{e}, +\infty[$.
On donne aussi $\ln 10 \approx 2,30$.
Soit W un voisinage de 0, on peut imaginer que W contient $[-10^{-k}, 10^{-k}]$.
On note $f(10^{-m}) = -m \ln 10 \times 10^{-m} \approx -2,3m10^{-m}$.
Donc $f(10^{-(k+\log_{10}(3k))}) = -2,3(k+\log_{10}(3k))\frac{10^{-k}}{3k} = -\frac{2,3}{3}(1+\frac{1}{k}\log_{10}(k))10^{-k} \in W$.
Et par décroissance de f : $f(\mathbb{R}_+^* \cap [10^{-(k+\log_{10}(3k))}, 10^{-(k+\log_{10}(3k))}]) \subset]0, 10^{-k}] \subset W$.
Donc pour tout voisinage W de 0, il existe un voisinage V de 0 tel que $f(\mathbb{R}_+^* \cap V) \subset W$.
f tend vers 0 lorsque x tend vers 0.

Pour aller plus loin - Point d'adhérent ou d'accumulation
Un point isolé, donc adhérent, ne serait pas un bon candidat pour regarder la limite (on aurait $f^{-1}(W) = \{a\} \notin \mathcal{V}_a$.
Mais comme ici, on se situe dans un intervalle, il n'y a pas de point isolé et on ne peut pas différencier les points adhérents de points d'accumulation.

Attention - L'importance de l'intervalle de définition
Notons que $f : \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} 1 & \text{si } x > 0 \\ 0 & \text{si } x \leqslant 0 \end{cases}$ n'est pas continue en 0.
En revanche, $f_1 : \mathbb{R}_- \to \mathbb{R}, x \mapsto 0$ est continue en 0. Puisqu'ici, par définition de I, la limite de f en 0, impose de regarder $x \to 0^-$.
Ainsi si une fonction f n'est pas définie sur un intervalle (mais une réunion, par exemple), il faudrait préciser la continuité selon quel intervalle. On pourrait écrire ici que f est continue en 0, selon (l'intervalle) $\mathbb{R}_-$.

Attention à l'ordre des quantificateurs

Remarque - Ordre et quantificateurs
On souligne l'ordre des objets et les quantificateurs associés :

1. $\forall$ associé au voisinage image
2. $\exists$ associé au voisinage des antécédents (et qui dépend donc du voisinage image fixé en 1.).

Remarque - Selon la nature de a et de ℓ
Cette définition recouvre en fait plusieurs définitions suivant que a ou ℓ sont réels ou infinis.

- $a \in \mathbb{R}, \ell \in \mathbb{R}$: $f(x) \underset{x \to a}{\longrightarrow} \ell$ si

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in I, |x-a| \leqslant \eta \Rightarrow |f(x) - \ell| \leqslant \varepsilon$$

- $a \in \mathbb{R}, \ell = +\infty$: $f(x) \underset{x \to a}{\longrightarrow} +\infty$ si

$$\forall A > 0, \exists \eta > 0, \forall x \in I, |x-a| \leqslant \eta \Rightarrow f(x) \geqslant A$$

- $a \in \mathbb{R}, \ell = -\infty$: $f(x) \underset{x \to a}{\longrightarrow} -\infty$ si

$$\forall A < 0, \exists \eta > 0, \forall x \in I, |x-a| \leqslant \eta \Rightarrow f(x) \leqslant A$$

- $a = +\infty, \ell \in \mathbb{R}$ $f(x) \underset{x \to +\infty}{\longrightarrow} \ell$ si

$$\forall \varepsilon > 0, \exists B > 0, \forall x \in I, x \geqslant B \Rightarrow |f(x) - \ell| \leqslant \varepsilon$$

- $a = +\infty, \ell = +\infty$ $f(x) \underset{x \to +\infty}{\longrightarrow} +\infty$ si

$$\forall A > 0, \exists B > 0, \forall x \in I, x \geqslant B \Rightarrow f(x) \geqslant A$$

- $a = +\infty, \ell = -\infty$ $f(x) \underset{x \to +\infty}{\longrightarrow} +\infty$ si

$$\forall A < 0, \exists B > 0, \forall x \in I, x \geqslant B \Rightarrow f(x) \geqslant A$$

On peut le résumer en un tableau (à compléter)

	$\ell = -\infty$ $\forall\ A < 0 \ldots\ldots f(x) < A$	$\ell \in \mathbb{R}$ $\forall\ \epsilon > 0 \ldots\ldots \lvert f(x) - \ell \rvert < \epsilon$	$\ell = +\infty$ $\forall\ A > 0 \ldots\ldots f(x) > A$
$a = -\infty$ $\ldots \exists\ B < 0$ tq $x < B \Rightarrow \ldots$			
$a = -\infty$ $\ldots \exists\ \eta > 0$ tq $\lvert x - a \rvert < \eta \Rightarrow \ldots$			
$a = +\infty$ $\ldots \exists\ B > 0$ tq $x > B \Rightarrow \ldots$			

Remarque - Inégalités larges ou strictes
Selon une remarque précédente, les inégalités larges dans les définitions peuvent être remplacées par des inégalités strictes et les voisinages fermés par des voisinages ouverts.

Unicité

La seconde partie de la définition est plus efficace, mais elle cache le rôle joué par l'ensemble I de définition de f. Pour la démonstration du théorème qui suit, on exploitera plutôt la première définition.

Théorème - Unicité
Si f admet une limite en $a \in \overline{\mathbb{R}}$, celle-ci est unique.
Lorsque $f(x) \underset{x \to a}{\longrightarrow} \ell$ $((a, \ell) \in \overline{\mathbb{R}}^2)$, cette proposition permet donc de parler de « la » limite de f en a et de noter $\ell = \lim\limits_{x \to a} f(x)$.

Cette limite peut être à valeurs dans $\overline{\mathbb{R}}$.

Démonstration
Soit ℓ_1 et ℓ_2 deux limites de f en a.
Si $\ell_1 \neq \ell_2$, alors il existe $W_1 \in \mathcal{V}_{\ell_1}$ et $W_2 \in \mathcal{V}_{\ell_2}$ tels que $W_1 \cap W_2 = \emptyset$.
(Sinon, tout voisinage de ℓ_1 est un voisinage de ℓ_2 et donc $\ell_1 = \ell_2$ - c'est la séparabilité de $\mathbb{R}$).
Par définition de la limite :
Il existe alors V_1 et V_2 voisinages de a telles que $f(I \cap V_1) \subset W_1$ et $f(I \cap V_2) \subset W_2$.
Puis, $V = V_1 \cap V_2$ est un voisinage de a (non vide) et $f(I \cap V) \subset f(I \cap V_1) \subset W_1$ et $f(I \cap V) \subset f(I \cap V_2) \subset W_2$.
Donc $f(I \cap V) \subset W_1 \cap W_2 = \emptyset$ ce qui est impossible car $I \cap V \neq \emptyset$ (sinon a non adhérent à I).
(On a $x \in I \cap V$ et donc $f(x) \in f(I \cap V)$) □

Proposition - Limite finie donc bornée
Toute fonction admettant une limite finie en $a \in \overline{\mathbb{R}}$ est bornée sur un voisinage de a.

Démonstration
Soit $\ell = \lim_a(f)$. Il existe V voisinage de a tel que $f(I \cap V) \subset]\ell - 1, \ell + 1[$.
Donc sur un voisinage de a, f est bornée.
□

Limite à droite, limite à gauche

Définition - Limite à gauche, à droite
Soit $f : I \to \mathbb{R}$.
— On suppose que $a \in \mathbb{R}$ n'est pas la borne inférieure de I. On dit que f admet $\ell \in \overline{\mathbb{R}}$ pour limite à gauche si la fonction $f_{|I \cap]-\infty, a[}$ admet ℓ pour limite en a, c'est-à-dire :
(cas $\ell = -\infty$) : $\forall A < 0, \exists \eta > 0 \,|\, \forall x \in I,\ a - \eta \leqslant x < a \Rightarrow f(x) < A$
(cas $\ell \in \mathbb{R}$) : $\forall \epsilon > 0, \exists \eta > 0 \,|\, \forall x \in I,\ a - \eta \leqslant x < a \Rightarrow |f(x) - \ell| \leqslant \epsilon$.
(cas $\ell = +\infty$) : $\forall A > 0, \exists \eta > 0 \,|\, \forall x \in I,\ a - \eta \leqslant x < a \Rightarrow f(x) > A$
On note $f(x) \underset{x \to a, x<a}{\longrightarrow} \ell$ ou $f(x) \underset{x \to a^-}{\longrightarrow} \ell$.
— On suppose que $a \in \mathbb{R}$ n'est pas la borne supérieure de I. On dit que f admet $\ell \in \overline{\mathbb{R}}$ pour limite à droite si la fonction $f_{I \cap]a, +\infty[}$ admet ℓ pour limite en a, c'est-à-dire
(cas $\ell = -\infty$) : $\forall A < 0, \exists \eta > 0 \,|\, \forall x \in I,\ a \leqslant x < a + \eta \Rightarrow f(x) < A$
(cas $\ell \in \mathbb{R}$) : $\forall \epsilon > 0, \exists \eta > 0 \,|\, \forall x \in I,\ a < x \leqslant a + \eta \Rightarrow |f(x) - \ell| \leqslant \epsilon$
(cas $\ell = +\infty$) : $\forall A > 0, \exists \eta > 0 \,|\, \forall x \in I,\ a \leqslant x < a + \eta \Rightarrow f(x) > A$
On note $f(x) \underset{x \to a, x>a}{\longrightarrow} \ell$ ou $f(x) \underset{x \to a^+}{\longrightarrow} \ell$.

Proposition - Limite et limite à gauche et droite
Soit $f : I \to \mathbb{R}$ et $a \in I$.
Si a n'est pas une extrémité de I, f admet ℓ pour limite en a si et seulement si f admet ℓ pour limite à gauche et à droite en a et si $f(a) = \ell$.

Si a est une extrémité de I, on a le même résultat en supprimant *limite à gauche* si a est l'extrémité gauche ou *limite à droite* si a est l'extrémité droite.

Caractérisation à l'aide de suites

Théorème - Caractérisation séquentielle
Soit $f \in \mathcal{F}(I, \mathbb{R})$ et $a \in \overline{\mathbb{R}}$ un point ou une extrémité de I. Soit $\ell \in \overline{\mathbb{R}}$.
On a $\lim_{x \to a} f(x) = \ell$ si et seulement si pour toute suite réelle (u_n) de points de I ayant pour limite a, la suite $(f(u_n))$ a pour limite ℓ.

Remarque - Convergence de suites et voisinage
On a (u_n) converge vers ℓ
ssi $\forall\, \epsilon > 0, \exists\, N \in \mathbb{N}$ tel que $\forall\, n > N, |u_n - \ell| < \epsilon$.
ssi $\forall\, W \in \mathcal{V}_\ell$, il existe $V \in \mathcal{V}_{+\infty}$ tel que $\forall\, n \in \mathbb{N} \cap V,\ u_n \in W$.

Démonstration
Supposons que $\lim_{x \to a} f(x) = \ell$.
Soit (u_n) suite qui tend vers a.
Soit $\epsilon > 0$ et $W =]\ell - \epsilon, \ell + \epsilon[$ un voisinage de ℓ.
Il existe V voisinage de a tel que $f(I \cap V) \subset W$.
Or (u_n) tend vers a. Donc il existe $N \in \mathbb{N}$ tel que $\forall\, n \geqslant N,\ u_n \in V$.
Alors $f(u_n) \in W$ et donc $|f(u_n) - \ell| < \epsilon$. Par conséquent $f(u_n) \to \ell$.
Pour la réciproque, nous allons faire un raisonnement par contraposée.
Supposons que $\lim_{x \to a} f(x) \neq \ell$.
$\exists\, \epsilon > 0, \forall\, \eta > 0, \exists\, x \in I$ tel que $|x - a| < \eta$ et $|f(x) - \ell| > \epsilon$.
On va alors créer une suite (u_n) qui converge vers a et $(f(u_n))$ ne converge pas vers ℓ.
On a donc (avec $\eta = \frac{1}{n}$), l'existence de x_n tel que $|x_n - a| < \frac{1}{n}$ et $|f(x_n) - \ell| > \epsilon$.
Alors, pour cette suite (x_n), on a par domination : $(x_n) \to a$ mais aussi $(f(x_n))$ ne converge pas vers ℓ. □

Exercice
Prouver que la fonction définie sur $]0, +\infty[$ par $x \mapsto \sin \dfrac{1}{x}$ n'a pas de limite en 0.
De même on prouverait que les fonctions sin ou cos n'ont pas de limite en $+\infty$.

Correction
Les suites $u_n = \frac{1}{n\pi}$ et $v_n = \frac{1}{n\pi + \frac{\pi}{2}}$ convergent vers 0.
Et $\sin(u_n) = \sin(n\pi) = 0$ et $\sin(v_n) = \sin(n\pi + \frac{pi}{2}) = 1$.
Par contraposée de la caractérisation séquentielle : $x \mapsto \sin \dfrac{1}{x}$ ne peut avoir de limite en 0.

2.2. Ordre et limites

Théorème - Passage à la limite dans les inégalités
Soient f, g deux fonctions définies sur I intervalle de $\mathbb{R}$ et $a \in \overline{I}$.
On suppose que sur un voisinage V de a on a $f(x) \leqslant g(x)$ et que $\lim\limits_{x \to a} f(x) = \ell$, $\lim\limits_{x \to a} g(x) = \ell'$. Alors $\ell \leqslant \ell'$.

Démonstration
Soit $\epsilon > 0$. $[\ell - \epsilon, \ell + \epsilon] \in \mathcal{V}_\ell$ et $[\ell' - \epsilon, \ell' + \epsilon] \in \mathcal{V}_{\ell'}$ Il existe V_1, V_2 voisinage de a tel que $f(V_1 \cap I) \subset [\ell - \epsilon, \ell + \epsilon]$ et $g(V_2 \cap I) \subset [\ell' - \epsilon, \ell' + \epsilon]$.
Notons $V = V_1 \cap V_2 \cap I$, c'est un voisinage de a, non vide.
Soit $x \in V$, alors $f(x) \subset [\ell - \epsilon, \ell + \epsilon]$ et $g(x) \subset [\ell' - \epsilon, \ell' + \epsilon]$.
Donc $\ell - \epsilon \leqslant f(x) \leqslant g(x) \leqslant \ell' + \epsilon$.
On a donc pour tout $\epsilon > 0$, $\ell - \epsilon \leqslant \ell' + \epsilon$, soit $\ell - \ell' \leqslant 2\epsilon$.
Nécessairement : $\ell - \ell' \leqslant = \inf(\mathbb{R}_+^*) = 0$ et donc $\ell \leqslant \ell'$ □

Exercice
Refaire la démonstration en exploitant le théorème sur les suites.

Correction
On applique le théorème sur les suites.
Soit (u_n) convergeant vers a, alors $f(u_n)$ converge vers ℓ et $g(u_n)$ converge vers ℓ'.
Et il existe $N > 0$ tel que $\forall\, n > N,\ (u_n) \in V$.
Donc pour tout $n > N$, $f(u_n) \leqslant g(u_n)$ et en passant à la limite : $\ell \leqslant \ell'$.

Théorème - Théorème de limite par encadrement, dit « des gendarmes' »
Soient f, g, h trois fonctions définies sur un voisinage V de $a (\in \overline{I})$ et $\ell \in \mathbb{R}$.
On suppose que $\lim\limits_{x \to a} f(x) = \lim\limits_{x \to a} h(x) = \ell$ et que $\forall x \in V,\ f(x) \leqslant g(x) \leqslant h(x)$.
Alors le fonction g admet une limite en a et $\lim\limits_{x \to a} g(x) = \ell$.

Démonstration
On pourrait exploiter le même théorèmes sur les suites.
Soit W un voisinage de ℓ.
Donc il existe $\epsilon > 0$, $]\ell-\epsilon,\ell+\epsilon[\subset W$.
Il existe V_1 et V_2, voisinages de a tel que $f(I\cap V_1)\in W$ et $h(I\cap V_2)\in W$.
Pour tout $x\in U = V\cap V_1\cap V_2$, voisinage de a,
$\ell-\epsilon \leqslant f(x)\leqslant g(x)\leqslant h(x)\leqslant \ell+\epsilon$, ainsi $g(x)\in W$.
Donc pour tout $W\in\mathcal{V}_\ell$, il existe $U\in\mathcal{V}_a$ tel que $g(I\cap U)\subset W$. □

On a un résultat analogue au théorème précédent pour les limites infinies.

Théorème - Divergence vers $+\infty$ par minoration (resp. $-\infty$ par majoration)
Soient f et g deux fonctions définie sur un voisinage V de $a\in\overline{I}$ telles que $\forall x\in V$, $f(x)\leqslant g(x)$. Alors

$$f(x)\xrightarrow[x\to a]{}+\infty \Longrightarrow g(x)\xrightarrow[x\to a]{}+\infty$$

$$g(x)\xrightarrow[x\to a]{}-\infty \Longrightarrow f(x)\xrightarrow[x\to a]{}-\infty$$

Démonstration
C'est pratiquement la même démonstration.
Soit W un voisinage de $+\infty$.
Donc il existe $A>0$, $]A,+\infty[\subset W$.
Il existe V_1, voisinage de a tel que $f(I\cap V_1)\in W$.
Pour tout $x\in U = V\cap V_1$, voisinage de a,
$A\leqslant f(x)\leqslant g(x)$, ainsi $g(x)\in W$.
Donc pour tout $W\in\mathcal{V}_{+\infty}$, il existe $U\in\mathcal{V}_a$ tel que $g(I\cap U)\subset W$.(...) □

2.3. Opérations sur les limites

Lemme -
Si $f(x)\xrightarrow[x\to a]{}0$ et g bornée, au voisinage de $a\in\overline{I}$,
alors $(f\times g)(x)\xrightarrow[x\to a]{}0$

Démonstration
Soit V un voisinage de 0. Il existe $\epsilon>0$ tel que $]-\epsilon,\epsilon[\subset V$.
g est bornée au voisinage de a. Il existe $M>0$ et $W\in\mathcal{V}_a$ tel que $|g(W)|\leqslant M$.
$f(x)\xrightarrow[x\to a]{}0$. Donc il existe $W'\in\mathcal{V}_a$ tel que $|f(W)|\subset]-\frac{\epsilon}{M},\frac{\epsilon}{M}[$.
Alors $|f\times g|(W\cap W')\in]-\epsilon;\epsilon[\subset V$. □

Théorème - Opération sur les limites
On suppose que f et g ont des limites respectives $\ell\in\overline{\mathbb{R}}$ et $\ell'\in\overline{\mathbb{R}}$ en $a\in\overline{I}$.
Alors :
— $|f|$ a une limite en a qui est $|\ell|$;
— lorsque $\lambda\ell$ n'est pas une forme indéterminée, λf a une limite qui est $\lambda\ell$;
— lorsque $\ell+\ell'$ n'est pas une forme indéterminée, $f+g$ a une limite qui est $\ell+\ell'$;
— lorsque $\ell\ell'$ n'est pas une forme indéterminée, fg a une limite qui est $\ell\ell'$;
— si $\ell'\neq 0$, il existe un voisinage de a sur lequel g ne s'annule pas et la restriction de $\frac{1}{g}$ à ce voisinage a une limite en a qui est $\frac{1}{\ell'}$.

Démonstration
Un à un
— Si $\ell>0$, cela est immédiat. Supposons $\ell<0$, donc $|\ell|=-\ell$.
Soit W un voisinage de $|\ell|=-\ell$ (supposons le fini),
alors $-W=\{-x, x\in W\}$ est un voisinage de ℓ
En effet, il existe $\alpha>0$ tel que $]-\ell-\alpha,-\ell+\alpha[\subset W$ et donc $]\ell-\alpha,\ell+\alpha[\subset -W$.
Par ailleurs, il existe V, voisinage de a tel que $f(V\cap I)\subset -W$, puis $|f(V\cap I)|=-f(V\cap I)\subset W$.
— Soit $\lambda\in\mathbb{R}$.
Soit W un voisinage de $\lambda\ell|$ (supposons $\lambda\neq 0$, sinon, $\lambda f=0$),
alors $\overline{W}=\{\frac{1}{\lambda}x, x\in W\}$ est un voisinage de ℓ
En effet, il existe $\alpha>0$ tel que $]-\lambda\ell-\lambda\alpha,-\lambda\ell+\lambda\alpha[\subset W$ et donc $]\ell-\alpha,\ell+\alpha[\subset\overline{W}$.
Par ailleurs, il existe V, voisinage de a tel que $f(V\cap I)\subset\overline{W}$, puis $\lambda f(V\cap I)=\subset W$.
— Soit W un voisinage de $\ell+\ell'$.
Il existe $\alpha>0$ tel que $]\ell+\ell'-\alpha,\ell+\ell'+\alpha[\subset W$ Notons $W_1=]\ell-\frac{\alpha}{2},\ell+\frac{\alpha}{2}[$, voisinage de ℓ et $W_2=]\ell'-\frac{\alpha}{2},\ell'+\frac{\alpha}{2}[$ voisinage de ℓ',
on a $\{y_1+y_2 \mid y_1\in W_1, y_2\in W_2\}\subset W$.
il existe V (quitte à prendre une intersection) voisinage de a tel que $f(I\cap V)\subset W_1$ et $f(I\cap V)\subset W_2$.
Donc $(f_1+f_2)(I\cap V)\subset\{y_1+y_2 \mid y_1\in W_1, y_2\in W_2\}\subset W$
— Si $\ell\ell'\in\mathbb{R}$.

$$[fg-\ell\ell'](x)=[(f-\ell)g+\ell(g-\ell')](x)\xrightarrow[x\to a]{}0$$

par produit de limite nulle et d'une fonction bornée.
Ainsi $f(x)g(x)\xrightarrow[x\to a]{}\ell\ell'$.
Si $\ell=+\infty$ et $\ell'<0$.
Soit $A\in\mathbb{R}_-$
$\exists\, W_1\in\mathcal{V}_a$ tel que $g(W_1)<\frac{\ell}{2}<0$.
$\exists\, W_2\in\mathcal{V}_a$ tel que $f(W_2)>\frac{2A}{\ell}>0$.
Donc $(fg)(W_1\cap W_2)<\frac{2A}{\ell}\times\frac{\ell}{2}=A$.
Ainsi $f(x)g(x)\xrightarrow[x\to a]{}-\infty=\ell\ell'$.
— $\frac{1}{g}-\frac{1}{\ell'}=\frac{\ell'-g}{\ell' g}\to 0$: produit d'une limite nulle et d'une fonction bornée (car $\ell' g$ tend vers ℓ'^2.

□

Exercice
Montrer que si $g\to 0$, alors $|\frac{1}{g}|\to+\infty$.
Si on maitrise le signe de $\frac{1}{g}$ (constant au voisinage de a), on peut trouver $\lim\frac{1}{g}$.

Correction
Soit $A>0$. Alors, $]\frac{-1}{A},\frac{1}{A}[$ est un voisinage de 0.
Donc il existe V, voisinage de a tel que $\forall\, x\in V$, $g(x)\in]\frac{-1}{A},\frac{1}{A}[$, donc $|g(x)|\in[0,\frac{1}{A}]$ et donc $|\frac{1}{g(x)}|\geqslant A$.

Théorème - Composition des limites
Soient I et J deux intervalles de $\mathbb{R}$, $f\in\mathscr{F}(I,\mathbb{R})$, $g\in\mathscr{F}(J,\mathbb{R})$, $f(I)\subset J$. Soit $a\in\overline{I}$ (élément ou extrémité de I). On suppose que $f(x)\xrightarrow[x\to a]{}b$ et que $g(y)\xrightarrow[y\to b]{}\ell$. Alors

$$g\circ f(x)\xrightarrow[x\to a]{}\ell.$$

Démonstration
Soit W un voisinage de ℓ.
Il existe V voisinage de b tel que $g(J\cap V)\subset W$.
Il existe U voisinage de a tel que $f(I\cap U)\subset V$.
Donc $(g\circ f)(I\cap U)\subset W$ (on notera que $f(I)\subset J$). □

On voit ici l'idée principale de la définition des limites de fonctions : penser en application réciproque (de l'arrivée vers le départ)

2.4. Cas des fonctions monotones

Dans le cas des fonctions monotones, on obtient un résultat sur l'existence des limites similaires à celui obtenu pour les suites monotones.

Théorème - Théorème de la limite monotone

Soient $(a,b) \in \overline{\mathbb{R}}^2$ et $f :]a,b[\to \mathbb{R}$ une fonction monotone.

- si f est croissante majorée, alors f admet une limite finie en b égale à $\sup\{f(x), x \in]a,b[\}$;
- si f est croissante non majorée, alors $f(x) \underset{x\to b}{\longrightarrow} +\infty$;
- si f est croissante minorée, alors f admet une limite finie en a égale à $\inf\{f(x), x \in]a,b[\}$;
- si f est croissante non minorée, alors $f(x) \underset{x\to a}{\longrightarrow} -\infty$;

de même :

- si f est décroissante minorée, alors f admet une limite finie en b égale à $\inf\{f(x), x \in]a,b[\}$;
- si f est décroissante non minorée, alors $f(x) \underset{x\to b}{\longrightarrow} -\infty$;
- si f est décroissante majorée, alors f admet une limite finie en a égale à $\sup\{f(x), x \in]a,b[\}$;
- si f est décroissante non majorée, alors $f(x) \underset{x\to a}{\longrightarrow} +\infty$.

Démonstration

Comme pour les suites, l'ensemble $\{f(x), x \in]a,b[\}$ est majoré dans $\mathbb{R}$.
Il admet une borne supérieure $B = \sup\{f(x), x \in]a,b[\}$.
Et donc $\forall\, \epsilon > 0$, il existe $x_0 \in]a,b[$ tel que $B - \epsilon < f(x_0)$.
Et par croissance de f, $\forall\, x \in]x_0, b[$, $B - \epsilon < f(x_0) \leqslant f(x)$.
Donc $f(x) \in]B-\epsilon, B[$.
Ainsi pour tout voisinage W de B, il existe un voisinage V de b tel que $f(V \cap I) \subset W$.
Si f est croissante non majorée : $\forall\, A > 0$, il existe x_0 tel que $f(x_0) > A$ et par croissance : $\forall\, x > x_0$, $f(x) > A$.
Ainsi pour tout voisinage W de $+\infty$, il existe un voisinage V de b tel que $f(V \cap I) \subset W$.
(...) □

Théorème - Limite monotone en touts points

Soit $f : I \to \mathbb{R}$ monotone. Alors f admet des limites finies à droite et à gauche en tout point de I qui n'est pas une extrémité de I. Si f est croissante on a

$$\lim_{x\to a^-} f(x) \leqslant f(a) \leqslant \lim_{x\to a^+} f(x).$$

Démonstration

Si f est monotone sur I. Soit $x_0 \in I$, qui n'est pas une extrémité. Alors $f_{|[\frac{a+x_0}{2}, \frac{x_0+b}{2}]}$ est bornée (fermée).
$\forall\, x \in [\frac{a+x_0}{2}, \frac{x_0+b}{2}]$, $f(\frac{a+x_0}{2}) \leqslant f(x) \leqslant f(\frac{b+x_0}{2})$.
On applique ensuite le théorème précédent. On a une limite à gauche et à droite (comme resp. en b et a du théorème de la limite monotone)
En ce qui concerne les inégalités, on applique le théorème « Passage à la limite dans les inégalités ».
En effet, pour $x < a$, $f(x) < g(x) = f(a)$. (où g est ainsi définie)... □

Exercice

Soit $f :]0, +\infty[\to \mathbb{R}$ croissante. On suppose de plus que $x \mapsto \dfrac{f(x)}{x}$ est décroissante sur $]0, +\infty[$.
Montrer que f admet une limite en tout point.

Correction

f admet une limite à droite et à gauche en tout point a de R_+^*, avec $\lim_{x\to a^-} f(x) \leqslant f(a) \leqslant \lim_{x\to a^+} f(x)$..

Par ailleurs, $x \mapsto \dfrac{f(x)}{x}$ est décroissante.

Si $x < a$, $\frac{f(x)}{x} \geqslant \frac{f(a)}{a}$, donc $f(x) \geqslant \frac{x}{a} f(a)$ $(x > 0)$.
En passant à la limite pour $x \to a^-$: $\lim_{x\to a^-} f(x) \geqslant 1 f(a)$.
Et de même $\lim_{x\to a^+} f(x) \leqslant 1 f(a)$.

On a donc l'égalité : $\lim_{x\to a^-} f(x) = f(a) = \lim_{x\to a^+} f(x)$ et f admet une limite en a.

Ceci est vrai pour tout $a \in \mathbb{R}_+^*$.

Histoire - Continuité au XIX

Cauchy introduit en 1821 le concept de fonction continue, en exigeant que des variations indéfiniment petites de x produisent des variations indéfiniment petites de y.
Bolzano (1817) et Weierstrass (1874) furent plus précis : la différence $f(x) - f(x_0)$ peut être arbitrairement petite, à condition qur la différence $x - x_0$ soit suffisamment petite

2.5. Continuité en un point

Continuité (en un point)

Définition - Continuité en un point x_0

Soit $f \in \mathscr{F}(I, \mathbb{R})$.
Soit $x_0 \in I$. On dit que f est continue en x_0 si $f(x) \underset{x\to x_0}{\longrightarrow} f(x_0)$ ce qui peut aussi s'écrire :

$$\forall\, \varepsilon > 0, \exists\, \delta > 0 \mid \forall\, x \in I, |x - x_0| \leqslant \delta \Rightarrow |f(x) - f(x_0)| \leqslant \epsilon$$

Remarque - Lien avec les limites

D'après ce que l'on a vu précédemment, f est continue en $x_0 \in I$ si et seulement si elle admet une limite finie en x_0 (égale à $f(x_0)$).

Remarque - Continuité à gauche, à droite

On peut également définir la continuité à gauche, ou à droite en x_0.

Discontinuité(s)

Définition - Discontinuité de deux types

On dit qu'une fonction f définie sur l'intervalle I possède en un point $a \in \bar{I}$ une discontinuité de première espèce ou une discontinuité simple si f est discontinue en ce point mais que $\lim_{a^+} f$ et $\lim_{a^-} f$ existent.
Tous les autres points de discontinuité sont dits de seconde espèce.

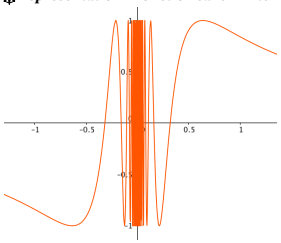
Exercice

Donner un exemple de chacune de ces deux discontinuités.

Correction

Pour le premier cas, la fonction d'Heaviside : $f = [x \geqslant 0]$.
Pour le second cas : $f : x \mapsto \sin\frac{1}{x}$ si $x \neq 0$ et $f(0) = 0$.

Représentation - Fonction sans limite



La fonction $x \mapsto \sin\frac{1}{x}$ n'admet pas de limite en 0.
Sauriez-vous le prouver?

Caractérisation séquentielle (=à l'aide de suite) de la continuité

Proposition - Caractérisation séquentielle de la continuité

Soit $f \in \mathscr{F}(I, \mathbb{R})$ et $x_0 \in I$. Alors f est continue en x_0 si et seulement si pour toute suite réelle (u_n) de points de I convergeant vers x_0, la suite $(f(u_n))$ converge vers $f(x_0)$.

Démonstration

On applique tout simplement le théorème de caractérisation séquentielle des limites □

Corollaire - Limite de suite $u_{n+1} = f(u_n)$

Soit f une fonction continue et (u_n) une suite définie par u_0 et $\forall n \in \mathbb{N}$, $u_{n+1} = f(u_n)$.
Si (u_n) converge alors sa limite ℓ vérifie $f(\ell) = \ell$.

Démonstration

Si (u_n) converge vers ℓ et f continue, donc en ℓ en particulier,
alors $f(u_n)$ converge vers $f(\ell)$.
Or $f(u_n) = u_{n+1}$, donc elle converge aussi vers ℓ (suite extraite convergente).
Enfin, par unicité des limites, ℓ vérifie $\ell = f(\ell)$. □

Savoir faire - Démontrer la non-continuité d'une fonction en exploitant les suites

Le théorème précédent fournit un moyen de prouver qu'une fonction n'a pas de limite en a.

3. Fonction continue sur un ensemble (intervalle, segment...)

3.1. Fonctions continues sur I

Continuité sur un intervalle

La définition suivante donne la continuité sur un intervalle. On voit comment la notion de jauge (re)fait son entrée. Elle permet une *sorte* d'interversion des quantificateurs : $\forall\, x_0 \exists\, \eta$:

Définition - Continuité sur un intervalle

Soit $f \in \mathscr{F}(I,\mathbb{R})$.
On dit que f est continue sur I si elle est continue en tout point de I

$$\forall\, x_0 \in I, \forall\, \epsilon > 0, \exists\, \delta > 0 \mid , \forall\, x \in I, |x - x_0| \leqslant \delta \Rightarrow |f(x) - f(x_0)| \leqslant \epsilon$$

ou de manière équivalente

$$\forall\, \epsilon > 0 \exists\, \delta_\epsilon : I \to \mathbb{R}_+^* \text{ jauge } \mid \forall\, x \in I, |x - x_0| \leqslant \delta_\epsilon(x_0) \Rightarrow |f(x) - f(x_0)| \leqslant \epsilon$$

On note $C(I)$ ou $\mathscr{C}^0(I)$ l'ensemble des fonctions continues sur I. ($C(I,\mathbb{R})$ ou $\mathscr{C}^0(I,\mathbb{R})$ s'il y a un risque de confusion sur l'ensemble d'arrivée).

Attention - Fonctions usuelles, continues ?

La plupart des fonctions usuelles sont continues sur leur ensemble de définition, mais il existe des fonctions qui ne sont pas continues partout, par exemple la fonction partie entière ou la fonction indicatrice de $\{0\}$.
Il existe même des fonctions nulle part continues, comme le montre l'exercice suivant

Exercice
Montrer que la fonction indicatrice de $\mathbb{Q}$, $1_{\mathbb{Q}}$, n'est continue en aucun point de $\mathbb{R}$.

Correction
Soit $x \in \mathbb{R}$.
On sait que $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont dense dans $\mathbb{R}$.
Donc il existe (u_n), suite de rationnels et (v_n) suite d'irrationnels tel que $\lim(u_n) = x = \lim(v_n)$.
Et pour tout $n \in \mathbb{N}$, $1_{\mathbb{Q}}(u_n) = 1$ alors que $1_{\mathbb{Q}}(v_n) = 0$.
Donc $1_{\mathbb{Q}}$ n'admet pas de limite en x. Ceci est vrai pour tout x.
Donc $1_{\mathbb{Q}}$ n'est continue en aucun point.

Une application : résoudre des équations fonctionnelles

Exercice
On veut déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ continues vérifiant

$$\forall (x,y) \in \mathbb{R}^2,\ f(x+y) = f(x) + f(y).$$

1. Déterminer $f(0)$. Montrer que f est impaire.
2. Déterminer la restriction de f à $\mathbb{N}$, à $\mathbb{Z}$, puis à $\mathbb{Q}$.
3. Déterminer finalement f.

Correction

1. $f(0+0) = f(0) = f(0) + f(0) = 2f(0)$, donc $(2-1)f(0) = 0$, donc $f(0) = 0$.
   Soit $x \in \mathbb{R}$, $f(0) = 0 = f(x) + f(-x)$, donc $f(-x) = -f(x)$.
   Ainsi f est impaire.
2. $f(2) = f(1) + f(1) = 2f(1)$.
   Par récurrence, $f(n) = nf(1)$, pour tout $n \in \mathbb{N}$.
   Puis $f(-n) = -f(n) - nf(1)$, par imparité, donc $f(m) = mf(1)$, pour tout $m \in \mathbb{Z}$.
   Toujours par récurrence, $mf(1) = f(m) = f(n\frac{m}{n}) = nf(\frac{m}{n})$.
   Donc pour tout $r \in \mathbb{Q}$, $f(r) = rf(1)$.
   On a intérêt pour la récurrence de montrer que $f(na) = nf(a)$, pour tout $a \in \mathbb{R}$
3. Par continuité, pour tout $x \in \mathbb{R}$, $f(x) = xf(1)$ (avec une suite $(r_n) \in \mathbb{Q}^{\mathbb{N}}$ qui converge vers x).

Savoir faire - Définir f (continue) de X à $\overline{X}$

Si f est définie sur un ensemble X, la continuité de f peut permettre d'étendre f sur $\overline{X}$.

Opérations sur les fonctions et continuité

Proposition - Opération de continuité

Si f et g sont deux fonctions de I dans $\mathbb{R}$, continues en $x_0 \in I$, alors $|f|$, $f+g$, fg sont continues en x_0, ainsi que $\frac{1}{g}$ et $\frac{f}{g}$ si $g(x_0) \neq 0$.
On a le même résultat concernant la continuité sur un intervalle I.

Démonstration
Pour démontrer ce résultat on applique directement le théorème d'opération sur les limites □

Exercice
Soit $f : \mathbb{R} \to \mathbb{R}$ et $x_0 \in \mathbb{R}$. On définit les fonctions f^+ et f^- par $f^+(x) = \max(f(x), 0)$ et $f^-(x) = \max(-f(x), 0)$. Montrer que si f est continue en x_0, alors f^+ et f^- sont continues en x_0.

Correction
Comme f est continue en x_0, il en est de même de $|f|$.
Puis $f^+ = \frac{1}{2}(f + |f|)$ et $f^- = \frac{1}{2}(|f| - f)$, donc par addition f^+ et f^- sont continues en x_0.
On remarque que la réciproque est vraie : si f^+ et f^- sont continue en x_0, alors $f = f^+ - f^-$ l'est également.

Proposition - Continuité d'une composée

Soient I et J deux intervalles de $\mathbb{R}$, $f \in \mathscr{F}(I,\mathbb{R})$, $g \in \mathscr{F}(J,\mathbb{R})$, $f(I) \subset J$. Soit $x_0 \in I$. Si f est continue en x_0 et g continue en $f(x_0)$, alors $g \circ f$ est continue en x_0.
On a le même résultat concernant la continuité sur J de g, sur I de f et donc également de $g \circ f$.

Démonstration
On applique le théorème de composition des limites □

3.2. Prolongement par continuité

Définition - Prolongement par continuité

Soit I un intervalle.

— Soit $f : I \to \mathbb{R}$, x_0 une extrémité réelle de I, $x_0 \notin I$.
Si f admet une limite réelle ℓ en x_0, alors la fonction $\tilde{f}$ définie sur $I \cup \{x_0\}$ par

$$\begin{cases} \tilde{f}(x) = f(x) \text{ si } x \neq x_0; \\ \tilde{f}(x_0) = \ell \end{cases}$$

prolonge f à $I \cup \{x_0\}$ et est continue en x_0.

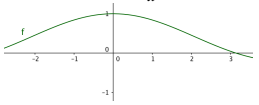
— Si $x_0 \in I$, si f définie sur $I \setminus \{x_0\}$ admet des limites réelles à droite et à gauche en x_0 et si ces limites sont égales (à ℓ) alors la fonction $\tilde{f}$

définie sur I par
$$\begin{cases} \tilde{f}(x) = f(x) \text{ si } x \neq x_0; \\ \tilde{f}(x_0) = \ell \end{cases}$$
prolonge f à I et est continue en x_0.
Dans les deux cas $\tilde{f}$ s'appelle le prolongement par continuité de f en x_0.

Exemple - $x \mapsto \dfrac{\sin x}{x}$

La fonction définie sur $\mathbb{R}^*$ par $x \mapsto \dfrac{\sin x}{x}$ est prolongeable par continuité à $\mathbb{R}$.

Représentation - $\dfrac{\sin x}{x}$



Remarque - Sur le vocabulaire
Si f n'est pas définie en x_0, il y a une infinité de façon de définir un prolongement de f à $I \cup \{x_0\}$, mais il y a au plus un prolongement qui soit continu, c'est le prolongement par continuité.

Exercice

Montrer que la fonction $x \mapsto x\left\lfloor \dfrac{1}{x} \right\rfloor$ est prolongeable par continuité en 0.

Correction

$\dfrac{1}{n}\left\lfloor \dfrac{1}{\frac{1}{n}} \right\rfloor = 1$. Si une limite existe, elle ne peut être qu'égale à 1.

Soit $x \neq 0$, on suppose que $n = \lfloor \frac{1}{x} \rfloor$, on a donc
$$n \leqslant \frac{1}{x} < n+1 \Rightarrow \begin{cases} xn \leqslant 1 < xn + x & \text{si} \quad x > 0 \\ xn \geqslant 1 > xn + x & \text{si} \quad x < 0 \end{cases} \Rightarrow \begin{cases} 1 - x < xn \leqslant 1 & \text{si} \quad x > 0 \\ 1 \leqslant xn < 1 - x & \text{si} \quad x < 0 \end{cases}$$
En faisant tendre x vers 0, par encadrement : $xn = x\lfloor \frac{1}{x} \rfloor \to 1$.
La fonction est donc prolongeable par continuité en 0 et a pour limite 1.

Savoir faire - Démontrer la continuité de f sur I ou prolonger la continuité de f sur I

Dans les deux cas, la méthode est la même :

1. On s'assure, par les théorèmes généraux, que f est continue sur I sauf en un point x_0 particulier.
2. Puis on regarde la limite de f en x_0.
   - Si $x_0 \in \mathscr{D}_f$, alors $f(x_0)$ existe. Il s'agit de démontrer la continuité de f en x_0.
   - Si $x_0 \notin \mathscr{D}_f$, alors $f(x_0)$ n'existe pas (ou pas encore). Il s'agit de voir si on peut ajouter un point x_0 dans l'ensemble de définition de f. De manière à ce que f reste continue. On dit que l'on fait un prolongement par continuité de f.

3.3. Théorème des valeurs intermédiaires

C'est un théorème de surjectivité. L'hypothèse est simple : la continuité de f.

Théorème - Théorème des valeurs intermédiaires
Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ continue.
Soient a et b deux réels, $(a,b) \in I^2$ et $a < b$. On suppose que $f(a) \times f(b) \leqslant 0$.
Alors il existe $c \in [a,b]$ tel que $f(c) = 0$.

La démonstration a été vu au chapitre précédent avec le processus de dichotomie. A savoir (re)faire.

Corollaire - TVI entre $f(a)$ et $f(b)$
Soit $f : I \to \mathbb{R}$ continue sur I. Soient a et b deux réels, $(a,b) \in I^2$ et $a < b$.
Alors pour toute valeur d comprise entre $f(a)$ et $f(b)$ il existe $t \in [a,b]$ tel

Pour aller plus loin - Exercices
Autre démonstration possible pour l'élève motivé :
démontrer le TVI avec l'axiome de la borne supérieure.

que $f(t) = d$.

Démonstration
Soit $d \in (f(a), f(b))$.
On considère $g : x \mapsto f(x) - d$.
On a $g(a) \times g(b) = (f(a) - d)(f(b) - d) < 0$. Donc il existe $t \in [a,b]$ tel que $g(t) = 0$.
Cela donne $f(t) = g(t) + d = d$ □

Corollaire - Image d'un intervalle par une fonction continue
Soit I un intervalle et f une fonction continue sur I. Alors $f(I)$ est un intervalle de $\mathbb{R}$.
Mieux : si I est un connexe de $\mathbb{R}$, alors $f(I)$ est également connexe.

Démonstration
Soient $y_1, y_2 \in f(I)$.
Alors il existe x_1 et $x_2 \in I$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.
Soit $y \in [y_1, y_2]$, d'après le corollaire précédent, il existe $t \in [x_1, x_2]$ tel que $f(t) = y$.
Donc $t \in I$ et $y \in f(I)$ ainsi $f(I)$ est bien un intervalle. □

Exercice
Montrer que toute fonction polynomiale de degré impair s'annule au moins une fois sur $\mathbb{R}$.

Correction
Soit ax^n le terme dominant du polynôme, on a $\lim\limits_{+\infty} p = \text{signe}(a)\infty$ et $\lim\limits_{-\infty} p = -\text{signe}(a)\infty$.
On applique le TVI à p continue, et il existe $t \in \mathbb{R}$ tel que $p(t) = 0$.
On verra une autre démonstration très différente dans le chapitre sur les polynômes

Exercice
Soit $f : [0,1] \to [0,1]$ continue. Montrer que f admet un point fixe.

Correction
Soit $\varphi : x \mapsto f(x) - x$.
Alors $\varphi(0) = f(0) \geqslant 0$ et $\varphi(1) = f(1) - 1 \leqslant 0$.
Donc il existe $t \in [0,1]$ tel que $\varphi(t) = 0$ i.e. $f(t) = t$

Exercice
Supposons que f continue et ne s'annule pas. Donc pour tout $t \in [a,b]$, $f(t) \neq 0$.
Soit $\delta : [a,b] \to \mathbb{R}_+^*$, $t \mapsto \alpha(t) > 0$, tel que $f([t - \alpha(t), t + \alpha(t)]) \subset [f(t) - \epsilon, f(t) + \epsilon]$ avec $\epsilon = \left| \dfrac{f(t)}{2} \right|$.
En appliquant le lemme de Cousin, montrer que f est de signe constant. Conclure.

Correction
Pour tout t, que $f(t)$ soit positif ou négatif : $0 \notin [f(t) - \epsilon, f(t) + \epsilon]$, donc $0 \notin f([t - \alpha(t), t + \alpha(t)])$.
Soit $([x_{i-1}, x_i], t_i)_{i \in \mathbb{N}_n}$, une subdivision δ-fine de $[a,b]$.
Alors pour tout $i \in \mathbb{N}_n$, $f(x_{i-1})$ et $f(x_i)$ sont du signe de $f(t_i)$. Nécessairement, tous les $f(t_i)$ sont de même signe.
En fait, on a mieux : $f([x_{i-1}, x_i])$ est non nul, (stricitement) du signe de $f(t_i)$. Donc f ne s'annule jamais.
On a démontré, avec le lemme de Cousin, le théorème des valeurs intermédiaires.

3.4. Cas de l'image d'un segment par f continue

Théorème - Théorème de Weierstrass
Soit $f : [a,b] \to \mathbb{R}$ continue sur le segment $[a,b]$. Alors f est bornée et atteint ses bornes :
$$\exists (x_1, x_2) \in [a,b]^2 \mid f(x_1) = \inf_{x \in [a,b]} f(x) \text{ et } f(x_2) = \sup_{x \in [a,b]} f(x).$$
$f(x_1)$ s'appelle l'infinimum de f et $f(x_2)$ le supremum de f.

Remarque - Mieux

Si f est continue. Si K est un compact de $\mathbb{R}$, alors $f(K)$ est également compact.

Heuristique - Deux résultats!

Il y a en fait deux parties dans ce théorème :
- $f([a,b])$ est borné. C'est l'existence de $\sup_{x\in[a,b]} f(x)$.
- Cette borne supérieure est atteinte : $\exists\, x_0 \in [a,b]$ tel que $f(x_0) = \sup_{x\in[a,b]} f(x)$

La démonstration se fera également en deux temps (avec le principe de dichotomie).
On notera que pour cette démonstration, on exploite de deux façons distinctes ce principe : une fois par l'absurde (méthode ascendante et globale), une fois pour exhiber un nombre en particulier (méthode descendante et locale).

Démonstration

1. On considère la fonction d'intervalle G définit par :
pour tout $\alpha < \beta \in [a,b]$, $G(\alpha,\beta) = 0$ si $f([\alpha,\beta])$ est majorée et $G(\alpha,\beta) = 1$ sinon.
G est sous-additive :

$$G(\alpha,\beta) + G(\beta,\gamma) = 0 \Rightarrow f([\alpha,\beta]) \text{ et } f([\beta,\gamma]) \text{ sont majorée}$$

$$\Rightarrow f([\alpha,\gamma]) \text{ est majorée par } \max(\sup_{[\alpha,\beta]} f, \sup_{[\beta,\gamma]} f) \Rightarrow G(\alpha,\gamma) = 0$$

Si $G([a,b]) = 1$, alors il existe (a_n), (b_n) adjacentes telles que pour tout entier n, $G(a_n,b_n) = 1$.
On note $\ell = \lim(a_n)(= \lim(b_n))$. f est continue en ℓ

$$\exists\, \eta > 0 \mid |x-\ell| < \eta \Rightarrow |f(x) - f(\ell)| \leqslant 1 \Rightarrow f(x) \leqslant f(\ell) + 1$$

Par ailleurs, comme $\ell = \lim(a_n)(= \lim(b_n))$, il existe N tel que $|a_N - \ell| \leqslant \eta$ et $|b_N - \ell| \leqslant \eta$.
et donc pour tout $x \in [a_n,b_n]$, $|x-\ell| < \eta$ et donc $f([a_n,b_n])$ est majorée par $f(\ell)+1$.
Donc $G(a_n,b_n) = 0$. On a une contradiction. Donc $G(a,b) = 0$: $f([a,b])$ est majorée.
2. On note $M = \sup f([a,b])$. On note $H(\alpha,\beta) = 1$ ssi $\sup f([\alpha,\beta] = M$ et $H(\alpha,\beta) = 0$ sinon.
H est sous-additive : $\sup f([\alpha,\gamma]) = \max(\sup f([\alpha,\beta]), \sup f([\beta,\gamma]))$.
Puis, nécessairement $H(a,b) = 1$, donc il existe (a_n) et (b_n) adjacentes telles que pour tout $n \in \mathbb{N}$, $H(a_n,b_n) = 1$.
Notons $\ell = \lim(a_n)(= \lim(b_n))$.
Pour tout entier n, $\sup f([a_n,b_n]) = M$, donc il existe $c_n \in [a_n,b_n]$ tel que $M - \frac{1}{n} < f(c_n) \leqslant M$.
Comme $a_n \leqslant c_n \leqslant b_n$, alors $(c_n) \to \ell$ donc par continuité de f en ℓ : $f(c_n) \to f(\ell)$
puis par encadrement $f(c_n) \to M$.
Par unicité de la limite : $M = f(\ell)$. □

Exercice

Démontrer le théorème de Weierstrass à l'aide du théorème de Bolzano-Weierstrass.

1. Supposons que f n'est pas bornée sur $[a,b]$.
Montrer qu'il existe $(x_n) \in [a,b]^{\mathbb{N}}$ tel que $f(x_n) \to +\infty$.
En déduire une contradiction avec le théorème de Bolzano-Weierstrass.
2. On considère alors $M = \sup f$. Montrer qu'il existe $(y_n) \in [a,b]^{\mathbb{N}}$ tel que $f(y_n) \to M$.
Conclure avec le théorème de Bolzano-Weierstrass.

Correction

1. Si f n'est pas bornée, alors pour tout $n \in \mathbb{N}$, $\exists\, x_n \in [a,b]$ tel que $f(x_n) \geqslant n$.
Ainsi $f(x_n) \to +\infty$ et on peut extraire de (x_n) une suite convergente (BW) vers $\ell = \lim x_{\varphi(n)}$.
Par continuité : $f(x_{\varphi(n)}) \to f(\ell) < +\infty$. C'est impossible.
Donc f est bien bornée
2. On considère alors $M = \sup f$.
Donc $\forall\, n \in \mathbb{N}$, $\exists\, y_n \in [a,b]$ tel que $f(y_n) \leqslant M < f(y_n) + \frac{1}{n}$.
Donc il existe $(y_n) \in [a,b]^{\mathbb{N}}$ tel que $f(y_n) \to M$.
Et on peut extraire de (y_n) une suite convergente (BW) vers $\ell' = \lim y_{\psi(n)} \in [a,b]$.
Par continuité : $f(y_{\psi(n)}) \to f(\ell') = M$, par unicité de la limite.

Exercice

Démontrer le théorème de Weierstrass à l'aide du lemme de Cousin.
L'existence d'un maximum est facile dans le cas d'un ensemble fini. En prenant un jauge puis une subdivision pointée bien choisies, on peut réduire à la recherche d'un maximum pour un nombre fini de points

Correction

On applique un raisonnement par l'absurde.
Supposons que f n'admette pas de maximum sur $[a,b]$.
Soit $t \in [a,b]$, comme $f(t)$ n'est pas un maximum, il existe $y_t \in [a,b]$ tel que $f(y_t) > f(t)$.
Soit $\epsilon_t = \frac{f(y_t)-f(t)}{2} > 0$, $\exists\, \eta_t > 0$ tq $\forall\, u \in [t-\eta, t+\eta]$, $|f(u)-f(t)| < \epsilon$, donc $f(u) < \frac{f(y_t)+f(t)}{2} < f(y_t)$.
On définit alors $\delta(t) = \eta_t$.
Soit $([x_{i-1},x_i], t_i)$ une subdivision δ-fine.

$$\forall\, i \in \mathbb{N}_n \qquad \exists\, y_i \text{ tel que } \forall\, u \in [x_{i-1},x_i] \subset [t_i - \delta(t_i), t_i + \delta(t_i)] = [t_i - \eta_{t_i}, t_i + \eta_{t_i}], f(u) < f(y_i)$$

Soit $k \in \mathbb{N}_n$ tel que $y_k = \max(y_i)$. Puis il existe j tel que $y_k \in [x_{j-1},x_j]$.
On a alors $f(y_k) < f(y_j) \leqslant f(y_k)$, donc $f(y_k) < f(y_k)$. Impossible.

Histoire - Karl Weierstrass



Karl Weierstrass est né le 31 octobre 1815 à Ostenfelde (Westphalie), et est mort le 19 février 1897 à Berlin. C'était un mathématicien allemand, souvent qualifié de « père de l'analyse moderne ». Il a été lauréat de la médaille Copley en 1895.

Théorème - Image d'un segment par une fonction continue

Soit $f : [a,b] \to \mathbb{R}$ continue sur le segment $[a,b]$. Alors $f([a,b])$ (image directe du segment) est un segment de $\mathbb{R}$.

Démonstration

C'est un corollaire du théorème précédent. □

Exercice

Montrer qu'une fonction périodique, continue sur $\mathbb{R}$, est bornée et atteint ses bornes.

Correction

Soit f périodique de période T.
Donc $f(\mathbb{R}) = f([0,T])$. On applique ensuite le théorème à f sur le segment borné $[0,T]$

Savoir faire - Montrer l'existence d'un point x tel que ...

Plusieurs possibilités :
- Théorème des valeurs intermédiaires (φ continue sur $]a,b[$) :
$\exists\, c \in]a,b[$ tel que $\varphi(c) \in [\varphi(a),\varphi(b)]$ ou $[\varphi(b),\varphi(a)]$
- Théorème de Weierstrass (φ continue sur $[a,b]$) :
$\exists\, c \in [a,b]$ tel que $\varphi(a) = \sup_{[a,b]} \varphi$
- Principe de dichotomie.
$\exists\, ([a_n,b_n])_n$ suite de segments emboîtés de limite ℓ telle que...
- Principe de convergence monotone ((a_n) monotone et bornée).
$\exists\, \ell = \lim(a_n)$.
- Théorème de Bolzano-Weierstrass ((a_n) suite bornée).
$\exists\, c$, limite d'une sous-suite de (a_n) telle que...
- Théorème de Cauchy ((a_n) suite de Cauchy).
$\exists\, c$, limite de (a_n) telle que...
- Une autre possibilité au chapitre suivant avec le théorème de Rolle (ou E.A.F.) - (φ dérivable sur $]a,b[$) :
$\exists\, c \in]a,b[$ tel que $\varphi'(c) = \frac{\varphi(b)-\varphi(a)}{b-a}$

Si cela n'est pas naturel, la difficulté consiste à trouver la bonne fonction φ. En particulier, si on cherche un point fixe d'une fonction f, on prend $\varphi : x \mapsto f(x) - x$...

Exercice

Soit f continue sur $[a,b]$ et $\alpha \in \mathbb{R}$ tel que pour tout $x \in [a,b]$, $f(x) < \alpha$.
Montrer qu'il existe $\epsilon > 0$ tel que $\forall\, x \in [a,b]$, $f(x) \leqslant \alpha - \epsilon$.

Correction

D'après le théorème de Weierstrass, il existe $c \in [a,b]$ tel que $\forall\, x \in [a,b]$, $f(x) \leqslant f(c)$.
Or $f(c) < \alpha$. Notons $\epsilon = \alpha - f(c) > 0$, cela répond à la question posée.

Exercice

Soit $f : [a,b] \to [a,b]$, continue tel que pour tout $x \neq y \in [a,b]$, $|f(y) - f(x)| < |y - x|$.

1. Montrer que f admet un unique point fixe, noté x_0.
2. On considère la suite (u_n) définie par récurrence par $u_0 \in [a,b]$ et $u_{n+1} = f(u_n)$.
Montrer que $(u_n) \to x_0$.

Correction

On considère $\varphi : x \mapsto |f(x) - x|$, continue sur $[a,b]$ (soustraction de fonctions continues.

1. Démontrons d'abord l'unicité (plus simple). Si x_1 et x_2 sont des points fixes de f :
$|f(x_1)-f(x_2)| = |x_1-x_2| < |x_1-x_2|$, par hypothèse, sauf si $x_1 = x_2$.
Donc nécessairement $x_1 = x_2$, et le point fixe de f est au plus unique.
$[a,b]$ est un segment, donc φ (continue) admet un minimum sur $[a,b]$ en x_0 :

$$\forall\, x \in [a,b], \qquad \varphi(x_0) \leqslant \varphi(x)$$

Or $\varphi(x_0) = f(x_0) - x_0$. Considérons $x = f(x_0)$, on a donc

$$\varphi(x) = |f(x)-x| = |f(x)-f(x_0)| < |x-x_0| = |f(x_0)-x_0| = \varphi(x_0)$$

On a une contradiction, si $x = f(x_0) \neq x_0$. Donc nécessairement $x_0 = f(x_0)$.

2. Posons pour tout $n \in \mathbb{N}$, $v_n = |u_n - x_0|$. Fixons $n \in \mathbb{N}$.

$$v_{n+1} = |f(u_n)-f(x)| < |u_n - x| = v_n$$

Donc la suite (v_n) est décroissante, minorée par 0 donc convergente. On note $\ell = \lim(v_n)$.
Par ailleurs, (u_n) est bornée (dans $[a,b]$), et donc admet une sous-suite convergente $(u_{\psi(n)}) \to m$.

$$v_{\psi(n)} = |u_{\psi(n)} - x_0| \to |m - x_0| \qquad v_{\psi(n)} \to \ell$$

Par unicité de la limite : $|m-x_0| = \ell$.
Si $m \neq x_0$: $|f(m)-f(x_0)| = |f(m)-x_0| < |m-x_0| = \ell$.
Mais aussi, par continuité de f :

$$|f(m)-x_0| = |f(\lim(u_{\psi(n)}))-x_0| = |\lim f(u_{\psi(n)})-x_0| = \lim|u_{\psi(n)+1}-x_0| = \lim v_{\psi(n)+1} = \ell$$

On a donc $\ell < \ell$. Impossible. Donc $m = x_0$, $\ell = 0$ et $(u_n) \to x_0$

3.5. Théorème de la bijection (bis)

C'est un théorème d'injectivité. L'hypothèse est simple, en plus de la continuité : la stricte monotonie de f.

Théorème - Injectivité et monotonie stricte
Soit $f : I \to \mathbb{R}$ continue sur I. Alors f est injective si et seulement si elle est strictement monotone.

Démonstration
Si f est strictement monotone, alors pour $x_1 \neq x_2$, on a $f(x_1) \neq f(x_2)$.
(par exemple : f décroissante, $x_1 < x_2$ alors $f(x_1) > f(x_2)\ldots$)
Donc f est injective.
Réciproquement, si f n'est pas strictement monotone.
Il existe $x_1 < x_2 < x_3$ tel que $f(x_1) \leqslant f(x_2)$ et $f(x_3) \leqslant f(x_2)$ (ou bien : $f(x_1) \geqslant f(x_2)$ et $f(x_3) \geqslant f(x_2)$).
On applique le TVI entre x_1 et x_2 puis entre x_2 et x_3 :

$$\exists\, y_1 \in]x_1,x_2[, y_2 \in]x_2,x_3[\mid f(y_1) = f(y_2) \in]\max(f(x_1),f(x_3)), f(x_2)[$$

$$\left(\exists\, y_1 \in]x_1,x_2[, y_2 \in]x_2,x_3[\mid f(y_1) = f(y_2) \in]f(x_2), \min(f(x_1),f(x_3))[\right)$$

et donc f n'est pas injective.
□

Théorème - Théorème de la bijection
Soit f une fonction définie sur I, continue, strictement monotone sur I (intervalle de $\mathbb{R}$), alors f est bijective de I sur l'intervalle $J = f(I)$.
Sa bijection réciproque f^{-1} est continue sur J, de même sens de variations que f.

Démonstration
• D'après le théorème des valeurs intermédiaires, on sait que $J = f(I)$ est un intervalle. f étant strictement monotone, elle est injective. f réalise donc une bijection de I sur J. On note f^{-1} sa bijection réciproque.
• On vérifie que f^{-1} est strictement monotone de même sens de variations que f :
Pour $(y_1,y_2) \in J^2$, on a

$$x_1 = f^{-1}(y_1) \Leftrightarrow f(x_1) = y_1 \text{ avec } x_1 \in I$$

$$x_2 = f^{-1}(y_2) \Leftrightarrow f(x_2) = y_2 \text{ avec } x_2 \in I$$

Si f est strictement croissante, on a

$$y_1 < y_2 \Leftrightarrow f(x_1) < f(x_2) \Leftrightarrow x_1 < x_2 \Leftrightarrow f^{-1}(y_1) < f^{-1}(y_2).$$

On obtient le résultat de la même manière pour f strictement décroissante.
• Montrons maintenant que f^{-1} est continue.
Soit $y_0 \in J$, $y_0 \neq \inf J$, et supposons f^{-1} strictement croissante.
Soit $x_0 = f^{-1}(y_0)$ et $\epsilon > 0$ suffisamment petit pour que $[x_0-\epsilon, x_0+\epsilon] \subset I$
(possible car x_0 ne peut être une borne de I).
Pour $y \in J$ on a

$$|f^{-1}(y)-f^{-1}(y_0)| \leqslant \epsilon \Leftrightarrow x_0-\epsilon \leqslant f^{-1}(y) \leqslant x_0+\epsilon \Leftrightarrow f(x_0-\epsilon) \leqslant y \leqslant f(x_0+\epsilon).$$

Comme f est strictement croissante, on a $f(x_0-\epsilon) < y_0 < f(x_0+\epsilon)$
et on peut trouver η tel que $[y_0-\eta, y_0+\eta] \subset [f(x_0-\epsilon), f(x_0+\epsilon)]$.
On a alors

$$\forall\, y \in J, |y-y_0| \leqslant \eta \Rightarrow |f^{-1}(y)-f^{-1}(y_0)| \leqslant \epsilon$$

et donc f^{-1} est continue en y_0. □

Remarque - Un théorème supplémentaire?
Le dernier point de la démonstration montre que :
si f est monotone sur I et $f(I)$ est un intervalle, alors f est nécessairement continue

3.6. Continuité uniforme

Définition - Fonction uniformément continue
Soit $f \in \mathscr{F}(I,\mathbb{R})$. On dit que f est uniformément continue sur I si

$$\forall\, \epsilon > 0, \exists \eta > 0 \mid \forall\, (x,y) \in I^2, |x-y| \leqslant \eta \Rightarrow |f(x)-f(y)| \leqslant \epsilon.$$

Attention - Différence entre continuité et uniforme continuité
La différence avec la définition de la continuité en x est que le réel η est le même pour tout $x \in I$.
A comparer :

$$\forall\, \epsilon > 0, \exists \eta > 0 \mid \forall\, (x,y) \in I^2, |x-y| \leqslant \eta \Rightarrow |f(x)-f(y)| \leqslant \epsilon.$$

$$\forall\, \epsilon > 0, \forall\, x \in I \exists \eta > 0 \mid \forall\, y \in I, |x-y| \leqslant \eta \Rightarrow |f(x)-f(y)| \leqslant \epsilon.$$

Attention - Ordre des quantificateurs
Insistons un peu... L'ordre des quantificateurs est important :
— $\exists \cdots \forall \cdots \neq \forall \cdots \exists \cdots$ (l'exercice qui suit donne un contre-exemple)
— En revanche : $\exists \cdots_1 \exists \cdots_2 = \exists \cdots_2 \exists \cdots_1$ et $\forall \cdots_1 \forall \cdots_2 = \forall \cdots_2 \forall \cdots_1$

Proposition - Implication
Une fonction uniformément continue sur I est continue sur I.

Démonstration
Soit f uniformément continue. Donc

$$\forall\, \epsilon>0, \exists \eta>0 \,|\, \forall\, (x,y)\in I^2, |x-y|\leqslant \eta \Rightarrow |f(x)-f(y)|\leqslant \epsilon.$$

On considère alors $x\in I$, donc

$$\forall\, \epsilon>0, \exists \eta>0 \,|\, \forall\, y\in I, |x-y|\leqslant \eta \Rightarrow |f(x)-f(y)|\leqslant \epsilon.$$

Et f est ainsi continue en x. □

Il existe une réciproque, dans le cadre des fonctions définie sur un segment. C'est le théorème de Heine :

Théorème - Théorème de Heine
Une fonction continue sur un segment de $\mathbb{R}$ est uniformément continue sur ce segment.

Remarque - Démonstration
Pour faire cette démonstration, nous allons exploiter le lemme de Cousin.
Il s'agit en fait de rendre η constant minimal (mais non nul). Ce serait simple si $\inf \eta > 0$.
Mais en fait, bien que $\forall\, x\in I$, $\eta(x)>0$, on n'a pas assurément $\inf\eta>0$.
Nous faisons la démonstration avec le lemme de Cousin, car il se joue ici la même manipulation que pour manipuler l'intégrale de Kurzweil-Henstock (que nous verrons - définie avec un jauge variable) est plus subtile que l'intégrale de Riemann (vue ailleurs - définie avec un jauge constante, grâce au théorème de Heine).

Remarque - Faire un schéma de la démonstration!
Pour les démonstrations topologiques, il faut faire des dessins!

Démonstration
Notons $[a,b]$ ce segment de $\mathbb{R}$. Soit f continue sur $[a,b]$.
Soit $\epsilon>0$.
Alors pour tout $t\in[a,b]$. Comme f est continue en t,

$$\exists\, \delta(t)>0 \text{ tel que } \forall\, x\in[a,b], |x-t|<\delta(t) \Longrightarrow |f(x)-f(t)|<\frac{\epsilon}{2}$$

si $x,y\in[t-\delta(t),t+\delta(t)]$, $|f(x)-f(y)|=|f(x)-f(t)+f(t)-f(y)|\leqslant |f(x)-f(t)|+|f(y)-f(t)|\leqslant\epsilon$.
Notons $\delta:[a,b]\to\mathbb{R}_+^*, t\mapsto\delta(t)$. δ est une jauge (c'est la jauge de continuité).
Considérons alors une subdivision δ-fine de $[a,b]$ que l'on peut noter $\mathscr{P}=\{(I_k,t_k), k\in[\![1,n]\!]\}$.
Rappelons que cela signifie que $[t_k-\frac{\delta(t_k)}{2}, t_k+\frac{\delta(t_k)}{2}]\subset I_k$.
Considérons alors $\eta=\frac{1}{4}\min(\delta(t_1),\delta(t_2),\dots\delta(t_n))$.
Soient $x,y\in[a,b]$, donc il existe $k\in[\![1,n]\!]$ tels que $x\in I_k$.
Si de plus $|x-y|\leqslant\frac{\eta}{4}$, alors x et $y\in[t_k-\delta(t_k),t_k+\delta(t_k)]$.
En effet, c'est vrai pour x par définition de k
et $|y-t_k|\leqslant|y-x|+|x-t_k|\leqslant\frac{\eta}{4}+\frac{\delta(t_k)}{2}\leqslant\frac{3}{4}\delta(t_k)$.
On a vu plus haut que cela implique $|x-y|\leqslant\epsilon$.
Par conséquent, f est uniformément continue sur $[a,b]$. □

Remarque - Commentaires sur la démonstration
En fait on peut dire les choses autrement :
— f est continue sur I, si

$$\forall\, \epsilon>0, \exists\, \delta: I\to\mathbb{R}_+^* \text{ (jauge) telle que } \forall\, x\in I, |y-x|\leqslant\delta(t)\Longrightarrow|f(y)-f(x)|\leqslant\epsilon$$

— f est uniformément continue sur I, si

$$\forall\, \epsilon>0, \exists\, \delta>0 \text{ (jauge } \textbf{CONSTANTE}\text{) telle que } \forall\, x\in I, |y-x|\leqslant\delta\Longrightarrow|f(y)-f(x)|\leqslant\epsilon$$

On comprend ainsi bien l'emploi du mot uniforme dans uniforme continuité.
On comprend également bien pourquoi l'uniforme continuité implique la continuité sur I (l'hypothèse est plus restrictive).
Enfin, la démonstration indique que si $[a,b]$ est un compact (segment de $\mathbb{R}$ - fermé et borné), alors il est possible de le considérer avec une propriété de finitude. On peut alors prendre $\delta=\min\delta(t_k)$, ce qui permet de passer de la continuité à la continuité uniforme.

Exercice
Soit f continue sur $[a,b]$ et $\epsilon>0$.
On note pour tout $\alpha<\beta\in[a,b]$,

$$G(\alpha,\beta)=0 \text{ si } \exists\, \delta>0 \mid \forall\, x,y\in[\alpha,\beta], |x-y|\leqslant\delta\Rightarrow|f(x)-f(y)|\leqslant\epsilon$$

et $G(\alpha,\beta)=1$, sinon.

Pour aller plus loin - Propriété de compacité
Dans la démonstration, on peut voir le passage de l'étude sur un ensemble infini (même pas dénombrable de points) - $\forall\, x,y$, à l'étude pour un nombre fini de points - t_k.
C'est vraiment la propriété de compacité

Pour aller plus loin - $\inf$ d'une réunion
On a exploité ici : $\inf_{x\in A\cup B} f(x) = \min(\inf_{x\in A} f(x), \inf_{x\in B} f(x))$.

Pour aller plus loin - Principe de prolongement
Si une propriété est vraie pour tout x sur un de ses voisinages, et vérifie la sous-additivité pour la fonction d'intervalle associée, alors cette propriété est vraie sur tout le segment (compact) sur lequel est étudié le problème

1. Montrer que G est sous-additive (on pourra utiliser la continuité en β)
2. Montrer que si $G(a,b)=1$, on a une contradiction.
3. En déduire que f est uniformément continue sur $[a,b]$

Correction

1. Soient $\alpha,\beta,\gamma\in[a,b]$ et supposons que $G(\alpha,\beta)=0$ et $G(\beta,\gamma)=0$.
Alors il existe $\delta_1>0$ tel que $\forall\, x,y\in[\alpha,\beta], |x-y|\leqslant\delta_1\Rightarrow|f(x)-f(y)|\leqslant\epsilon$.
Alors il existe $\delta_2>0$ tel que $\forall\, x,y\in[\beta,\gamma], |x-y|\leqslant\delta_2\Rightarrow|f(x)-f(y)|\leqslant\epsilon$.
Puis par continuité en β : $\exists\,\delta_3>0$ tel que $\forall\, x\in[a,b], |x-\beta|\leqslant\eta_3\Rightarrow|f(x)-f(\beta)|\leqslant\frac{\epsilon}{2}$.
Soient $\delta=\min(\delta_1,\delta_2,\delta_3)$. Soient $x,y\in[\alpha,\gamma]$ tels que $|x-y|\leqslant\delta$.
— Ou bien, $x,y\in[\alpha,\beta]$, donc $|x-y|\leqslant\delta\leqslant\delta_1\Rightarrow|f(x)-f(y)|\leqslant\epsilon$.
— Ou bien, $x,y\in[\beta,\gamma]$, donc $|x-y|\leqslant\delta\leqslant\delta_2\Rightarrow|f(x)-f(y)|\leqslant\epsilon$.
— Ou bien, $x\in[\alpha,\beta]$ et $y\in[\beta,\gamma]$ (SPDG),
on a alors $x<\beta<y$, et donc $|x-\beta|\leqslant|x-y|\leqslant\delta\leqslant\delta_3\Rightarrow|f(x)-f(\beta)|\leqslant\epsilon$.
on a alors $x<\beta<y$, et donc $|y-\beta|\leqslant|x-y|\leqslant\delta\leqslant\delta_3\Rightarrow|f(y)-f(\beta)|\leqslant\epsilon$.
Ainsi $|f(x)-f(y)|\leqslant|f(x)-f(\beta)|+|f(\beta)-f(y)|\leqslant\epsilon$, par inégalité triangulaire.
Donc $G(\alpha,\gamma)=0$.
Ainsi G est sous-addditive.
2. On suppose que $G(a,b)=1$. Donc d'après le principe de dichotomie, il existe (a_n), (b_n) adjacentes de limite ℓ telles que pour tout $n\in\mathbb{N}$, $G(a_n,b_n)=1$.
Or f est continue en ℓ. Donc il existe $\delta>0$ tel que $\forall\, x\in[a,b], |x-\ell|\leqslant\delta\Rightarrow|f(x)-f(\ell)|\leqslant\frac{\epsilon}{2}$.
On a alors pour tout $x,y\in[\ell-\delta,\ell+\delta]$, $|f(x)-f(y)|\leqslant|f(x)-f(\ell)|+|f(\ell)-f(y)|\leqslant\epsilon$ (Inégalité triangulaire).
Puis, il existe $n\in\mathbb{N}$, tel que $\ell-\delta<a_n<\ell<b_n<\ell+\delta$ et donc $\forall\, x,y\in[a_n,b_n]$, $|f(x)-f(y)|\leqslant\epsilon$.
Donc $G(a_n,b_n)=0$. Contradiction.
Ainsi $G(a,b)=0$.
3. D'après la question précédente, pour tout $\epsilon>0$, $\exists\,\delta>0 \mid \forall\, x,y\in[\alpha,\beta], |x-y|\leqslant\delta\Rightarrow|f(x)-f(y)|\leqslant\epsilon$.
Donc f est uniformément continue sur $[a,b]$.

Exercice
Il s'agit de démontrer le théorème de Heine avec le théorème de Bolzano-Weierstrass.
On considère f continue sur $[a,b]$ et par l'absurde, on suppose que f n'est pas uniformément continue.

1. Formaliser cette dernière hypothèse. On considèrera un tel ϵ.
2. Montrer qu'il existe deux suites (x_n) et (y_n) de $[a,b]$ telles que $(x_n-y_n)\to0$ mais pour tout $n\in\mathbb{N}$, $|f(x_n)-f(y_n)|>\epsilon$
3. Aboutir à une contradiction en exploitant le théorème de Bolzano-Weierstrass

Correction

1. $\exists\,\epsilon>0, \forall\,\eta>0, \exists\, x,y\in[a,b]$ tel que $|x-y|\leqslant\eta$ et $|f(x)-f(y)|>\epsilon$.
On considèrera un tel ϵ.
2. On considère alors $\eta=\frac{1}{n}$, $\exists\, x_n,y_n\in[a,b]$ tel que $|x_n-y_n|\leqslant\frac{1}{n}$ et $|f(x)-f(y)|>\epsilon$ Dans ce cas : $(x_n-y_n)\to0$ et pour tout $n\in\mathbb{N}$, $|f(x_n)-f(y_n)|>\epsilon$
3. (x_n) est bornée, il existe φ tel que $(x_{\varphi(n)})$ converge vers $x\in[a,b]$.
Puis $y_{\varphi(n)}=[y_{\varphi(n)}-x_{\varphi(n)}]+x_{\varphi(n)}\to x$, par addition.
Puis par continuité de f sur $[a,b]$, donc en x : $|f(x_{\varphi(n)})-f(y_{\varphi(n)})|\to|f(x)-f(x)|=0$.
Impossible.

Pour aller plus loin - Fonction lipschitzienne
On dit que f est lipschitzienne sur I si :
il existe $k\in\mathbb{R}^+$ tel que

$$\forall\, x,y\in I, |f(x)-f(y)|\leqslant k|x-y|$$

Exercice

1. Montrer que si f est lipschitzienne sur I alors f est uniformément continue sur I.
Montrer que sinus est lipschitzienne sur $\mathbb{R}$ (donc uniformément continue sur $\mathbb{R}$).
2. Montrer que $x\mapsto\sqrt{x}$ est uniformément continue sur $[0,+\infty[$ mais n'est pas lipschitzienne sur $[0,+\infty[$.
3. Montrer que $x\mapsto x^2$ n'est pas uniformément continue sur $[0,+\infty[$.

Correction

1. Il suffit de prendre $\eta=\frac{\epsilon}{k}$.
D'après l'inégalité des accroissements finis, comme $|\sin'(u)|\leqslant1$, $|\sin x-\sin y|\leqslant1|x-y|$

2. Soit $\epsilon > 0$.
   Notons $\eta = \epsilon^2$. Supposons que $|x-y| \leqslant \eta$.
   On a, pour $x > y$: $\sqrt{x} - \sqrt{y} \leqslant \sqrt{x-y} \leqslant \epsilon$,
   en effet cela est équivalent à $\sqrt{x} \leqslant \sqrt{x-y} + \sqrt{y} \Leftrightarrow 0 \leqslant 2\sqrt{y(x-y)}$.
   Toujours avec l'inégalité des accroissements finis : comme la dérivée de $x \mapsto \sqrt{x}$ est $x \mapsto \frac{1}{2\sqrt{x}}$ qui tend vers l'infini en 0^+, on doit pouvoir montrer que $\sqrt{\cdot}$ n'est pas lipschitzienne.
   En effet, supposons qu'elle le soit avec un rapport k : $\forall\, x, y \in [0, +\infty[$, $|\sqrt{x} - \sqrt{y}| \leqslant k|x-y|$.
   En prenant $y = 0$, on aurait $\frac{\sqrt{x}}{x}$ qui serait borné, ce qui est faux.
3. $y_n = n$ et $x_n = n + \frac{1}{n}$.
   Alors $|x_n - y_n| \leqslant \frac{1}{n}$ et $|f(x_n) - f(y_n)| = 2 + \frac{1}{n^2}$.
   On a donc $|x_n - y_n| \to 0$ et $|f(x_n) - f(y_n)| > 2$. Ceci serait impossible si f était uniformément continue.

4. Généralisation aux fonctions à valeurs dans $\mathbb{C}$

Soit X une partie de $\mathbb{R}$.

4.1. Opérations classiques sur $\mathscr{F}(X, \mathbb{C})$

Définition - Transformations classiques
A partir de $f \in \mathscr{F}(X, \mathbb{C})$, on définit les applications suivantes à valeurs dans $\mathbb{R}$:
• $|f|$ (module de f) : $\forall x \in X$, $|f|(x) = |f(x)|$
• $\mathrm{Re} f$ (partie réelle de f) : $\forall x \in X$, $(\mathrm{Re} f)(x) = \mathrm{Re}(f(x))$
• $\mathrm{Im} f$ (partie imaginaire de f) : $\forall x \in X$, $(\mathrm{Im} f)(x) = \mathrm{Im}(f(x))$
On définit également $\overline{f}$, fonction conjuguée de f, à valeurs dans $\mathbb{C}$, par $\forall x \in X$, $\overline{f}(x) = \overline{f(x)}$

4.2. Fonctions bornées

Définition - Fonctions à valeurs complexes bornées
On dit que $f \in \mathscr{F}(X, \mathbb{C})$ est bornée si la fonction $|f| \in \mathscr{F}(X, \mathbb{R})$ est majorée, c'est-à-dire si
$$\exists M \in \mathbb{R},\ \forall x \in X,\ |f(x)| \leqslant M.$$

Attention - Majoration dans $\mathbb{C}$
Dire qu'une fonction à valeurs dans $\mathbb{C}$ est majorée, ou minorée, n'a pas de sens.

Proposition - Stabilité pour fonctions bornées
$f \in \mathscr{F}(X, \mathbb{C})$ est bornée si et seulement si $\mathrm{Re} f$ et $\mathrm{Im} f$ ($\in \mathscr{F}(X, \mathbb{R})$) sont bornées.
Toute combinaison linéaire et tout produit de deux fonctions bornées sont des fonctions bornées.

Démonstration
On a pour tout $z \in \mathbb{C}$, $|\mathrm{Re}(z)| \leqslant |z|$, $|\mathrm{Im}(z)| \leqslant |z|$.
Donc si f est bornée, il en est de même de $\mathrm{Re} f$ et $\mathrm{Im} f$.
On a également pour tout $z \in \mathbb{C}$, $|z| \leqslant |\mathrm{Re}(z)| + |\mathrm{Im}(z)| \leqslant |z|$.
Donc réciproquement, si $\mathrm{Re} f$ et $\mathrm{Im} f$ sont bornée, il en est de même de $|f|$.
Concernant les combinaisons linéaires, notons que
$$|\lambda f + \mu g| \leqslant |\lambda||f| + |\mu||g|$$
Et pour le produit : $|fg| = |f| \times |g|$ □

4.3. Limites

Définition - Limite de fonction complexe
On dit que la fonction f à valeurs dans $\mathbb{C}$ admet le complexe ℓ pour limite en $a \in \overline{\mathbb{R}}$ (ou que $f(x)$ tend vers ℓ quand x tend vers a) si la fonction à valeurs réelles $|f - \ell|$ tend vers 0 en a.

Attention - Pas de limite infinie pour des fonctions à valeurs complexes
On ne définit pas de limite infinie pour une fonction à valeurs complexes...

Proposition - Critère de convergence
Soit f une fonction à valeurs complexes, $\ell \in \mathbb{C}$ et $a \in \overline{\mathbb{R}}$.
Alors f admet ℓ pour limite en a si et seulement si les fonctions $\mathrm{Re} f$ et $\mathrm{Im} f$ admettent respectivement $\mathrm{Re}\ell$ et $\mathrm{Im}\ell$ pour limite en a.
On en déduit que si f admet une limite en a, celle-ci est unique.

Démonstration
On utilise, comme pour les suites, dans un sens les inégalités $|(\mathrm{Re} f)(x) - \mathrm{Re}\ell| \leqslant |f(x) - \ell|$ et $|(\mathrm{Im} f)(x) - \mathrm{Im}\ell| \leqslant |f(x) - \ell|$, dans l'autre sens $|f(x) - \ell|^2 = |(\mathrm{Re})(x) f - \mathrm{Re}\ell|^2 + |(\mathrm{Im} f)(x) - \mathrm{Im}\ell|^2$.
L'unicité provient de l'unicité pour les fonctions $\mathrm{Re} f$ et $\mathrm{Im} f$ (ou d'une démonstration directe copiée sur celle dans $\mathbb{R}$). □

Proposition - Limite donc bornée
Si f admet une limite en $a \in \overline{\mathbb{R}}$, alors f est bornée au voisinage de a.

Démonstration
La même proposition appliquée aux fonctions à valeurs dans $\mathbb{R}$, $\mathrm{Re} f$ et $\mathrm{Im} f$, ou une démonstration directe copiée sur celle dans $\mathbb{R}$. □

4.4. Opérations sur les limites

Proposition - Bilan
Soient $f, g \in \mathscr{F}(X, \mathbb{C})$, $(\ell, m) \in \mathbb{C}^2$, $(\lambda, \mu) \in \mathbb{C}^2$.
On suppose que $\lim_{x \to a} f(x) = \ell$ et $\lim_{x \to a} g(x) = m$. Alors
$$\lim_{x \to a} |f|(x) = |\ell|$$
$$\lim_{x \to a} \overline{f}(x) = \overline{\ell}$$
$$\lim_{x \to a} (\lambda f + \mu g)(x) = \lambda\ell + \mu m$$
$$\lim_{x \to a} \frac{f}{g}(x) = \frac{\ell}{m} \text{ pour } m \neq 0$$
Soit $f \in \mathscr{F}(X, \mathbb{C})$, $a \in \overline{\mathbb{R}}$, telle que $\lim\limits_{x \to a} f(x) = \ell \in \mathbb{C}$;
soit (u_n) une suite de X telle que $\lim\limits_{n \to +\infty} u_n = a$.
Alors $\lim\limits_{n \to +\infty} f(u_n) = \ell$.
Soient $f \in \mathscr{F}(X, \mathbb{C})$, $a \in \overline{\mathbb{R}}$, $\phi \in \mathscr{F}(I, \mathbb{R})$ telle que $\phi(I) \subset X$, $t_0 \in \overline{\mathbb{R}}$.
Si $\lim\limits_{x \to a} f(x) = \ell \in \mathbb{C}$ et $\lim\limits_{t \to t_0} \phi(t) = a$ alors $\lim\limits_{t \to t_0} (f \circ \phi)(t) = \ell$.

Démonstration
A partir des parties réelles et imaginaires, ou en généralisant les démonstrations sur $\mathbb{R}$ à $\mathbb{C}$. □

4.5. Continuité

I désigne un intervalle de $\mathbb{R}$ non réduit à un point.

Définition - Continuité d'une fonction à valeurs complexes
Soit f définie sur I et $a \in I$, f admet une limite en a équivaut à dire que $\mathrm{Re}f$ et $\mathrm{Im}f$ admettent des limites réelles en a, c'est-à-dire qu'elles sont continues en a
Si c'est le cas on dit que f est continue en a.
$f \in \mathscr{F}(I,\mathbb{C})$ est continue sur I si elle est continue en tout point de I.
Cela équivaut à dire que $\mathrm{Re}f, \mathrm{Im}f \in \mathscr{F}(I,\mathbb{R})$ sont continues sur I.
On note $\mathscr{C}(I,\mathbb{C})$ ou $\mathscr{C}^0(I,\mathbb{C})$ l'ensemble des fonctions continues de I dans $\mathbb{C}$.

Proposition - Stabilité par continuité
Si $f \in \mathscr{F}(I,\mathbb{C})$ est continue sur I alors $\overline{f} \in \mathscr{F}(I,\mathbb{C})$ et $|f| \in \mathscr{F}(I,\mathbb{R})$ sont continues sur I.
Soient $f, g \in \mathscr{C}(I,\mathbb{C})$, $(\lambda,\mu) \in$
Ce^2. Alors :
$\lambda f + \mu g \in \mathscr{C}(I,\mathbb{C})$ ($\mathscr{C}(I,\mathbb{C})$ est un s.e.v. de $\mathscr{F}(I,\mathbb{C})$).
Si g ne s'annule pas, $\dfrac{f}{g} \in \mathscr{C}(I,\mathbb{C})$.
Si $\phi \in \mathscr{C}(J,\mathbb{R})$ avec $\phi(J) \subset I$ alors $f \circ \phi \in \mathscr{C}(J,\mathbb{C})$.

Exercice
Les propriétés suivantes restent-elles vraies en passant de $\mathbb{R}$ à $\mathbb{C}$

1. Soit $f : [a,b] \to \mathbb{C}$ continue sur $[a,b]$. Alors f est bornée sur $[a,b]$ et il existe $x_0 \in [a,b]$ tel que $|f(x_0)| = \sup_{[a,b]} |f(x)|$.
2. Le théorème des valeurs intermédiaires (image continue d'un segment).

Correction

1. **VRAI** : c'est le résultat correspondant appliqué à la fonction à valeurs réelles $|f|$.
2. **FAUX** : théorème des valeurs intermédiaires, image continue d'un segment.
   ces théorèmes n'ont pas de sens puisque les images par f ne sont pas dans $\mathbb{R}$, et même si $f(a)f(b)$ est un réel négatif, f ne s'annule pas forcément.
   Contre-exemple : f définie sur $[0,2\pi]$ par $f(t) = e^{it}$. On a $f(0)f(\pi) = -1$ mais f ne s'annule jamais.

5. Bilan

Synthèse

- ⇝ La continuité est d'abord une notion locale, qui se généralise à un intervalle.
- ⇝ La continuité/limite est une notion subtile qui mérite qu'on y passe un temps conséquent. Pour n'en perdre pas trop, il faut parfois plonger dans l'abstraction.
- ⇝ L'un des plus importants résultats de topologie réelle est le TVI : il n'y a pas de trou dans $\mathbb{R}$ et toute transformation qui conserve une partie sans trou (ou intervalle) de $\mathbb{R}$ doit être continue. L'enjeu est donc la continuité! Il faut pour cela définir la notion de limite de fonction, en un point, puis sur un intervalle.
- ⇝ Nous terminons par l'étude des fonctions à valeurs dans $\mathbb{C}$.

Savoir-faire et Truc & Astuce du chapitre

- — Savoir-faire - Démontrer la non-continuité d'une fonction en exploitant les suites
- — Savoir-faire - Démontrer la continuité de f sur I ou prolonger f par continuité.
- — Savoir-faire - Définir f (continue) de X à $\overline{X}$
- — Savoir-faire - Démontrer la continuité de f sur I ou prolonger la continuité de f sur I
- — Savoir-faire - Montrer l'existence d'un point tel que…

Notations

Notations		*Définitions*	*Propriétés*	*Re*
$\mathscr{C}(I,\mathbb{R})$ $\mathscr{C}(I,\mathbb{C})$	(resp.	Ensemble des fonctions continues de l'intervalle I sur $\mathbb{R}$ (resp. sur $\mathbb{C}$)		

Retour sur les problèmes

87. C'est une des clés de l'analyse. Et pour avoir accès à la limite, en règle générale, on encadre…
88. Rappelons la définition du cours : une fonction est continue sur I, si elle continue en tout point de I. Et une fonction est continue en un point x de I, si *simplement* elle admet une limite en x.
89. Oui, on a vu par exemple l'indicatrice de $\mathbb{Q}$.
90. Si I est un intervalle, $f(I)$ est un intervalle. Mais il peut être ouvert et donc on n'a pas nécessairement x_0 tel que $f(x_0) = \sup If$. Par exemple avec $f : x \mapsto x$ et $I = [0,1[$. Pour tout $x \in I$, $f(x) < 1 = \sup_I f$.
    Si l'intervalle est fermé, les choses sont différentes (cf. théorème de Weierstrass).
91. Voir dernier chapitre du cours. Pour la continuité des fonctions de $\mathbb{C}$ dans $\mathbb{C}$, cela est a priori plus compliqué car il n'y a pas de relation d'ordre dans $\mathbb{C}$…

Chapitre 21

Dérivation (approfondissements)

Résumé -

Au début d'année, nous avons déjà rencontré des fonctions dérivables. « A l'époque », notre motivation était surtout de mettre au point quelques bons réflexes d'ordre calculatoires. Dans ce chapitre, il s'agit plutôt de démontrer les résultats exploitées précédemment…
La construction est comparable à celle du chapitre précédent (et exactement opposée à la démarche d'usage de la dérivée) :

- *la dérivation est une notion locale (dérivable en un point).*
- *elle est étendue ensuite sur un intervalle*
- *enfin elle est généralisée : à des dérivations d'ordre supérieure et à des fonctions à valeurs complexes*

Dans ce chapitre, nous découvrons deux résultats importants : le théorème de Rolle (qui donne l'existence -non constructive - d'un point à la qualité particulière) et l'inégalité des accroissements finis (qui montre que la connaissance d'une majoration de la dérivée donne une connaissance sur une majoration de la fonction d'origine). Quelques vidéos :

- *Lê Nguyên Hoang - Le théorème de Rolle - https ://www.youtube.com/watch ?v=ahX2fiXUNs0*
- *Irem Paris7 - Les pratiques enseignantes concernant la dérivée - https ://video.irem.univ-paris-diderot.fr/videos/watch/048ae57b-99d0-46e2-8b0b-27b1625c1d1f*

Sommaire

1. Problèmes 410
2. Dérivée 410
2.1. Définitions 410
2.2. Règles de calcul 412
2.3. Fonctions de classe $\mathscr{C}^k$ 414
3. Etude globale des fonctions dérivables 417
3.1. Théorème de Rolle 417
3.2. Egalité des accroissements finis 419
3.3. Inégalité des accroissements finis 421
3.4. Prolongement dérivable ou limite de la dérivée . . . 422
3.5. Prolongement de la règle de l'Hospital 425
4. Généralisation aux fonctions à valeurs complexes 426
4.1. Définitions 426
4.2. Opérations 427
5. Bilan 428

I désigne un intervalle de $\mathbb{R}$.

1. Problèmes

Problème 93 - Fonction continue nulle part dérivable.

Donner une fonction continue non dérivable en un point.
Donner une fonction continue non dérivable en une infinité de points.
Donner une fonction continue, nulle part dérivable.

Problème 94 - Dérivation d'ordre n…

… d'une somme de fonctions : que vaut $(f+g)^{(n)}$? Et $(f_1+f_2+\cdots+f_k)^{(n)}$?
… d'un produit de fonctions : que vaut $(f\times g)^{(n)}$? Et $(f_1\times f_2\times\cdots\times f_k)^{(n)}$?
… d'une composition de fonctions : que vaut $(f\circ g)^{(n)}$? Et $(f_1\circ f_2\circ\cdots\circ f_k)^{(n)}$?

Pour aller plus loin - Notation Weierstrass

On a vu aussi : f dérivable en a ssi il existe $A\in\mathbb{R}$ tel que $f(x)=f(a)+(x-a)(A+\epsilon(x))$ avec $\epsilon(x)\underset{x\to a}{\longrightarrow}0$

ϵ est définie ensuite comme $x\mapsto\dfrac{f(x)-f(a)}{x-a}-A$…

Problème 95 - Dérivation en un point

La dérivée en x_0 existe, signifie que $\frac{f(x_0+h)-f(x_0)}{h}$ admet une limite pour $h\to 0$.
Existe-t-il un rapport entre f est dérivable en x_0 et f' admet une limite en x_0 ? Et si oui, quelle est la nature de ce lien (condition nécessaire ? suffisante ? les deux ?)

Problème 96 - Théorème de la mouche

Supposons que nous sachions qu'une mouche se trouve dans une pièce (même petite), est-il possible d'obtenir une connaissance (même partielle) de sa vitesse ?
Supposons que nous sachions que nous connaissions même approximativement la vitesse d'une mouche, est-il possible d'obtenir une connaissance (même partielle) de sa position ?

Problème 97 - Fonctions complexes

Que se passe-t-il si $f:\mathbb{R}\to\mathbb{C}$, à valeurs complexes. Comment les inégalités vus en cours (accroissements finis…) peuvent se transmettre alors que $\mathbb{C}$ n'est pas naturellement ordonné ?
Autre question pour $f:z\in\mathbb{C}\mapsto\mathbb{C}$, que peut signifier f est dérivable ?

2. Dérivée

2.1. Définitions

Avec une notion de limite plus claire, on peut reprendre :

Définition - Fonction dérivable en un point
Soient $f : I \to \mathbb{R}$ et $a \in I$.

— On dit que f est dérivable en a si l'application (taux d'accroissement de f en a)

$$\begin{array}{rccc} \tau_a f : & I\setminus\{a\} & \to & \mathbb{R} \\ & x & \mapsto & \frac{f(x)-f(a)}{x-a} \end{array}$$

admet une limite finie en a.
Dans ce cas, cette limite est appelée nombre dérivé de f en a et est notée $f'(a)$ (ou $Df(a)$, ou $\frac{df}{dx}(a)$) :

$$f'(a) = \lim_{x\to a} \frac{f(x)-f(a)}{x-a} = \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}.$$

— Si $\tau_a f$ admet une limite finie à droite en a (a n'étant pas l'extrémité droite de I), on dit que f est dérivable à droite en a :

$$f'_d(a) = \lim_{x\to a, x>a} \frac{f(x)-f(a)}{x-a} = \lim_{x\to a_+} \frac{f(x)-f(a)}{x-a}$$

— Si $\tau_a f$ admet une limite finie à gauche en a (a n'étant pas l'extrémité gauche de I), on dit que f est dérivable à gauche en a :

$$f'_g(a) = \lim_{x\to a, x<a} \frac{f(x)-f(a)}{x-a} = \lim_{x\to a_-} \frac{f(x)-f(a)}{x-a}$$

De la définition, on peut affirmer :

Proposition - Dérivée à gauche et à droite
Si a n'est pas une extrémité de I, f est dérivable en a si et seulement si elle est dérivable à gauche et à droite en a et si $f'_g(a) = f'_d(a)$.

On a la définition équivalente, démontrée au chapitre 5.

Proposition - Définition de Weierstrass
On rappelle que f est dérivable en a, si et seulement si
Il existe $A \in \mathbb{R}$, $\epsilon : I \to \mathbb{R}$, continue et nul en a, tels que $f(x) = f(a) + (x-a)[A+\epsilon(x)]$.
Dans ce cas $f'(a) = A$.

Définition - Fonction dérivable
$f : I \to \mathbb{R}$ est dite dérivable sur I si elle est dérivable en tout point de I.

Exemple - $x \mapsto |x|$
L'application $x \mapsto |x|$ est dérivable sur $\mathbb{R}_+^*$, sur $\mathbb{R}_-^*$.
Elle est dérivable à droite et à gauche en 0.
Qu'en pensez-vous, peut-on dire que $x \mapsto |x|$ est dérivable sur $\mathbb{R}_+$?

Théorème - Dérivabilité ⇒ continuité
Si $f : I \to \mathbb{R}$ est dérivable (resp. dérivable à droite, resp. dérivable à gauche) en $a \in I$, alors f est continue (resp. continue à droite, resp. continue à gauche) en a.

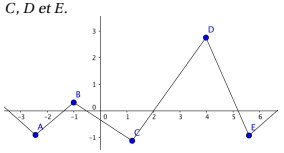
Pour aller plus loin - Fonctions lipschitzienne, hölderienne
Il existe des définitions adaptées pour des fonctions continues, mais non dérivables.
Par exemple les fonctions lipschitzienne vérifie :

$$\exists\, k \in \mathbb{R}_+ \mid \forall\, x, y \in I |f(x) - f(y)| \leqslant k|x-y|$$

D'une certaine façon, cela consiste à écrire que la fonction τ_a est bornée (mais sans nécessairement admettre une limite).
Pour les fonctions hölderiennes, il y a un coefficient supplémentaire :

$$\exists\, k \in \mathbb{R}_+, \exists\, a > 0 \mid \forall\, x, y \in I |f(x)-f(y)| \leqslant k|x-y|^a$$

Représentation - Fonction non dérivable
Pour être dérivable une fonction doit être « lisse ». Un skieur aux skis infiniment fins doit pouvoir skier sans à coup.
La courbe suivante n'est pas dérivable en A, B, C, D et E.



Démonstration
Si f est dérivable en a, alors cela signifie que $\lim_{x\to a} \frac{f(x)-f(a)}{x-a}$ existe.
Or le dénominateur tend vers 0, donc le numérateur aussi nécessairement.
Ainsi $\lim_{x\to a} f(x) = f(a)$. Et donc f est continue en a. □

Remarque - Réciproque fausse
La réciproque est fausse.
On peut le voir sur un graphe. On peut aussi le comprendre avec la fonction valeur absolue en 0.

Remarque - Approximation affine de f en a
Pour une fonction f dérivable en a, $f(x) = f(a) + f'(a)(x-a) + o(x-a)$ s'appelle le développement limité à l'ordre 1 de f en a, il donne, localement, une approximation affine de f.
Nous verrons une définition de ce o par la suite du cours.

2.2. Règles de calcul

On démontre des résultats énoncés au chapitre 5.

Proposition - Dérivation d'un produit
Soient f et g deux fonctions dérivables en a, λ et μ deux réels. Alors $\lambda f + \mu g$ et fg sont dérivables en a et

$$(\lambda f + \mu g)'(a) = \lambda f'(a) + \mu g'(a),$$

$$(fg)'(a) = f'(a)g(a) + f(a)g'(a)$$

Notons que les démonstrations découle des propriétés de stabilité de limite de fonctions…

Démonstration
Avec les notations Weierstrass :

$$\begin{aligned} \lambda f(x) + \mu g(x) &= \lambda[f(a) + (x-a)(f'(a)+\epsilon_1(x))] + \mu[g(a) + (x-a)(g'(a)+\epsilon_2(x))] \\ &\lambda f(a) + \mu g(a) + (x-a)[\lambda f'(a) + \mu g'(a) + \underbrace{\lambda\epsilon_1(x) + \mu\epsilon_2(x)}_{\epsilon_3(x)}] \end{aligned}$$

avec $\epsilon_3(x) \xrightarrow[x\to a]{} 0$, par addition de limite.

$$\begin{aligned} f(x)\times g(x) &= [f(a) + (x-a)(f'(a)+\epsilon_1(x))] \times [g(a) + (x-a)(g'(a)+\epsilon_2(x))] \\ &f(a)\times g(a) + (x-a)[f'(a)g(a) + f(a)g'(a) + \underbrace{(x-a)(g'(a)\epsilon_1(x) + f'(a)\epsilon_2(x))}_{\epsilon_4(x)}] \end{aligned}$$

avec $\epsilon_4(x) \xrightarrow[x\to a]{} 0$, par produit de limite.
□

Théorème - Dérivation de composition de fonctions
Soient J un intervalle de $\mathbb{R}$, $\phi : I \to \mathbb{R}$ telle que $\phi(I) \subset J$, $f : J \to \mathbb{R}$, $a \in I$.
Si ϕ est dérivable en a et f dérivable en $\phi(a)$ alors $f \circ \phi$ est dérivable en a et

$$(f\circ\phi)'(a) = \phi'(a) f'(\phi(a)).$$

Si ϕ est dérivable sur I, f dérivable sur J, alors $f \circ \phi$ est dérivable sur I et $(f\circ\phi)' = \phi' \times f' \circ \phi$.

Démonstration
Il suffit de regarder en un point.
On note $A = \varphi(a)$ et $X = \varphi(a) + (x-a)(\varphi'(a) + \epsilon_1(x))$

$$\begin{aligned} f\circ\varphi(x) &= f(\varphi(x)) = f[\varphi(a) + (x-a)(\varphi'(a)+\epsilon_1(x))] = f(X) \\ &= f(A) + (X-A)(f'(A)+\epsilon_3(X)) \\ &= f(\varphi(a)) + (x-a)(\varphi'(a)+\epsilon_1(x))(f'(A)+\epsilon_3(X)) \\ &= f(\varphi(a)) + (x-a)(f'(\varphi(a))\times\varphi'(a) + \underbrace{\epsilon_1(x)f'(A) + \epsilon_1(x)\epsilon_3(X)}_{\epsilon_2(x)}) \end{aligned}$$

avec $\epsilon_2(x) \xrightarrow[x\to a]{} 0$ par produit et addition. □

Théorème - Dérivée de l'inverse d'une fonction
Soient $f : I \to \mathbb{R}$, $a \in I$ tel que $f(a) \neq 0$ et f dérivable en a. Alors il existe un intervalle J de $\mathbb{R}$, voisinage de a dans I, tel que f ne s'annule pas sur J et $\frac{1}{f}$ (qui est donc définie sur J) est dérivable en a,

$$\left(\frac{1}{f}\right)'(a) = -\frac{f'(a)}{f(a)^2}$$

Démonstration
Pour tout $x \in J$ et $x \neq a$:

$$\frac{\frac{1}{f(x)} - \frac{1}{f(a)}}{x-a} = \frac{1}{f(x)f(a)} \frac{f(a)-f(x)}{x-a} \xrightarrow[x\to a]{} \frac{-1}{f^2(a)} f'(a)$$

□

Exercice
Nous souhaitons faire la démonstration à la Weiertrass

1. Ecrire le développement de $\frac{1}{f(x)}$ en exploitant la dérivée de f en a
2. Montrer que si $\varphi(x) \xrightarrow[x\to a]{} 0$, alors il existe ψ telle que $\psi(x) \xrightarrow[x\to a]{} 0$ et $\frac{1}{1+(x-a)(A+\varphi(x))} = 1-(x-a)(A+\psi(x))$.
3. En factorisant (nécessairement) par $\frac{1}{f(a)}$, montrer que f est dérivable en a et retrouver la valeur de $f'(a)$

Correction

1. $$\frac{1}{f(x)} = \frac{1}{f(a)+(x-a)(f'(a)+\epsilon(x))}$$
2. $1-(x-a)A - \frac{1}{1+(x-a)(A+\varphi(x))} = (x-A)\underbrace{\frac{-A(A+\varphi(x))}{1+(x-a)(A+\varphi(x))}}_{=\psi(x)}(x-a)$ avec $\psi(x) \xrightarrow[x\to a]{} 0$.
   Alors, par construction : $\frac{1}{1+(x-a)(A+\varphi(x))} = 1-(x-a)(A+\psi(x))$
3. $$\frac{1}{f(x)} = \frac{1}{f(a)} \times \frac{1}{1+(x-a)(\frac{f'(a)}{f(a)}+\epsilon_2(x))}$$
   $$= \frac{1}{f(a)} \times \left(1-(x-a)(\frac{f'(a)}{f(a)}+\epsilon_3(x))\right) = \frac{1}{f(a)} + (x-a)\left(\frac{-f'(a)}{(f(a))^2}+\epsilon_3(x)\right)$$
   Donc $\frac{1}{f}$ est dérivable en a et $\left(\frac{1}{f}\right)'(a) = \frac{-f'(a)}{f^2(a)}$

Théorème - Dérivation de la fonction réciproque en un point
Soient $f : I \to \mathbb{R}$ continue, strictement monotone sur I, dérivable en $a \in I$.
On sait que f réalise une bijection de I sur $f(I)$.
Alors f^{-1} est dérivable en $f(a)$ si et seulement si $f'(a) \neq 0$ et

$$(f^{-1})'(f(a)) = \frac{1}{f'(a)}.$$

Corollaire - Fonction réciproque
Soit f dérivable, strictement monotone sur I telle que f' ne s'annule pas sur I. Alors f^{-1} est dérivable sur $J = f(I)$ et $(f^{-1})' = \frac{1}{f' \circ f^{-1}}$.

Démonstration
Pour y proche de $f(a)$ (on note $x = f^{-1}(y)$, et $a = f^{-1}(A)$ donc $A = f(a)$) :

$$\frac{f^{-1}(y)-f^{-1}(f(a))}{y-f(a)} = \frac{x-a}{f(x)-f(a)}$$

Par composition des limites :

$$\lim_{y\to f(a)} \frac{f^{-1}(y)-f^{-1}(f(a))}{y-f(a)} = \lim_{x\to a} \frac{x-a}{f(x)-f(a)} = \frac{1}{f'(a)}$$

Donc

$$\lim_{y\to A} \frac{f^{-1}(y)-f^{-1}(A)}{y-A} = \frac{1}{f'(f^{-1}(A))}$$

□

2.3. Fonctions de classe $\mathscr{C}^k$

Définition - Dérivées successives en un point
Soit $f : I \to \mathbb{R}$. On définit par récurrence
• $f^{(0)} = f$
• pour $n \geqslant 1$, on dit que f est n fois dérivable en $a \in I$ s'il existe un intervalle $J \subset I$, J voisinage dans I de a, tel que f soit $n-1$ fois dérivable sur J et tel que $f^{(n-1)} : J \to \mathbb{R}$ soit dérivable en a.
On pose alors $\left(f^{(n-1)}\right)'(a) = f^{(n)}(a)$.
On note aussi $f^{(n)}(a) = D^n f(a) = \frac{\mathrm{d}^n f}{\mathrm{d}x^n}(a)$.

Attention - Voisinage de a
Notons que pour définir $f'(a)$, on a besoin d'un voisinage (a minima épontée) de a pour f.
De même pour définir $f^{(n)}(a)$, il faut un voisinage de a pour $f^{(n-1)}$ donc f dérivable $n-1$ fois sur plus qu'au seul point a.
On ne définit donc pas la n-dérivabilité en un point, mais bien sur un voisinage (a minima épointée).

Définition - Dérivées successives d'une fonction
On dit que f est n fois dérivable sur I si f est n fois dérivable en tout point de I.
L'application

$$\begin{cases} I \to \mathbb{R} \\ x \mapsto f^{(n)}(x) \end{cases}$$

est alors appelée dérivée n-ième de f et notée $f^{(n)}$ ou $D^n f$.

Exercice
Déterminer, pour $n \in \mathbb{N}$, $\sin^{(n)}$.

Correction
Par récurrence : $f^{(n)} = \begin{cases} (-1)^k \sin & \text{si } n = 2k \\ (-1)^k \cos & \text{si } n = 2k+1 \end{cases} = \sin(x + \frac{\pi}{2}n)$

Théorème - Théorème de Leibniz
Soient $f, g : I \to \mathbb{R}$ deux fonctions n fois dérivables en $a \in I$, alors fg est n fois dérivable en a et on a la formule :

$$(fg)^{(n)}(a) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(a) g^{(n-k)}(a).$$

Newton
proche de la
érences?

Exercice

Soit $h : x \mapsto (x^2+x+1)\sin 2x$. Calculer $h^{(n)}$ pour $n \in \mathbb{N}$.

Correction

On exploite le théorème de Leibniz.

$$h^{(2h)}(x) = (-1)^h\left((x^2+x+1)2^{2h}\sin(2x) - 2^h h(2x+1)(-1)^{h-1}\cos(2x) - h(2h-1)2^{h-1}\sin(2x)\right)$$

$$h^{(2h+1)}(x) = (-1)^h\left((x^2+x+1)2^{2h+1}\cos(2x) + 2^h(2h+1)(2x+1)\sin(2x) - h(2h+1)2^{h-1}\cos(2x)\right)$$

Démonstration

O peut le faire par récurrence par exemple.

On note $\mathscr{P}_n$: « si $f, g : I \to \mathbb{R}$ deux fonctions n fois dérivables en $a \in I$, alors $f \times g$ est n fois dérivable en a et : $(fg)^{(n)}(a) = \sum_{k=0}^{n}\binom{n}{k}f^{(k)}(a)g^{(n-k)}(a)$. »

— Pour $n = 0$, c'est assuré : $f^{(0)} = f$, $g^{(0)} = 0$, $(f\times g)^{(0)} = fg$ et $\binom{0}{0} = 1$.

— Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}_n$ est vraie.
Soient $f, g : I \to \mathbb{R}$ deux fonctions $n+1$ fois dérivables en $a \in I$.
Donc il existe J_1 et J_2 voisinages de a tel que f et g soient n fois dérivables sur J_1 et J_2 respectivement. Puis on considère $J = J_1 \cap J_2$.
Puis $f \times g$ est dérivable sur J et $(fg)' = f'g + fg'$.
Par hypothèse, f' est n fois dérivable en a, et g également.
Donc d'après $\mathscr{P}_n$, $f'g$ également.
De même, f est n fois dérivable en a, et g' également.
Donc d'après $\mathscr{P}_n$, fg' également.
Puis par addition, $(fg)'$ est n fois dérivable en a.
Ainsi fg est $n+1$ fois dérivable en a.
Il reste à calculer la dérivée $n+1$ en a. D'après $\mathscr{P}_n$:

$$\begin{aligned}
(fg)^{(n+1)}(a) &= \left((fg)'\right)^{(n)}(a) = (f'g+fg')^{(n)}(a)\\
&= \sum_{k=0}^{n}\binom{n}{k}(f')^{(k)}(a)g^{(n-k)}(a) + \sum_{k=0}^{n}\binom{n}{k}f^{(k)}(a)(g')^{(n-k)}(a)\\
&= \sum_{k=0}^{n}\binom{n}{k}f^{(k+1)}(a)g^{(n-k)}(a) + \sum_{k=0}^{n}\binom{n}{k}f^{(k)}(a)g^{(n-k+1)}(a)\\
&= \binom{n}{n}f^{(n+1)}(a)g^{(0)}(a) + \sum_{h=1}^{n}\binom{n}{h-1}f^{(h)}(a)g^{(n-h+1)}(a)\\
&\quad + \sum_{h=1}^{n}\binom{n}{k}f^{(h)}(a)g^{(n-h+1)}(a) + \binom{n}{0}f^{(0)}(a)g^{(n+1)}(a)\\
&= \binom{n+1}{n+1}f^{(n+1)}(a)g^{(0)}(a) + \sum_{h=1}^{n}\left(\binom{n}{h-1}+\binom{n}{h}\right)f^{(h)}(a)g^{(n-h+1)}(a) + \binom{n+1}{0}f^{(0)}(a)g^{(n+1)}(a)\\
&= \binom{n+1}{n+1}f^{(n+1)}(a)g^{(0)}(a) + \sum_{h=1}^{n}\binom{n+1}{h}f^{(h)}(a)g^{(n-h+1)}(a) + \binom{n+1}{0}f^{(0)}(a)g^{(n+1)}(a)\\
&= \sum_{h=0}^{n+1}\binom{n+1}{h}f^{(h)}(a)g^{(n-h+1)}(a)
\end{aligned}$$

Ainsi $\mathscr{P}_{n+1}$ est vérifiée.

La récurrence est donc bien établie. □

Corollaire - Composition n fois dérivable
Soient $\phi : I \to \mathbb{R}$, $f : J \to \mathbb{R}$ telles que $\phi(I) \subset J$, $a \in I$, $n \in \mathbb{N}^*$.
Si ϕ est n fois dérivable en a et f est n fois dérivable en $\phi(a)$,
alors $f \circ \phi$ est n fois dérivable en a.

Corollaire - Inverse n fois dérivable
Soient $f : I \to \mathbb{R}$, $a \in I$ tels que $f(a) \neq 0$ et f, n fois dérivable en a ($n \geqslant 1$).
Alors $\dfrac{1}{f}$ (définie sur un voisinage de a sur lequel f ne s'annule pas) est n fois dérivable en a.

Pour aller plus loin - La difficulté
La vraie difficulté qu'il faudra affronter, plus ou moins frontalement, lors de la démonstration. Quelle est l'expression de la dérivée n-ième d'une composition? Et d'une fonction réciproque?

Pourquoi est-ce bien des corollaires?

Démonstration

On raisonne par récurrence sur $n \in \mathbb{N}$, avec

$\mathscr{P}_n$: « $\forall\, \phi : I \to \mathbb{R}, f : J \to \mathbb{R}$ telles que $\phi(I) \subset J, a \in I$ et ϕ n fois dérivable en a, f n fois dérivable en $\phi(a)$, $f \circ \phi$ est n fois dérivable en a »

— Pour $n = 0$, le résultat est sans intérêt pour ce chapitre (continuité par composition)
— Pour $n = 1$, on a déjà montré le résultat.
— Supposons que le résultat soit vraie pour $n \in \mathbb{N}$. Soient ϕ est $n+1$ fois dérivable en a et f est $n+1$ fois dérivable en $\phi(a)$,
$f \circ \varphi$ est dérivable au voisinage V_a de a et pour tout $x \in V_a$, $(f\circ\varphi)'(x) = \varphi'(x) \times f'(\varphi(x))$.
Donc si ϕ est $n+1$ fois dérivable en a et f est $n+1$ fois dérivable en $\phi(a)$,
alors ϕ' est n fois dérivable en a et f' est n fois dérivable en $\phi(a)$.
On applique la proposition de récurrence à ϕ' et f'.
Donc d'après la formule de Leibniz, $(f\circ\varphi)' = \varphi' \times f'\circ\varphi$ est n fois dérivable en a.
Ainsi $f \circ \varphi$ est $n+1$ fois dérivable en a. Et $\mathscr{P}_{n+1}$ est vraie.

□

Démonstration

On note $H : x \mapsto \frac{1}{x}$.

Par récurrence, on montre facilement que :

$$\forall\, k \in \mathbb{N}\ H \text{ est derivable } k \text{ fois en tout } x \in \mathbb{R}* \text{ et } H^{(k)} : x \mapsto \frac{(-1)^k k!}{x^{k+1}}$$

(à faire, en exercice).

Puis par composition, $H \circ f$ est dérivable en tout $a \in \{x \in \mathbb{R} \mid f(x) \neq 0\}$ Par récurrence sur n pour une fonction f n fois dérivable en a :

— vrai pour $n = 1$
— supposé vrai pour un certain $n \geqslant 1$
au rang $n+1$: on sait que $\left(\frac{1}{f}\right)' = \frac{-f'}{f^2}$ avec f $n+1$ fois dérivable en a.
$-f'$ est donc n fois dérivable en a,
$\dfrac{1}{f^2}$ est n fois dérivable en a (en appliquant l'hypothèse de récurrence à la fonction f^2 qui est $n+1$ fois, donc n fois, dérivable en a)
donc d'après Leibniz $\left(\frac{1}{f}\right)' = \frac{-f'}{f^2}$ est n fois dérivable en a i.e. $\dfrac{1}{f}$ est $n+1$ fois dérivable en a.

□

Proposition - Réciproque n fois dérivable
Soit f continue, strictement monotone sur I. Soit $n \geqslant 1$. Si f est n fois dérivable sur I et si f' ne s'annule pas, alors f^{-1} est n fois dérivable sur $f(I)$.

Démonstration

On a déjà vu que f^{-1} est une fois dérivable et que $(f^{-1})' = \dfrac{1}{f'(f^{-1})}$.

Alors comme f' est dérivable $n-1$, et que $x \mapsto f'(f^{-1}(x))$ ne s'annule pas sur I,
alors $\dfrac{1}{f'} \circ f^{-1}$ est dérivable $n-1$ fois. □

Définition - Fonctions de classe $\mathscr{C}^n$
Soit $f : I \to \mathbb{R}$. On dit que f est de classe $\mathscr{C}^n$ (ou que f est n fois continûment dérivable) si

(i) f est n fois dérivable sur I
(ii) $f^{(n)}$ est continue sur I.

On dit que f est de classe $\mathscr{C}^\infty$ si elle est de classe $\mathscr{C}^n$ pour tout n. On note $\mathscr{C}^n(I,\mathbb{R})$ (resp. $\mathscr{C}^\infty(I,\mathbb{R})$) l'ensemble des applications de classe $\mathscr{C}^n$ (resp. $\mathscr{C}^\infty$) de I dans $\mathbb{R}$.

Remarque - Inclusion d'ensembles

• Si f est n fois dérivable sur I alors f est de classe $\mathscr{C}^{n-1}$.

• On a $\mathscr{C}^0(I) \supset \mathscr{C}^1(I) \supset \mathscr{C}^2(I) \supset \cdots \supset \mathscr{C}^{n-1}(I) \supset \mathscr{C}^n(I) \supset \cdots \supset \mathscr{C}^\infty(I)$

Donc $\bigcap_{i=h}^{k} \mathscr{C}^i(I) = \mathscr{C}^k(I)$ et $\bigcup_{i=h}^{k} \mathscr{C}^i(I) = \mathscr{C}^h(I)$.

D'après les résultats vus pour la dérivabilité en un point a, en prenant tout a de I :

Proposition - Opérations sur les fonctions de classe $\mathscr{C}^n$

Combinaison linéaire, produit, inverse, composée de fonctions de classe $\mathscr{C}^n$, fonction réciproque de f de classe $\mathscr{C}^n$ telle que f' ne s'annule pas sont de classe $\mathscr{C}^n$.

Nous avons précisé cela lors du chapitre 5 :

Proposition - Fonctions usuelles

Les fonctions polynomiales, les fonctions exp, ln, cos, sin, tan, arctan, sh, ch sont $\mathscr{C}^\infty$ sur leurs ensembles de définition.
Les fonctions $x \mapsto x^\alpha$, $\alpha \in \mathbb{R} \setminus \mathbb{N}$ sont $\mathscr{C}^\infty$ sur $]0, +\infty[$.
Les fonctions arcsin, arccos sont $\mathscr{C}^\infty$ sur $]-1, 1[$.

Exercice

Montrer que les solutions sur $\mathbb{R}$ de l'équation différentielle $(1+\sin^2 x)y'' + y' + e^{-5x}y = \operatorname{ch} x$ sont des fonctions de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$.

Correction

D'abord notons que l'équation peut se mettre sous forme normalisée sur $\mathbb{R}$ car $1+\sin^2 x \geqslant 1 > 0$.
On considère f une solution de E.
On montre par récurrence (sur $k \in \mathbb{N}$, $k \geqslant 2$) que f est de classe $\mathscr{C}^k$.
— f est de classe $\mathscr{C}^1$.
— f est de classe $\mathscr{C}^2$.
— si f est de classe $\mathscr{C}^n$ et $\mathscr{C}^{n+1}$.
Donc f et f' sont de classe $\mathscr{C}^n$.
Ainsi pour tout $x \in \mathbb{R}$, $f''(x) = \dfrac{\operatorname{ch} x - f'(x) - e^{-5x} f(x)}{1+\sin^2 x}$.
Et donc f'' est de classe $\mathscr{C}^n$, donc f de classe $\mathscr{C}^{n+2}$
f est de classe $\mathscr{C}^n$ pour tout $n \in \mathbb{N}$, donc de classe $\mathscr{C}^\infty$.

3. Etude globale des fonctions dérivables

3.1. Théorème de Rolle

Proposition - Annulation de la dérivée

Soient $f : I \to \mathbb{R}$ où I est un intervalle de $\mathbb{R}$, et $c \in I$, c n'étant pas une extrémité de I.
On suppose que f est dérivable en c et admet un maximum local en c.
Alors $f'(c) = 0$.

Remarque - Généralisation et vocabulaire

On observe qu'
— un point c tel que $f'(c) = 0$ s'appelle un point critique
— on a le même résultat pour un minimum local

Attention - Il s'agit d'une condition nécessaire, mais pas suffisante

$f'(c) = 0$ n'est pas une condition suffisante.
Le contre-exemple classique suivant le montre : $I = \mathbb{R}$, $x \mapsto x^3$ en 0.

Attention - La condition d'intérieur

La proposition est fausse pour c en une extrémité de I.. Le contre-exemple classique suivant le montre : $x \mapsto x+1$ sur $[-1, 1]$

Démonstration

On a donc pour tout $x < c$, $f(x) \leqslant f(c)$, donc $\dfrac{f(x)-f(c)}{x-c} \geqslant 0$.
et pour tout $x > c$, $f(x) \leqslant f(c)$, donc $\dfrac{f(x)-f(c)}{x-c} \leqslant 0$.
Or $f'(c)$ existe donc $\lim\limits_{x \to c^-} \dfrac{f(x)-f(c)}{x-c} = \lim\limits_{x \to c^+} \dfrac{f(x)-f(c)}{x-c}$.
Or la première limite est positive, le seconde négative. Par unicité : elles sont nulles et $f'(c) = 0$.
□

Histoire - Michel Rolle



Michel Rolle (1652-1719) est un mathématicien français à l'origine de la notation $\sqrt[n]{x}$

Théorème - Théorème de Rolle

Soit $f : [a, b] \to \mathbb{R}$ continue sur $[a, b]$, dérivable sur $]a, b[$. On suppose que $f(a) = f(b)$.
Alors il existe $c \in]a, b[$ tel que $f'(c) = 0$.

On va exploiter le théorème de Weierstrass, mais on ne peut pas le faire au bord. Il faut donc commencer par sortir du bord.

Démonstration

Ou bien f est constante, auquel cas pour tout $c \in]a, b[$, $f'(c) = 0$.
Ou bien f n'est pas constante, il existe donc $d \in]a, b[$ tel que $f(d) \neq f(a)$.
Si $f(d) > f(a)$.
La fonction f est continue sur $[a, b]$,
d'après le théorème de Weierstrass elle admet un maximum.
Celui-ci est plus grand que $f(d)$, donc il ne peut être atteint aux extrémités de $[a, b]$.
Il existe donc $c = \max f$, avec $c \neq a, b$. D'après la proposition précédente : $f'(c) = 0$.
Si $f(d) < f(a)$.
La fonction f est continue sur $[a, b]$,
d'après le théorème de Weierstrass elle admet un minimum.
Celui-ci est plus petit que $f(d)$, donc il ne peut être atteint aux extrémités de $[a, b]$.
Il existe donc $c = \min f$, avec $c \neq a, b$. D'après la proposition précédente : $f'(c) = 0$.
□

La même démonstration s'adapte tout à fait, au cas où $b = \infty$, mais dans ce cas, il faut prendre un B tel que $\forall\ x > B$, $|f(x) - f(a)| < |f(d) - f(a)|$:

Proposition - Généralisation du théorème de Rolle

Soit $f : [a, +\infty[\to \mathbb{R}$, continue sur $[a, +\infty[$, dérivable sur $]a, +\infty[$ telle que $f(a) = \lim\limits_{x \to +\infty} f(x)$.
Alors il existe $c \in]a, +\infty[$ tel que $f'(c) = 0$.

Exercice

Faire la démonstration

Correction

Ou bien f est constante, auquel cas pour tout $c \in]a, +\infty[$, $f'(c) = 0$.
Ou bien f n'est pas constante, il existe donc $d \in]a, b[$ tel que $f(d) \neq f(a)$.
Si $f(d) > f(a)$.
Comme $\lim\limits_{+\infty} f = f(a)$, il existe D tel que $\forall\ x \in [D, +\infty[$, $|f(x) - f(a)| < \epsilon := \frac{f(d)-f(a)}{2}$.
La fonction f est continue sur $[a, D]$,
d'après le théorème de Weierstrass elle admet un maximum.
Celui-ci est plus grand que $f(d)$, donc il ne peut être atteint aux extrémités en a ou D.
Il existe donc $c = \max f$, avec $c \neq a, D$. D'après la proposition précédente : $f'(c) = 0$.
Si $f(d) < f(a)$.
Comme $\lim\limits_{+\infty} f = f(a)$, il existe D tel que $\forall\ x \in [D, +\infty[$, $|f(x) - f(a)| < \epsilon := \frac{f(a)-f(d)}{2}$.
La fonction f est continue sur $[a, D]$,
d'après le théorème de Weierstrass elle admet un minimum.
Celui-ci est plus petit que $f(d)$, donc il ne peut être atteint aux extrémités en a ou D.
Il existe donc $c = \min f$, avec $c \neq a, b$. D'après la proposition précédente : $f'(c) = 0$.

Savoir faire - Les racines imbriquées

Bien souvent on applique le théorème de Rolle avec f continue sur $[a,b]$, dérivable sur $]a,b[$, $f(a)=f(b)=0$, on obtient alors la version suivante :
Entre deux zéros de f il y a un zéro de f'.

Exercice

Montrer la formule de Taylor-Lagrange :

Si $f\in\mathscr{C}^n([a,b])$ et $n+1$ fois dérivable, il existe $c\in]a,b[$ telle que

$$f(b)=\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(b-a)^k+\frac{f^{(n+1)}(c)}{(n+1)!}(b-a)^{n+1}$$

Correction

On considère $\varphi : t\mapsto f(b)-\sum_{k=0}^{n}\frac{f^{(k)}(t)}{k!}(b-t)^k-\frac{M}{(n+1)!}(b-t)^{n+1}$ de tel sorte que $\varphi(a)=0$.

Cela est possible, il suffit de prendre $M=\frac{(n+1)!}{(b-a)^{n+1}}\left(f(b)-\sum_{k=0}^{n}\frac{f^{(k)}(a)}{n!}(b-a)^n\right)$.

Notons que l'on a également $\varphi(b)=0$, on applique le théorème de Rolle :

$$\exists\, c\in]a,b[\text{ tel que } \varphi'(c)=0$$

Or

$$\varphi'(t)=-f'(t)-\sum_{k=1}^{n}\left(\frac{f^{k+1}(t)}{k!}(b-t)^k-\frac{f^k(t)}{(k-1)!}(b-t)^{k-1}\right)+\frac{M}{n!}(b-t)^n$$

Il apparait un télescopage :

$$\varphi'(t)=\frac{1}{n!}\left(M-f^{n+1}(t)\right)(b-t)^n$$

On a donc $f^{n+1}(c)=M$. La formule de Taylor-Lagrange est montrée

On prend $x=b$, il existe $c\in[a,x]$ (le résultat reste vrai si $a>b$) tel que $M=f^{n+1}(c)$ Avec $\epsilon : x\mapsto\frac{f^{n+1}(c)}{n+1}(x-a)$

Savoir faire - Quelle fonction φ choisir pour bien appliquer le théorème de Rolle?

De manière générale, on prend $\varphi=f-P$, où P est un polynôme bien choisi.

Mais il y a deux types de questions :

— Ou bien le point c à trouver est associé à une série de derivées de f, en un même point.
C'est le cas ici pour la formule de Taylor : $f^{(k)}(a)$.
On considère alors $P=\sum_{k=0}^{d}\frac{f^{(k)}(t)}{k!}(t-\alpha)$ (α bien choisi).
(C'est la base polynomiale de l'interpolation de Taylor, en fonction des dérivées). Au besoin on ajoute une constante multiplicative pour amorcer le théorème de Rolle (deux racines).

— Ou bien le point c à trouver est associé à une série de valeurs de f, en des points distincts : $x_1,\dots x_n$.
On considère alors $P=\sum_{k=0}^{d}f(x_k)\prod_{i\neq k}\frac{t-i}{k-i}$.
(C'est la base polynomiale de l'interpolation de Lagrange)

On annule et on dérive. On peut avoir à appliquer plusieurs fois le théorème de Rolle.

Pour aller plus loin - Formules de Taylor

Les formules de Taylor (sous toutes leurs formes) seront essentielles pour déterminer les développements limités des fonctions usuelles, lors du prochain chapitre… et en cours de physique

3.2. Egalité des accroissements finis

Enoncé

Théorème - Théorème (ou formule, ou égalité) des accroissements finis (A.F.)

Soit $f:[a,b]\to\mathbb{R}$ continue sur $[a,b]$, dérivable sur $]a,b[$. Alors il existe $c\in]a,b[$ tel que

$$f(b)-f(a)=(b-a)f'(c).$$

Il s'agit du cas $n=0$ pour la formule de Taylor-Lagrange vue plus haut.

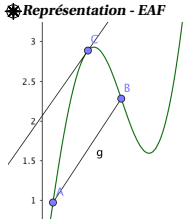
Remarque - Graphiquement

Il existe au moins un point de la courbe $\mathscr{C}_f$ d'abscisse dans $]a,b[$ en lequel la tangente à la courbe est parallèle à la droite (AB) où $A(a,f(a))$ et $B(b,f(b))$.

Démonstration

Considérons $\varphi : t\mapsto(b-a)f(t)-(f(b)-f(a))t$.
Alors $\varphi(a)=(b-a)f(a)-(f(b)-f(a))a=bf(a)-af(b)$ et $\varphi(b)=(b-a)f(b)-(f(b)-f(a))b=bf(a)-af(b)=\varphi(a)$.
Puis φ est dérivable (addition de fonction dérivable). On peut lui appliquer le théorème de Rolle.
Ainsi, il existe c tel que $0=\varphi'(c)=(b-a)f'(c)-(f(b)-f(a))$. □

Représentation - EAF



Application aux variations d'une fonction

Théorème - CNS de Variations de f

I désigne un intervalle. Soit $f:I\to\mathbb{R}$ continue sur I, dérivable sur $\mathring{I}$ (I privé de ses éventuelles bornes). Alors

— f est constante sur I si et seulement si $\forall x\in\mathring{I}$, $f'(x)=0$,
— f est croissante sur I si et seulement si $\forall x\in\mathring{I}$, $f'(x)\geqslant 0$,
— f est décroissante sur I si et seulement si $\forall x\in\mathring{I}$, $f'(x)\leqslant 0$.

Pour aller plus loin - Condition encore plus large de stricte monotonie

Soit $f:I\to\mathbb{R}$ continue sur I, dérivable sur $\mathring{I}$.
Si f' est de signe constant et ne s'annule qu'en des points isolés, alors f est strictement monotone sur I.
Avec la définition :
Un point d'annulation x_0 de f' est dit isolé s'il existe un intervalle de la forme $]x_0-\epsilon,x_0+\epsilon[$, avec $\epsilon>0$, ne contenant aucun autre point d'annulation de f' que x_0.)

Démonstration

Supposons que f est croissante sur I,
alors pour tout $x\in\mathring{I}$, il existe $\epsilon>0$ tel que $[x-\epsilon,x+\epsilon]\subset I$.
et $\forall\, y\in[x-\epsilon,x+\epsilon]$, $f(y)\leqslant f(x)$ ssi $y\leqslant x$.
Donc $f'(x)=\lim_{y\to x}\frac{f(y)-f(x)}{y-x}\geqslant 0$ (elle existe bien par hypothèse).
Supposons que $\forall\, x\in\mathring{I}$, $f'(x)\geqslant 0$.
Soit $a\leqslant b\in I$. D'après l' EAF, il existe c tel que $f(b)-f(a)=f'(c)(b-a)$.
Or $f'(c)\geqslant 0$ et $b-a\geqslant 0$, donc $f(b)-f(a)\geqslant 0$.
Par conséquent f est croissante sur I.
Raisonnement comparable pour f est décroissante sur I si et seulement si $\forall x\in\mathring{I}$, $f'(x)\leqslant 0$.
Enfin, on a

$$f \text{ constante} \Leftrightarrow f \text{ croissante et décroissante} \Leftrightarrow \forall\, x\in\mathring{I}, f'(x)\geqslant 0 \text{ et } f'(x)\leqslant 0 \Leftrightarrow f'(x)=0$$

□

Dans le cas de la seconde implication, avec que des inégalités strictes :

Proposition - Stricte monotonie (C.S)

Soit $f:I\to\mathbb{R}$ continue sur I, dérivable sur $\mathring{I}$, alors

$$\forall x\in\mathring{I}, f'(x)>0\Rightarrow f \text{ est strictement croissante sur } I.$$

Attention - La réciproque est fausse

$f:x\mapsto x^3$ est strictement croissante sur $]-1,1[$.
Et pourtant $f'(0)=0$, avec $0\in]-1,1[$

Exercice
En appliquant le théorème énoncé dans la marge, montrer que si $f : I \to \mathbb{R}$ est continue sur I, dérivable sur $\mathring{I}$ et si f' est de signe constant et ne s'annule qu'en un nombre fini de points, alors f est strictement monotone sur I.

Correction
Si f s'annule en un nombre fini n de points, on peut noter ces points $(x_i)_{i\in\mathbb{N}_n}$ avec $x_i < x_{i+1}$.
Alors pour tout $i \in \mathbb{N}_n$, avec $\epsilon_i = \frac{1}{2}\min(x_{i+1}-x_i, x_i - x_{i-1})$, on a $]x_i-\epsilon, x_i+\epsilon[$ qui ne contient aucun autre point d'annulation que x_i.

3.3. Inégalité des accroissements finis

Théorème - Inégalités des accroissements finis
Soit $f : [a,b] \to \mathbb{R}$, continue sur $[a,b]$, dérivable sur $]a,b[$.
Si $\forall x \in]a,b[$, $m \leqslant f'(x) \leqslant M$ alors

$$m(b-a) \leqslant f(b) - f(a) \leqslant M(b-a).$$

Il en découle le corollaire suivant ainsi que la définition des fonctions lipschiztienne :

Corollaire - f bornée et fonction lipschitzienne
Soit $f : I \to \mathbb{R}$ dérivable sur l'intervalle I. S'il existe $K \geqslant 0$ tel que $\forall x \in I, |f'(x)| \leqslant K$ alors f est K**-lipschitzienne sur** I c'est-à-dire que

$$\forall (x_1,x_2) \in I^2, |f(x_2) - f(x_1)| \leqslant K|x_2 - x_1|.$$

Remarque - Réciproque du corollaire
Réciproquement, si f est dérivable sur I et K-lipschitzienne sur I, alors nécessairement $|f'| \leqslant K$.

Savoir faire - Contrôler f' pour contrôler f
Si l'on cherche à maîtriser f, alors il suffit de maitrise f' et d'intégrer la relation.
Le contrôle réciproque ne marche pas (ce n'est pas parce qu'on connait f qu'on connaît f').
On a déjà vu ce résultat dans le cours sur les primitives et dans le cours sur les équations différentielles

Exercice
Démontrer l'affirmation faite dans cette remarque

Correction
Soit $x \in I$. Alors $\forall t \in I, t \neq x$, $\left|\frac{f(x)-f(t)}{x-t}\right| \leqslant K$ car f est K-lipschitzienne. Comme f est supposée dérivable sur I, on peut passer à la limite quand $t \to x$ et on trouve $|f'(x)| \leqslant K$.

Démonstration
La démonstration de l'IAF découle directement de l'égalité des accroissements finis.
Il existe $c \in [a,b] =]a,b[$ tel que $f'(c)(b-a) = f(b) - f(a)$.
Or $m \leqslant f'(c) \leqslant M \ldots \square$

Remarque - Interprétation autoroutière
Une voiture qui roule sur autoroute entre 100 et 130 km/h (conducteur non débutant !), parcourt en une demi-heure une distance comprise entre 50 et 65 km, en une heure une distance comprise entre 100 et 130 km...au delà de deux heures, elle s'arrête (prévention routière !)

Exercice
Une fonction à dérivée bornée est uniformément continue

Correction
On applique l'IAF. Et on a même mieux : f est K-lipscitzienne donc uniformément continue.

Représentation - Interprétation graphique
Si I est un intervalle tel que $\forall x \in I$, $m \leqslant f'(x) \leqslant M$ et $a \in I$, alors la courbe représentative de f se trouve entre les droites d'équations $y = f(a) + m(x-a)$ et $y = f(a) + M(x-a)$.

Savoir faire - Application à l'étude des suites $u_{n+1} = f(u_n)$
Cette méthode s'applique à toute suite (u_n) définie par $u_0 \in I$, $u_{n+1} = f(u_n)$ telle que
- I est un intervalle fermé stable par f
- f est dérivable et il existe $k \in]0,1[$ tel que $\forall x \in I, |f'(x)| \leqslant k$
- il existe $\ell \in I$ tel que $f(\ell) = \ell$

Dans ce cas, pour tout $n > 0$,

$$|u_n - \ell| \leqslant k|u_{n-1} - \ell| \leqslant k^n |u_0 - \ell|$$

(par récurrence géométrique). Et donc, par le théorème d'encadrement : $(u_n) \to \ell$

Exercice
On considère la suite définie par $u_0 \geqslant 0$ et $\forall n \in \mathbb{N}$, $u_{n+1} = \sqrt{2+u_n}$. Donner une majoration de $|u_{n+1}-2|$ en fonction de $|u_n - 2|$ puis une majoration de $|u_n - 2|$ en fonction de $|u_0 - 2|$ et n. En déduire que (u_n) est convergente.

Correction
Ici on note $f : x \mapsto \sqrt{2+x}$, on a donc pour tout $n \in \mathbb{N}$, $u_{n+1} = f(u_n)$
On remarque que si ℓ est point fixe de f, alors $\ell = \sqrt{2+\ell}$, donc $\ell^2 = 2+\ell$, ie $\ell = 2$ ou $\ell = -1$.
C'est pourquoi on étudie $u_{n+1} - 2$:

$$|u_{n+1} - 2| = |f(u_n) - f(2)| \leqslant K|u_n - 2| \leqslant K^{n+1}|u_0 - 2|$$

où K est obtenu par l'inégalité des accroissements finis...
Ici $|f'(x)| = |\frac{1}{2\sqrt{2+x}}| \leqslant \frac{1}{2\sqrt{2}} = K$ $(x > 0)$.
Enfin, comme $K < 1$, $\lim(K^{n+1}|u_0 - 2|) = 0$ et donc par encadrement : $(u_n) \to 2$

Exercice
Etudier la suite définie par $u_0 \in \mathbb{R}$ et $\forall n \in \mathbb{N}$, $u_{n+1} = 2 + \frac{1}{2}\sin u_n$.

Correction
Même chose avec $g : x \mapsto 2 + \frac{1}{2}\sin x$.
g est dérivable sur $\mathbb{R}$, $g'(x) = \frac{1}{2}\cos x$ donc $|g(x)| \leqslant \frac{1}{2}$.
ℓ, point fixe de g : $g(\ell) = \ell \longleftrightarrow \varphi(\ell) = 0$ avec $\varphi : x \mapsto g(x) - x$ Or $\varphi(0) = 2 > 0$, $\varphi(\pi) = 2 - \pi < 0$ et $\varphi'(x) = g'(x) - 1 \leqslant -\frac{1}{2} < 0$.
Donc φ est strictement décroissante sur $\mathbb{R}$, avec le TVI, elle admet une unique racine comprise entre 0 et π.
On a ensuite, pour $n > 0$,

$$|u_n - \ell| = |f(u_{n-1}) - f(\ell)| \leqslant \frac{1}{2}|u_{n-1} - \ell| \leqslant \frac{1}{2^n}|u_0 - \ell|$$

Donc (u_n) converge vers ℓ, unique solution du problème $x = 2 + \frac{1}{2}\sin x$ (elle est comprise entre 0 et π)

3.4. Prolongement dérivable ou limite de la dérivée

Théorème - Limite de la dérivée
Soit $f : [a,b] \to \mathbb{R}$ continue sur $[a,b]$, dérivable sur $]a,b]$.
On suppose que f' admet une limite finie ℓ en a.
Alors $\lim_{x\to a} \frac{f(x)-f(a)}{x-a} = \ell$, c'est-à-dire que f est dérivable en a et f' est continue en a $(f'(a) = \ell)$.

Corollaire - Limite de la dérivée (au coeur de l'intervalle)
Si $f : I \to \mathbb{R}$ est continue sur I, dérivable sur les deux intervalles constituant $I \setminus \{a\}$ et si f' admet une limite ℓ en a, alors f est dérivable en a et f' est continue en a $(f'(a) = \ell)$.

Démonstration
Soit $x > a$. D'après l'égalité des accroissements finis :

$$\exists\, c_x \in]a,x[\qquad f(x)-f(a) = f'(c_x)(x-a) \Longrightarrow \frac{f(x)-f(a)}{x-a} = f'(c_x)$$

On sait que f' admet une limite finie ℓ en a.
Soit $\epsilon > 0$, il existe $\eta > 0$ tel que $\forall\, x \in]a, a+\eta[$, $|f'(x)-\ell| < \epsilon$.
On a donc pour tout $x \in]a, a+\eta[$, $c_x \in]a, x[\subset]a, a+\eta[$, donc $|f'(c_x)-\ell| = \left|\dfrac{f(x)-f(a)}{x-a} - \ell\right| < \epsilon$.
C'est exactement la définition du fait que f est dérivable en a et $f'(a) = \ell$.
Evidemment, on a alors également $f'(a) = \ell = \lim\limits_{x\to a} f'(x)$, donc f' continue en a.
Pour le corollaire, on se place sur $[c, a[$ et sur $]a, b]$, puis on prolonge chacun des intervalles.
Et enfin on les recolle. □

Proposition - Limite de la dérivée infinie
Soit $f : [a,b] \to \mathbb{R}$, continue sur $[a,b]$, dérivable sur $]a,b]$. On suppose que $\lim\limits_{x\to a} f'(x) = +\infty$ (resp $-\infty$).
Alors $\lim\limits_{x\to a} \dfrac{f(x)-f(a)}{x-a} = +\infty$ (resp. $-\infty$), c'est-à-dire que f n'est pas dérivable en a mais que $\mathscr{C}_f$ admet une demi-tangente verticale en a.

Démonstration
On adapte la démonstration précédente à ce cas : Soit $x > a$. D'après l'égalité des accroissements finis :

$$\exists\, c_x \in]a,x[\qquad f(x)-f(a) = f'(c_x)(x-a) \Longrightarrow \frac{f(x)-f(a)}{x-a} = f'(c_x)$$

On sait que f' admet une limite infinie en a.
Soit $A > 0$, il existe $\eta > 0$ tel que $\forall\, x \in]a, a+\eta[$, $f'(x) > A$.
On a donc pour tout $x \in]a, a+\eta[$, $c_x \in]a, x[\subset]a, a+\eta[$, donc $f'(c_x) = \dfrac{f(x)-f(a)}{x-a} > A$.
C'est exactement la définition du fait que $\lim\limits_{x\to a} \frac{f(x)-f(a)}{x-a} = +\infty$.
□

Le théorème suivant est en fait un corollaire du premier théorème avec l'hypothèse supplémentaire que f' est continue sur $I \setminus \{a\}$.

Théorème - Théorème de classe $\mathscr{C}^1$ par prolongement
Soit $f : I \to \mathbb{R}$ continue sur I, de classe $\mathscr{C}^1$ sur $I \setminus \{a\}$. On suppose que f' admet une limite finie ℓ en a. Alors f est de classe $\mathscr{C}^1$ sur I et $f'(a) = \ell$.

Remarque - Force du théorème
Ce théorème remplace les **deux** calculs (a priori) de :
- $\lim\limits_{x\to a} \frac{f(x)-f(a)}{x-a}$ (pour la dérivabilité en a ou existence de $f\prime(a)$)
- et $\lim\limits_{x\to a} f'(x)$ (pour la continuité en a de $x \mapsto f'(x)$)

par uniquement celui de $\lim\limits_{x\to a} f'(x)$.

Exemple - Applications
Ce théorème s'applique fréquemment dans les deux situations suivantes :
- Lorsque f n'est pas définie en un point, mais peut se prolonger (dans un premier temps).
  Il faut voir alors si ce prolongement de f a pour conséquence un prolongement de f' (dans un second temps).
  Voir exercice plus bas.
- Dans le cadre de recollement d'équations différentielles en un point frontière (où l'équation n'est pas normalisée), on a besoin de voir les prolongements par continuité de classe $\mathscr{C}^1$…
  Avec ce théorème, la méthode sera souvent plus facile

On généralise par récurrence aux fonctions de classe $\mathscr{C}^k$

Théorème - Théorème de classe $\mathscr{C}^k$ par prolongement
Soit $f : I \setminus \{a\} \to \mathbb{R}$ de classe $\mathscr{C}^k$ sur $I \setminus \{a\}$. On suppose que pour tout $i \in \{0,1,\dots,k\}$ $f^{(i)}$ admet une limite finie ℓ_i en a. Alors f admet un prolongement de classe $\mathscr{C}^k$ sur I et pour tout $i \in \{0,1,\dots,k\}$ $f^{(i)}(a) = \ell_i$.

Pour aller plus loin - Calcul
Par récurrence : $P_0 = 1$ et $P_{n+1}(u) = -u^2(P_n(u) + P_n'(u))$

Exemple - Fonction $f : x \mapsto \begin{cases} e^{-1/x} & \textbf{si } x > 0 \\ 0 & \textbf{sinon} \end{cases}$
Par composition, $f_{|]0,+\infty[}$ et $f_{|\mathbb{R}_-}$ sont de classe $\mathscr{C}^\infty$.
Par récurrence, on montre que pour tout $n \in \mathbb{N}$, il existe P_n, polynôme de degré $2n$ tel que pour tout $x > 0$,

$$f^{(n)}(x) = P_n\left(\frac{1}{x}\right) e^{-1/x} \underset{x\to 0^+}{\longrightarrow} 0$$

Donc f est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$ entier.

Exercice
Soit

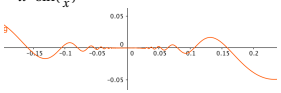
$$f : \begin{array}{l} [0,1] \to \mathbb{R} \\ x \mapsto \begin{cases} x^2 \sin\frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \end{array}$$

1. Montrer que f est continue sur $[0,1]$.
2. f' a-t-elle une limite en 0 ?
3. f est-elle dérivable sur $[0,1]$? de classe $\mathscr{C}^1$ sur $[0,1]$?
4. Que peut-on en conclure pour les théorèmes précédents ?

Correction

1. Pour tout $x \neq 0$, $|\sin(\frac{1}{x})| \leqslant 1$, donc $|f(x)| \leqslant x^2$.
   Par encadrement, f admet une limite en 0 égale à $f(0)$, donc f est continue en 0.
   Elle est par ailleurs (composition et produit) continue sur $]0,1]$.
2. f est dérivable sur $]0,1]$ et pour $x \neq 0$, $f'(x) = 2x\sin\frac{1}{x} - \cos\frac{1}{x}$.
   Cette fonction n'admet pas de limite en 0.
   En effet, on a pour tout $n \in \mathbb{N}$, $f(\frac{1}{n\pi}) = -1$ et $f(\frac{1}{n\pi+\pi/2}) = \frac{2}{n\pi+\pi/2} \underset{n\to\infty}{\longrightarrow} 0$.
3. On démontre que f est dérivable sur $]0,1]$ (comme pour la continuité).
   Enfin
   $$\left|\frac{f(x)-f(0)}{x-0}\right| = \left|x\sin\frac{1}{x}\right| \leqslant |x|$$
   Et donc par encadrement, f est dérivable en 0 et $f'(0) = 0$. f' ne peut pas être continue en 0, donc f n'est pas de classe $\mathscr{C}^1$ sur $[0,1]$
4. Cela nous montre qu'il n'y a pas d'équivalence entre le limite de la fonction dérivée et la dérivé en un point, mais bien uniquement une implication. Cela prouve aussi qu'« être de classe $\mathscr{C}^1$ » est plus que d'« être dérivable ».

Représentation - Representation de $x \mapsto x^2\sin(\frac{1}{x})$



Savoir faire - Exploiter le théorème de la limite de la dérivée
Ici, il est surtout important de montrer au correcteur que l'on écrit pas n'importe quoi.
- Par exemple, ce n'est pas la dérivée qui est prolongée.
- Savoir si une fonction est dérivable en un point, ne consiste pas a priori, à savoir si la dérivée admet une limite en ce point.

Cette dernière observation ($\lim_{x_0} f'$) s'étudie comme conséquence d'un super théorème!
Pour être assuré que le correcteur a bien compris qu'on exploite ce théorème, on rappelle avec insistance les hypothèses à vérifier pour appliquer le théorème (continuité de f…).
Si on doit le démontrer pour les dérivées de tous les ordres, on fait une récurrence, avec un contrôle pour s'assurer le passage à la limite.

Exercice

Pour $x \neq 0$, on pose $f(x) = \dfrac{\sin x^2}{x}$. Montrer que f se prolonge sur $\mathbb{R}$ en une fonction de classe $\mathscr{C}^1$.

Correction

On sait que pour tout $y \in \mathbb{R}$, $|\sin(y)| \leqslant |y|$, donc $|f(x)| \leqslant \left|\dfrac{x^2}{x}\right| = |x|$.

Par le théorème d'encadrement : $\lim\limits_0 f = 0$.

On peut donc prolonger f en posant $f(0) = 0$.

f est de classe $\mathscr{C}^1$ sur $\mathbb{R}^*$ et pour tout $x \neq 0$, $f'(x) = \dfrac{2x^2\cos(x^2) - \sin(x^2)}{x^2} = \cos(x^2) - \dfrac{\sin(x^2)}{x^2}$.

Par addition (et en exploitant $\lim\limits_y \dfrac{\sin(y)}{y} = 1$), on $\lim\limits_0 f' = 1 - 1 = 0$.

Donc le prolongement de f donne une fonction de classe $\mathscr{C}^1$ sur $\mathbb{R}$.

3.5. Prolongement de la règle de l'Hospital

Analyse - Cas $\frac{f'(a)}{g'(a)}$ indéterminé

On a vu en début d'année : si $f(x) - f(a) = (x-a)(f'(a) + \epsilon_1(x))$ et $g(x) - g(a) = (x-a)(g'(a) + \epsilon_2(x))$, avec ϵ_1 et ϵ_2 continue et nulle en 0,

alors si $\dfrac{f'(a)}{g'(a)}$ n'est pas indéterminée :

$$\lim_{x\to a} \frac{f(x)-f(a)}{g(x)-g(a)} = \lim_{x\to a} \frac{f'(a)+\epsilon_1(x)}{g'(a)+\epsilon_2(x)} = \frac{f'(a)}{g'(a)}$$

Mais que se passe-t-il si $\dfrac{f'(a)}{g'(a)}$ est indéterminée?

Proposition - Prolongement de la règle de l'Hospital
Soit $a \in I$, f et g dérivable sur $I \setminus \{a\}$.
Si $\dfrac{f'}{g'}$ admet une limite en a et $g' \neq 0$ sur un voisinage épointé de a.
Alors $x \mapsto \dfrac{f(x)-f(a)}{g(x)-g(a)}$ admet une limite en a égale à $\lim\limits_a \dfrac{f'}{g'}$.

Démonstration
Soit $x \in I \setminus \{a\}$.
Considérons $h : t \mapsto f(t)(g(x)-g(a)) - g(t)(f(x)-f(a))$.
alors h est dérivable sur $I \setminus \{a\}$, de dérivée $h'(t) = f'(t)(g(x)-g(a)) - g'(t)(f(x)-f(a))$.
Puis $h(a) = h(x) = f(a)g(x) - g(a)f(x)$. D'après le théorème de Rolle :
il existe $c_x \in]a,x[$ (ou $]x,a[$) tel que $h'(c_x) = 0$ i.e. $f'(c_x)(g(x)-g(a)) = g'(c_x)(f(x)-f(a))$
Ainsi pour tout $x \in I \setminus \{a\}$, suffisamment proche de a, il existe c_x tel que $\dfrac{f(x)-f(a)}{g(x)-g(a)} = \dfrac{f'(c_x)}{g'(c_x)} \xrightarrow[x\to a]{} \lim\limits_a \dfrac{f'}{g'}$. □

Un petit d'exercice d'application qui donne un savoir-faire et reprend un résultat du DM2.

Exercice

Calculer $\lim\limits_{x\to 0} \dfrac{\sin x - x + \frac{1}{6}x^3}{x^4}$

Correction

On note $f : x \mapsto \sin x - x + \frac{1}{6}x^3$ et $g : x \mapsto x^4$.
Ces fonctions sont dérivables 4 fois sur $\mathbb{R}$ et pour tout $x \in \mathbb{R}$,

$$f^{(1)}(x) = \cos x - 1 + \frac{1}{2}x^2,\ f^{(2)}(x) = -\sin x + x,\ f^{(3)}(x) = -\cos x + 1,\ f^{(4)}(x) = \sin x$$

$$g^{(1)}(x) = 4x^3,\ g(2)(x) = 12x^2,\ g^{(3)}(x) = 24x,\ g^{(4)}(x) = 24$$

On remonte les indéterminations.
Comme $\dfrac{f^{(4)}(x)}{g^{(4)}(x)} \to 0$, alors $\dfrac{f^{(3)}(x)}{g^{(3)}(x)} \to 0$ puis $\dfrac{f^{(2)}(x)}{g^{(2)}(x)} \to 0$, et $\dfrac{f^{(1)}(x)}{g^{(1)}(x)} \to 0$ et enfin $\dfrac{f(x)}{g(x)} \to 0$.

4. Généralisation aux fonctions à valeurs complexes

I désigne un intervalle de $\mathbb{R}$ non réduit à un point.

4.1. Définitions

Définition - Taux de variations ou parties réelle et imaginaire
Soit $f \in \mathscr{F}(I,\mathbb{C})$, $a \in I$. On définit la fonction τ_a sur $I \setminus \{a\}$ par

$$\tau_a(x) = \frac{f(x)-f(a)}{x-a}.$$

Il y a équivalence entre les deux propriétés suivantes :

- τ_a possède une limite en a (limite dans $\mathbb{C}$).
- $\mathrm{Re}f$ et $\mathrm{Im}f$ (fonctions à valeurs réelles) sont dérivables en a.

On dit alors que f est dérivable en a. On note $f'(a) = Df(a) = \dfrac{df}{dx}(a)$ cette limite.
On a $f'(a) = (\mathrm{Re}f)'(a) + i(\mathrm{Im}f)'(a)$.

Remarque - Démonstration?
Il faudrait démontrer l'équivalence entre les deux propriétés.
Cela découle simplement de

$$\tau_a(x) = \frac{\mathrm{Re}f(x) - \mathrm{Re}f(a)}{x-a} + i\frac{\mathrm{Im}f(x) - \mathrm{Im}f(a)}{x-a}$$

Puis on prend les limites

Proposition - Dérivabilité ⇒ Continuité (en un point)
Si $f \in \mathscr{F}(I,\mathbb{C})$ est dérivable en a, alors elle est continue en a.

Démonstration
Même démonstration que pour le cas réelle : pour être dérivable, il faut que le numérateur s'annule. □

Proposition - Dérivabilité ⇒ Continuité (sur un intervalle)
f est dite dérivable sur I si elle est dérivable en tout point de I. Dans ce cas elle est continue sur I.

Définition - Dérivations successives
On définit les dérivées successives de la même manière que pour les fonctions à valeurs dans $\mathbb{R}$.
On dit qu'une fonction est de classe $\mathscr{C}^n$ sur I si elle est n fois dérivable sur I et si sa dérivée n-ième est continue sur I.
On dit qu'elle est de classe $\mathscr{C}^\infty$ si elle est de classe $\mathscr{C}^n$ pour tout n (soit si elle est dérivable à n'importe quel ordre).
On note $\mathscr{C}^n(I,\mathbb{C})$ (resp. $\mathscr{C}^\infty(I,\mathbb{C})$) l'ensemble des fonctions de classe $\mathscr{C}^n$ (resp. $\mathscr{C}^\infty$) sur I.

4.2. Opérations

Les propositions qui suivent se démontrent aisément en prenant les parties réelles et imaginaires de chaque fonction et en appliquant alors les résultats pour les fonctions à valeurs réelles…

Proposition - Stabilité
Soient $f,g\in\mathscr{F}(I,\mathbb{C})$ dérivables en a et $(\lambda,\mu)\in\mathbb{C}^2$ alors
• $\lambda f+\mu g$, fg, $\dfrac{f}{g}$ (si g ne s'annule pas en a) sont dérivables en a, les formules donnant les dérivées étant les mêmes que pour les fonctions à valeurs dans $\mathbb{R}$.
• Si $\phi\in\mathscr{F}(J,\mathbb{R})$ dérivable en $f(a)$ et $f(I)\subset J$, alors $\phi\circ f$ est dérivable en a et
$$(\phi\circ f)'(a)=f'(a)\times\phi'(f(a))$$
• $\overline{f}$ est dérivable en a et $(\overline{f})'(a)=\overline{f'(a)}$.
• L'exponentielle complexe de f ($e^f:x\mapsto e^{f(x)}=e^{\mathrm{Re}f(x)}(\cos(\mathrm{Im}f(x))+i\sin(\mathrm{Im}f(x)))$ est dérivable en a et $(e^f)'(a)=f'(a)e^{f(a)}$.

Plus généralement encore :

Proposition - Stabilité
On a donc que si $f,g\in\mathscr{F}(I,\mathbb{C})$ sont dérivables sur I, ϕ dérivable sur J, alors $\lambda f+\mu g$, fg, $\dfrac{f}{g}$ (si g ne s'annule pas sur I), $f\circ\phi$, $\overline{f}$, e^f sont dérivables sur I avec les formules usuelles de dérivation.

Proposition - Généralisation au dérivée n-ièmes
• $f\in\mathscr{F}(I,\mathbb{C})$ admet une dérivée n-ième sur I si et seulement si les fonctions à valeurs réelles $\mathrm{Re}f$ et $\mathrm{Im}f$ admettent une dérivée n-ième sur I et alors :
$$\mathrm{Re}(f^{(n)})=(\mathrm{Re}f)^{(n)}\text{ et }\mathrm{Im}(f^{(n)})=(\mathrm{Im}f)^{(n)}$$
• Si $f,g\in\mathscr{F}(I,\mathbb{C})$ sont n fois dérivables sur I (resp. de classe $\mathscr{C}^n$ sur I) alors $\lambda f+\mu g$, fg, $\dfrac{f}{g}$ (si g ne s'annule pas sur I) sont n fois dérivables sur I (resp. de classe $\mathscr{C}^n$ sur I) et
$$(\lambda f+\mu g)^{(n)}=\lambda f^{(n)}+\mu g^{(n)}$$
$$(fg)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}f^{(k)}g^{(n-k)}\text{(formule de Leibniz)}$$

Exercice
Préciser (et démontrer) si les affirmations suivantes restent vraies dans le cas complexe :
1. $f\in\mathscr{F}(I,\mathbb{C})$ dérivable sur I est constante sur I si et seulement f' est nulle sur I
2. Le théorème de Rolle et l'égalité des accroissements finis.
3. Inégalité des accroissements finis.
Soit $f:[a,b]\to\mathbb{C}$, continue sur $[a,b]$, dérivable sur $]a,b[$ (avec $a<b$) telle que $\forall x\in]a,b[,|f'(x)|\leqslant M$. Alors
$$\left|f(b)-f(a)\right|\leqslant M|b-a|.$$

Correction

1. VRAI : **Mais** en revanche l'étude du sens de variation de f n'a pas de sens.
2. FAUX : **Contre-exemple** : f définie sur $[0,2\pi]$ par $f(t)=e^{it}$.
On a en effet $f'(t)=ie^{it}$ qui ne s'annule jamais alors que $f(0)=f(2\pi)$. Cela provient du fait que les dérivées des parties réelle et imaginaire s'annulent bien (cos et sin) mais pas simultanément.
D'un point de vue cinématique, une fonction complexe pouvant représenter un mouvement dans le plan, cela se traduit par le fait qu'un mobile peut revenir à son point de départ sans pour autant que sa vitesse s'annule (ce qui n'est pas possible pour un mouvement rectiligne).
3. VRAI. On a $f(b)-f(a)=re^{i\theta}$ avec $(r,\theta)\in\mathbb{R}^+\times\mathbb{R}$. On applique l'inégalité des accroissements finis à la fonction à valeurs réelles $\mathrm{Re}g$ où g est la fonction définie sur $[a,b]$ par $g(x)=f(x)e^{-i\theta}$.
$$\mathrm{Re}\big(g(b)-g(a)\big)=\mathrm{Re}\big(|f(b)-f(a)|e^{-i\theta}\big)=|f(b)-f(a)|$$
car $f(b)-f(a)=|f(b)-f(a)|e^{i\theta}$. Ainsi
$$|f(b)-f(a)|=\mathrm{Re}\big(g(b)-g(a)\big)\leqslant|b-a|\sup(\mathrm{Re}g)'\leqslant|b-a|\sup\left(\mathrm{Re}f'e^{i\theta}\right)$$

5. Bilan

Synthèse

⇝ Si l'on souhaite encore plus maîtriser les variations de $f(x)$, en maitrisant les variations de x, il est bon de connaitre le rapport entre ces deux types de variations. C'est la dérivée.

⇝ Tout le cours consiste à redémontrer les résultats exploités en début d'année. On gagne, dans ce chapitre : le théorème de Rolle qui s'étend en égalité des accroissements finis (EAF) sur $\mathbb{R}$) ou inégalités des accroissements finis (IAF) sur $\mathbb{R}$ ou $\mathbb{C}$, on donne enfin la démonstration sur l'impact du signe de f' qui donne les variations de f et les conséquences lorsque f' admet une limite…

⇝ Comme d'habitude on termine par l'extension sur $\mathbb{C}$. En perdant la relation d'ordre, on perd l'EAF…

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Les racines imbriquées
— Savoir-faire - Quelle fonction φ choisir pour bien appliquer le théorème de Rolle?
— Savoir-faire - Contrôle f' pour contrôler f
— Savoir-faire - Application (I.A.E.) à l'étude des suites $u_{n+1}=f(u_n)$
— Savoir-faire - Exploiter le théorème de la limite de la dérivée

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\mathscr{C}^k(I)$	Ensemble des fonctions k fois dérivables sur I et donc la k-ième dérivée est continue sur I	$\mathscr{C}^{k+1}(I)\subset\mathscr{C}^k(I)$	On dit aussi que f est de classe $\mathscr{C}^k$.
$\mathscr{C}^\infty(I)$	Ensemble des fonctions infiniment dérivables sur I	$\mathscr{C}^\infty(I)=\bigcap_{k\in\mathbb{N}}\mathscr{C}^k(I)$	On dit aussi que f est de classe $\mathscr{C}^\infty$.

Retour sur les problèmes

92. $x\mapsto|x|$ est continue, non dérivable en 0.
On note $\theta(x)=x-\lfloor x\rfloor$, partie décimale de x. Alors $x\mapsto\theta(x)[\theta(x)\leqslant\frac{1}{2}]+(1-\theta(x))[\theta(x)>\frac{1}{2}]$ est continue, non dérivable en tous les points $\dfrac{m}{2}$ avec $m\in\mathbb{Z}$.
Un gribouillage est continue, nulle part dérivable. Abel a également un célebre contre-exemple trouvable sur internet.
93. Cours. Mais les formules ne sont pas toujours faciles (composition).

94. Le fameux théorème qui n'est pas le prolongement de la fonction dérivée…
95. Oui ! La maîtrise de la dérivée, donne un encadrement de la fonction f.
96. Cours. Pour les fonctions de $\mathbb{C} \to \mathbb{C}$, on appelle holomorphe la qualité d'être dérivable. Cela donne une grande rigidité à la fonction et donc quelques qualités. Comme la plupart des fonctions usuelles sont holomorphes (toutes celles qui peuvent s'écrire sous forme de série), elles possèdent donc de nouvelles qualités (du moins, que l'on ignorait).

Chapitre 22

Convexité

Résumé -

Les fonctions ne sont rarement totalement croissantes ou décroissantes, mais seulement par morceaux. De même, dans notre sac de fonctions, la plupart sont convexes ou concaves par morceaux. Cela nous donne une série d'inégalités facilement, celles-ci permettent en retour d'offrir des propriétés de régularité forte!
Quelques vidéos :

- *Bibmath - Des vidéos comme pastilles démonstratives - https ://www.bibmath.net/ressources/index.php ?action=affiche&quoi=mathspe/cours/convexe.html*
- *Kiffelesmaths - Fonctions concaves et convexes (L'école des mathématiques) - https ://www.youtube.com/watch ?v=va9NqRKArcw*
- *Lesbonsprofs (c'est eux qui le disent) - Fonctions convexe et fonction concave - https ://www.youtube.com/watch ?v=4P658MI1xxE*

Sommaire

1. Problèmes 432
2. Fonctions convexes 432
2.1. Ecriture paramétrique d'un segment 432
2.2. Définition d'une fonction convexe (et concave) . . . 432
2.3. Stabilité de l'ensemble des fonctions convexes . . . 433
3. Inégalités 433
3.1. Généralisation 433
3.2. Comparaison des pentes 434
3.3. Tangente 435
4. Régularité 436
4.1. Continuité 436
4.2. Critères de convexité (avec la dérivation) 436
5. Bilan 438

I désigne un intervalle de $\mathbb{R}$.

1. Problèmes

Problème 98 - Une dérivée seconde positive...

Les inégalités sont essentielles en analyse réelle.
Pour obtenir les inégalités, on exploite souvent la croissance (d'une différence) de fonctions. Quand tout va bien, on les obtient souvent par étude du signe de la dérivée.
Parfois, il faut dérivée deux fois. Par exemple pour obtenir $\sup_I |f'|$, lors de l'application de l'inégalité des accroissements finis.
Que dire d'une fonction dont la dérivée seconde est positive (cas d'application de l"inégalité des accroissements finis)? Quelle régularité cela donne?

Problème 99 - Convexité $\Rightarrow$ Dérivabilité ?

Réciproquement, la convexité implique-t-elle la dérivabilité? Et d'abord la continité?
La réponse est non, car $x \mapsto |x|$ est convexe mais non dérivable.
Néanmoins, on peut penser que tout n'est pas perdu...

2. Fonctions convexes

2.1. Ecriture paramétrique d'un segment

Analyse - Equation paramétrique d'un segment

Soient $x, y \in I$. Si u est situé entre x et y, on note $x \leqslant u \leqslant y$.
Donc $0 \leqslant \dfrac{u-x}{y-x} \leqslant 1$.
On a donc en notant $\lambda = \frac{u-x}{y-x}$, $\lambda(y-x) = u-x$ puis $u = \lambda y + (1-\lambda)x$.
Le segment $[x, y]$ est paramétré par $\{\lambda y + (1-\lambda)x \mid \lambda \in [0,1]\}$.

Proposition - Paramétrisation du segment $[a, b]$

Soient $a, b \in \mathbb{R}$.

$$t \in [a,b] \Longleftrightarrow \exists\, \lambda \in [0,1] \text{ tel que } t = \lambda a + (1-\lambda) b$$

A savoir ce nombre λ vérifie (réciproquement) : $\lambda = \dfrac{t-b}{a-b}$.

On vérifie aussi que $\lambda = 1 \Longleftrightarrow t = a$ et $\lambda = 0 \Longleftrightarrow t = b$.

2.2. Définition d'une fonction convexe (et concave)

Définition - Fonction convexe et concave

On dit que f est convexe sur I si

$$\forall\, x, y \in I, \forall\, \lambda \in [0,1], \qquad f\big(\lambda x + (1-\lambda) y\big) \leqslant \lambda f(x) + (1-\lambda) f(y)$$

Lorsque l'inégalité est stricte, alors on dit que la fonction f est strictement convexe.

On dit que f est concave (si $-f$ est convexe) sur I si

$$\forall\, x,y\in I, \forall\, \lambda\in[0,1],\qquad f\big(\lambda x+(1-\lambda)y\big)\geqslant \lambda f(x)+(1-\lambda)f(y)$$

Evidemment une fonction peut être ni convexe ni concave.

Exemple - $x\mapsto x^2$

Pour tout $x,y\in\mathbb{R}$, $\lambda\in[0,1]$,

$$\begin{aligned}\lambda x^2+(1-\lambda)y^2-(\lambda x+(1-\lambda)y)^2 &= [\lambda-\lambda^2]x^2+[(1-\lambda)-(1-\lambda)^2]y^2-2\lambda(1-\lambda)xy\\ &= [\lambda(1-\lambda)](x^2+y^2-2xy)=\lambda(1-\lambda)(x-y)^2\geqslant 0\end{aligned}$$

Donc la fonction $x\mapsto x^2$ est convexe.

Remarque - Critères de convexité

On démontrera par la suite que la fonction $x\mapsto e^x$ est convexe, ainsi que beaucoup d'autres fonctions… (au moins par morceaux).
Nous verrons un critère simple plus loin avec la dérivation (seconde).

Exercice

Que dire de f si f est convexe et concave sur I.

Correction

En fait, f est affine

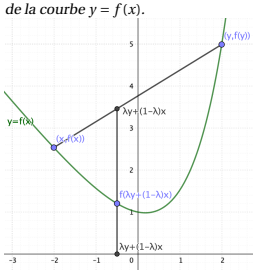
Savoir faire - Inégalité de convexité de manière explicite (et non uniquement paramétrique)

On cherche à énoncer l'inégalité de convexité pour $z\in[x,y]$, en remplaçant la forme paramétrique du segment $[x,y]$ par une version explicite.
Soit $z\in[x,y]$, alors il existe $\lambda\in[0,1]$ tel que $z=\lambda x+(1-\lambda)y$, il s'agit de $\lambda=\dfrac{z-y}{x-y}$ et $1-\lambda=\dfrac{z-x}{y-x}$.
On a alors

$$f(z)=f\big(\lambda x+(1-\lambda)y\big)\leqslant \lambda f(x)+(1-\lambda)f(y)=\frac{(z-y)f(x)-(x-z)f(y)}{x-y}$$

Représentation - Graphique

On a donc, pour tout $A(x,f(x))$ et $B(y,f(y))$ deux points de la courbe $y=f(x)$, le segment qui lie ses deux points (la corde) est au-dessus de la courbe $y=f(x)$.



2.3. Stabilité de l'ensemble des fonctions convexes

Proposition - Stabilité

Si f et g sont convexes sur I, alors $f+g$ est convexe sur I.
Si f est convexe sur I et $k\geqslant 0$. Alors kf est convexe sur I.

Démonstration

Les inégalités sont conservées par additions et multiplication par un nombre réel positif. □

La convexité (concavité) sert surtout pour obtenir facilement des inégalités…

3. Inégalités

3.1. Généralisation

Proposition - Généralisation - Inégalité de Jensen

Si f est convexe sur I, alors pour tout $n\in\mathbb{N}$, $a_1,a_2,\dots a_n\in I$ et $\lambda_1,\lambda_2,\dots\lambda_n\in[0,1]$ tel que $\sum_{k=1}^{n}\lambda_k=1$, on a

$$f\left(\sum_{k=1}^{n}\lambda_k a_k\right)\leqslant\sum_{k=1}^{n}\lambda_k f(a_k)$$

Démonstration

On démontre le résultat par récurrence sur n.
Notons, pour tout $n\in\mathbb{N}^*$ et $n\geqslant 2$,

$$\mathscr{P}_n:\text{« }\forall\, a_1,a_2,\dots a_n\in I,\lambda_1,\lambda_2,\dots\lambda_n\in[0,1]\mid \sum_{k=1}^{n}\lambda_k=1,\qquad f\left(\sum_{k=1}^{n}\lambda_k a_k\right)\leqslant\sum_{k=1}^{n}\lambda_k f(a_k).\text{ »}$$

— Puisque f est convexe, $\mathscr{P}_2$ est vraie.
— Soit $n\in\mathbb{N}$ et $n\geqslant 2$. Supposons que $\mathscr{P}_n$ est vraie.

Soient $a_1,a_2,\dots a_n,a_{n+1}\in I$ et $\lambda_1,\lambda_2,\dots\lambda_n,\lambda_{n+1}\in[0,1]$ tel que $\sum_{k=1}^{n+1}\lambda_k=1$, on a

$$\sum_{k=1}^{n+1}\lambda_k=\left(\sum_{k=1}^{n}\lambda_k\right)+\lambda_{n+1}=1$$

Donc $1-\lambda_{n+1}=\sum_{k=1}^{n}\lambda_k$.
On note $a=\dfrac{\sum_{k=1}^{n}\lambda_k a_k}{\sum_{k=1}^{n}\lambda_k}$.
Notons $a_-=\min(a_k,k\leqslant n)$ et $a_+=\max(a_k,k\leqslant n)$.
alors $\sum_{k=1}^{n}\lambda_k a_-\leqslant\sum_{k=1}^{n}\lambda_k a_k\leqslant\sum_{k=1}^{n}\lambda_k a_+$.
et donc $a_-\leqslant a\leqslant a_+$. Ainsi $a\in[a_-,a_+]\subset I$.
Puis, on applique la convexité pour f :

$$\begin{aligned}f\left(\sum_{k=1}^{n+1}\lambda_k a_k\right) &= f\left(\sum_{k=1}^{n}\lambda_k a_k+\lambda_{n+1}a_{n+1}\right)=f(\lambda_{n+1}a_{n+1}+(1-\lambda_{n+1})a)\\ &\leqslant\lambda_{n+1}f(a_{n+1})+(1-\lambda_{n+1})f(a)\end{aligned}$$

On note $\mu_k=\dfrac{\lambda_k}{1-\lambda_{n+1}}$, on a donc $\sum_{k=1}^{n}\mu_k=\dfrac{1}{1-\lambda_{n+1}}\sum_{k=1}^{n}\lambda_k=\dfrac{1-\lambda_{n+1}}{1-\lambda_{n+1}}=1$.
Ainsi, d'après $\mathscr{P}_n$,

$$f(a)=f\left(\sum_{k=1}^{n}\frac{\lambda_k}{1-\lambda_{n+1}}a_k\right)=f\left(\sum_{k=1}^{n}\mu_k a_k\right)\leqslant\sum_{k=1}^{n}\mu_k f(a_k)$$

Donc

$$f\left(\sum_{k=1}^{n+1}\lambda_k a_k\right)\leqslant\lambda_{n+1}f(a_{n+1})+(1-\lambda_{n+1})\sum_{k=1}^{n}\mu_k f(a_k)=\sum_{k=1}^{n+1}\lambda_k a_k$$

Donc $\mathscr{P}_{n+1}$ est vérifiée.
□

Savoir faire - Normaliser les coefficients pour la convexité

On notera la technique classique qui consiste étant donné une famille de coefficients $(\lambda_i)_{i\in I}$ positifs tel que $\sum_{i\in I}\lambda_i=S$ de considérer $\mu_i=\dfrac{\lambda_i}{S}$.
Alors $\mu_i\in[0,1]$ et $\sum_{i=1}^{n}\mu_i=1$.

3.2. Comparaison des pentes

Les inégalités suivantes, équivalentes à la convexité, aident pour l'étude de la continuité, voire de la dérivabilité de f.

Lemme - Inégalité des trois pentes

Soit f une fonction convexe sur I. Alors pour tout $x,y,z\in I$ et $x<y<z$,
on a $\dfrac{f(y)-f(x)}{y-x}\leqslant\dfrac{f(z)-f(x)}{z-x}\leqslant\dfrac{f(z)-f(y)}{z-y}$

ois pentes



Démonstration
Comme $y \in [x,z]$, il existe $\lambda \in [0,1]$ tel que $y = \lambda z + (1-\lambda)x$.
Il suffit de prendre $\lambda = \dfrac{y-x}{z-x}$.
Et donc $f(y) \leqslant \lambda f(z) + (1-\lambda) f(x) = \dfrac{y-x}{z-x} f(z) + \dfrac{z-y}{z-x} f(x)$.
Or $z - x \geqslant 0$, donc $(z-x)f(y) \leqslant (y-x)f(z) + (z-y)f(x)$.
• Ainsi en retranchant $(z-x)f(x)$: $(z-x)(f(y)-f(x)) \leqslant (y-x)f(z) + (x-y)f(x)$.
Or $y-x$ et $z-x \geqslant 0$ donc $\dfrac{f(y)-f(x)}{y-x} \leqslant \dfrac{f(z)-f(x)}{z-x}$ • Egalement : $(z-x)(f(z)-f(y)) = (z-x)f(z) - (z-x)f(y) \geqslant (z-x)f(z) - (y-x)f(z) - (z-y)f(x) = (z-y)(f(z)-f(x))$.
Or $z-y$ et $z-x \geqslant 0$ donc $\dfrac{f(z)-f(y)}{z-y} \geqslant \dfrac{f(z)-f(x)}{z-x}$ □

Proposition - Croissance des pentes
Soit f définie sur I.
f est convexe sur I si et seulement si,
pour tout $a \in I$, $\varphi_a : x \mapsto \dfrac{f(x)-f(a)}{x-a}$ est croissante sur $I \setminus \{a\}$

Démonstration
Supposons que f est convexe sur I.
Soit $a \in I$. Soit $u, v \in I \setminus \{a\}$.
On peut supposer sans perte de généralité que $u \leqslant v$.
Il y a trois possibilités : $\underbrace{a \leqslant u}_{\text{cas 1}}$; $\underbrace{v \leqslant a}_{\text{cas 3}}$ et $\underbrace{v \leqslant a \leqslant v}_{\text{cas 2}}$.
On applique alors le lemme des trois pentes : • pour le cas 1 : $x \leftarrow a$, $y \leftarrow u$ et $z \leftarrow v$.
• pour le cas 2 : $x \leftarrow u$, $y \leftarrow a$ et $z \leftarrow v$. • pour le cas 3 : $x \leftarrow u$, $y \leftarrow v$ et $z \leftarrow a$. Dans tous les cas, la conclusion est $\varphi_a(u) \leqslant \varphi_a(v)$. Donc φ_a croissante.
Réciproquement, supposons que pour tout a, φ_a est croissante.
Soient $x, y \in I$. SPDG : $x \leqslant y$. Soit $\lambda \in [0,1]$. Soit $a = \lambda x + (1-\lambda)y$.
Alors $\varphi_a(x) \leqslant \varphi_a(y)$ i.e. $\dfrac{f(x)-f(a)}{x-a} \leqslant \dfrac{f(y)-f(a)}{y-a}$.
$x - a < 0$ et $y - a > 0$: $(y-a)(f(x)-f(a)) \geqslant (x-a)(f(y)-f(a))$.
Ainsi $(y-a-x+a) = (y-x)f(a) \leqslant (y-a)f(x) + (x-a)f(y) = \lambda(y-x)f(x) + (1-\lambda)(y-x)f(y)$.
En simplifiant par $y - x \geqslant 0$, on trouve l'inégalité de convexité.
□

3.3. Tangente

On suppose localement que f est dérivable.

Proposition - Inégalité des tangentes
Soit f convexe sur I.
On suppose de plus que f est dérivable sur I.
Soit $x_0 \in I$, alors pour tout $x \in I$, $f(x) \geqslant f'(x_0)(x - x_0) + f(x_0)$

Démonstration
Dans le cas où $x < x_0$.
Soit $u \in [x, x_0]$, d'après le lemme des trois pentes :

$$\frac{f(u)-f(x)}{u-x} \leqslant \frac{f(x_0)-f(x)}{x_0-x} \leqslant \frac{f(x_0)-f(u)}{x_0-u}$$

En passant à la limite $u \to x_0$ dans la seconde inégalité (car la limite EXISTE) : $\dfrac{f(x_0)-f(x)}{x_0-x} \leqslant f'(x_0)$.
Comme $x_0 - x \geqslant 0$, on trouve $f(x) \geqslant f(x_0) - (x_0 - x)f'(x_0)$.
Dans le cas où $x < x_0$.
Soit $u \in [x_0, x]$, d'après le lemme des trois pentes :

$$\frac{f(u)-f(x_0)}{u-x_0} \leqslant \frac{f(x)-f(x_0)}{x-x_0} \leqslant \frac{f(x)-f(u)}{x-u}$$

En passant à la limite $u \to x_0$ dans la première inégalité : $f'(x_0) \leqslant \dfrac{f(x)-f(x_0)}{x-x_0}$.
Comme $x - x_0 \geqslant 0$, on trouve $f(x) \geqslant f(x_0) - (x_0 - x)f'(x_0)$.
□

A retenir : selon que l'on cherche une majoration de $f(x)$ ou une minoration,

Savoir faire - Utilisation de la convexité (inégalités)
Trois façons d'exploiter la convexité d'une fonction :
— La comparaison à la corde qui donne un **majorant** à $f(x)$
— La comparaison à la tangente qui donne un **minorant** à $f(x)$
— La comparaison des pentes, croissantes (avec le lemme des trois pentes ou directement).

4. Régularité

4.1. Continuité

Remarque - Rappel - Intérieur
On appelle intérieur de l'intervalle I, l'ensemble des nombres réels x tels qu'il existe $\epsilon > 0$ tel que $]x-\epsilon, x+\epsilon[\subset I$.
On note cet ensemble $\mathring{I}$. Cf chapitre de topologie réel.
Si I est ouvert, alors tout point x de I est nécessairement un point de $\mathring{I}$.

Proposition - Convexité implique continuité
Soit I un intervalle.
Si f est une fonction convexe sur I, alors f est continue sur $\mathring{I}$ (l'intérieur de I).

Démonstration
Soit $x \in \mathring{I}$. Donc il existe $\epsilon > 0$ tel que $]x-\epsilon, x+\epsilon[\subset I$.
On commence par la limite à droite.
Pour tout $u \in [x, x+\epsilon]$, il existe $\lambda \in [0,1]$ tel que $u = \lambda(x+\epsilon) + (1-\lambda)x$.
Par convexité : $f(u) \leqslant \lambda f(x+\epsilon) + (1-\lambda) f(x)$.
Notons que le terme de droite admet une limite pour $\lambda \to 0$, i.e. $u \to x$, qui vaut $f(x)$.
Puis $x \in [x-\epsilon, u]$ donc il existe $\lambda \in [0,1]$ tel que $x = \lambda(x-\epsilon) + (1-\lambda)u$.
Par convexité : $f(x) \leqslant \lambda f(x-\epsilon) + (1-\lambda) f(u)$.
$\dfrac{1}{1-\lambda}\big(f(x) - \lambda f(x-\epsilon)\big) \leqslant f(u)$.
Notons que le terme de gauche admet une limite pour $\lambda \to 0$, i.e. $u \to x$, qui vaut $f(x)$.
Donc, par double encadrement, $f(u)$ converge pour $u \to x^+$ vers $f(x)$.
Et donc f admet une limite à droite en x.
De manière équivalente, on montre que f admet une limite à gauche en x. □

On verra mieux au chapitre suivant.

4.2. Critères de convexité (avec la dérivation)

Avec f'

Lorsqu'une fonction est suffisamment régulière, démontrer sa convexité est simple.

Proposition - Critère de convexité avec la dérivée
Si f est dérivable sur I.
Alors f est convexe sur I ssi f' est croissante sur I

Démonstration
Supposons f est convexe.
Soient $a<b\in I$ et $h\in]a,b[$.
D'après le lemme des trois pentes : $\frac{f(h)-f(a)}{h-a}\leqslant\frac{f(b)-f(a)}{b-a}\leqslant\frac{f(b)-f(h)}{b-h}$.
On fait $h\to a$ dans la première inégalité et donc $f'(a)\leqslant\frac{f(b)-f(a)}{b-a}$.
On fait $h\to b$ dans la seconde inégalité et donc $f'(b)\geqslant\frac{f(b)-f(a)}{b-a}$.
Par transitivité, on trouve la croissance de f'.
Réciproquement, supposons que f' est croissante.
Soient $x,y\in I$ et $\lambda\in[0,1]$ et $z=\lambda x+(1-\lambda)y$.
Sans perte de généralité, on peut supposer que $x<y$.
D'après l'égalité des accroissements finis, il existe $c_1\in[x,z]$ tel que $\frac{f(z)-f(x)}{z-x}=f'(c_1)$.
D'après l'égalité des accroissements finis, il existe $c_2\in[z,y]$ tel que $\frac{f(y)-f(z)}{y-z}=f'(c_2)$.
Par croissance de f' : $\frac{f(z)-f(x)}{z-x}\leqslant\frac{f(y)-f(z)}{y-z}$
et donc, comme $y-z>0$ et $z-x>0$:
$(y-x)f(z)\leqslant(z-x)f(y)+(y-z)f(x)$.
Mais $z-x=(1-\lambda)(y-x)$, $y-z=\lambda(y-x)$ et $y-x\geqslant0$,
donc $f(z)\leqslant(1-\lambda)f(y)+\lambda f(x)$.
Ainsi f est convexe. □

Savoir exploiter f'', si possible

Savoir faire - Démontrer qu'une fonction est convexe.
Dans de très nombreux cas, on montre que f est convexe en montrant que f est dérivable et f' est croissante.
Et la plupart du temps, on a f dérivable deux fois. Dans ce cas f est convexe si (et seulement si) $f''\geqslant0$

Exercice

1. Montrer que exp est convexe.
2. En déduire que l'inégalité arithmético-géométrique sur $\mathbb{R}+$: $\frac{a+b}{2}\geqslant\sqrt{ab}$

Correction

1. exp est de classe $\mathscr{C}^\infty$ et $\exp''=\exp\geqslant0$.
2. Posons $a=e^A$ et $b=e^B$,
$\sqrt{ab}=\sqrt{\exp A\exp B}=\exp(\frac{A+B}{2})\leqslant\frac{1}{2}e^A+\frac{1}{2}e^B=\frac{a+b}{2}$

Dérivabilité (partielle) par la convexité

Proposition - Dérivabilité à gauche et à droite
Soit f convexe sur l'intervalle I.
Alors f est dérivable à gauche et à droite en tout point x de $\mathring{I}$ et $f'_g(x)\leqslant f'_d(x)$.

Mais on n'a pas nécessairement $f'_g(x)=f'_d(x)$, comme pour $x\mapsto|x|$, sinon f serait dérivable en x.

Démonstration
Soit $x\in\mathring{I}$. Il existe $u,v\in I$ tel que $u<x<v$.
On sait que $\varphi_x:t\mapsto\frac{f(t)-f(x)}{t-x}$ est croissante sur $I\setminus\{x\}$.
Alors φ_x est croissante et bornée sur $[u,x[\cup]x,v]$.
Elle est minorée par $\varphi_x(u)$ et majorée par $\varphi_x(v)$.
Alors elle admet une limite pour $t\to x^-$ égale à $\sup_{t<x}\varphi_x(t)$.
Et de même φ_x et minorée par $\varphi_x(u)$.

Alors elle admet une limite pour $t\to x^+$ égale à $\inf_{t>x}\varphi_x(t)$.
Enfin, pour tout $T>x$, $\varphi_x(T)$ est un majorant de $\{\varphi_x(t),t<x\}$ (par croissance de φ_x),
Donc $\varphi_x(T)>\sup_{t<x}\varphi_x(t)=f'_g(x)$ (le plus petit des majorants).
Par conséquent, $f'_g(x)$ est un minorant de $\{\varphi_x(T),T>x\}$.
Donc $f'_d(x)=\inf_{t>x}\varphi_x(t)>f'_g(x)$ (le plus grand des minorants). □

On retrouve en corollaire la continuité de f en x.

5. Bilan

Synthèse

⇝ L'un des plus importants résultats de topologie réelle est le TVI : il n'y a pas de trou dans $\mathbb{R}$ et toute transformation qui conserve une partie sans trou (ou intervalle) de $\mathbb{R}$ doit être continue. L'enjeu est donc la continuité! Il faut pour cela définir la notion de limite de fonction, en un point, puis sur un intervalle.

⇝ Nous terminons par l'étude des fonctions à valeurs dans $\mathbb{C}$.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Inégalité de convexité de manière explicite (et non uniquement paramétrique)
— Savoir-faire - Normaliser les coefficients pour la convexité.
— Savoir-faire - Démontrer qu'une fonction est convexe.
— Savoir-faire - Utilisation de la convexité (inégalités)

Notations

Notations	*Définitions*	*Propriétés*	*Re*
$\mathring{I}$	Intérieur de l'ensemble I	$\{x\in I\mid\exists\epsilon>0\mid]x-\epsilon,x+\epsilon[\subset I\}$	Si val

Retour sur les problèmes

97. Attention, c'est une condition suffisante, mais non nécessaire. Voir le problème suivant
98. On a vu dans le cours que la convexité impliquait la dérivabilité à droite et à gauche en tout point, mais pas la dérivabilité générale.

Chapitre 23

Développements limités

Résumé -

Au voisinage d'un point a, une courbe est tout à fait comparable à une droite; pas n'importe laquelle : sa tangente d'équation $y = a + f'(a)(x-a)$. Est-il possible d'être encore plus précis? Les développements limités répondent à cette question : ils permettent de transformer une fonction quelconque en une famille plus simple de fonctions -polynômes de Taylor- très proche.

Pour pouvoir affirmer ce résultat (et l'exploiter abusivement en sciences physiques), il faut d'abord commencer par formaliser du vocabulaire très précis : une fonction f est dominé par (resp. négligeable devant, équivalente à) une fonction g au voisinage de a si…

Au passage, on formalisera l'expression bien connue des lycées : « g l'emporte sur f »…

Au lieu d'une liste de problème, nous commençons par l'étude d'un cas précis.

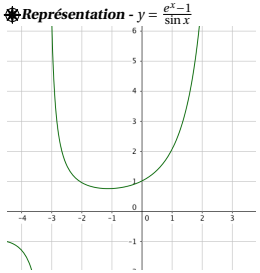
Quelques vidéos :

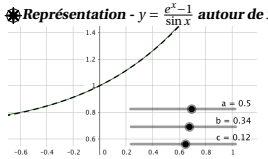
- *Optimal sup/spé - Formules de Taylor et Développements limités - https ://www.youtube.com/watch ?v=TVW8UBTmT58*
- *Avenir-cours - DLA(1) de ln(x)/x? a partir de DL connus MPSI - https ://www.youtube.com/watch ?v=a8Q5ErJNPYs*
- *Science for all - Les développements limités Relativité 3 - https ://www.youtube.com/watch ?v=TM9HdSBat8o*

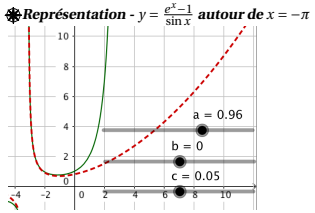
Sommaire

1. Problème 440
2. Vocabulaire et opérations pour des développements asymptotiques de fonctions 440
2.1. Rappel : le cas des suites 440
2.2. Définitions 441
2.3. Relations d'équivalence. Relation de préordre 443
2.4. Echelle de comparaison 444
2.5. Algèbre des relations de comparaison 445
3. Développements limités 447
3.1. Définitions 447
3.2. Propriétés 448
3.3. Existence de développements limités 449
3.4. Opérations 453
3.5. Généralisation 456
4. Applications des DL 457
4.1. Recherche de limites et d'équivalents (suite ou fonction) 457
4.2. Etude locale d'une fonction 457
5. Bilan 459

1. Problème







Problème 100 - Une courbe, des zooms

Considérons une fonction exemplaire :

$$f(x) = \frac{e^x - 1}{\sin x}$$

Le tracé de cette courbe figure en marge.
Elle semble de classe $\mathscr{C}^\infty$ sur $]-\pi,\pi[$.
On peut alors visiblement obtenir certains nombres significatifs : $f(0)$, $f'(0)\ldots$, mais aussi $\lim_{+\pi^-} f$ ou encore $\lim_{+\pi^-} f'\ldots$
On peut dire mieux, au lieu de regarder en un point, on peut regarder au voisinage d'un point. On zoome par exemple en 0 ou en $+\pi$ (cf. en marge).
Cela la puissance du zoom, on voit alors apparaître une famille de fonctions plus ou moins simples ; plus ou moins connue.

- Au voisinage de 0 : Visiblement $f(0) = 1$. Une première approximation est $f = 1$. Pas satisfaisant… Puis par tâtonnement, il semble que la courbe d'équation (polynomiale) $y = 1 + \frac{1}{2}x + \frac{1}{3}x^2 + \frac{1}{8}x^3$ semble très proche de $y = f(x)$, au moins au voisinage de 0.
- Au voisinage de $-\pi$: La valeur est infini, cela ressemble plus à une hyperbole.
  Par tâtonnement, il semble que $y = \frac{1-e^{-\pi}}{x+\pi} + e^{-\pi}(-1 + \frac{1}{2}(x+\pi))$

Le principe d'un développement limité, consiste à approcher une fonction (ou une suite) par une fonction (ou une suite) mieux connue ; polynomiale par exemple

Heuristique - Développement limité

Le principe est le suivant :

1. On remplace une fonction par un développement mieux maîtrisé (polynôme…)
2. Cela dépend du voisinage du point considéré.
3. Plus on souhaite qu'il soit bon, plus il faudra qu'il y ait de coefficients.

Il est d'abord nécessaire de comprendre comment comparer deux fonctions (celle de référence et sa version locale polynômiale). On s'intéresse donc dans cette partie aux relations de comparaison entre fonctions.
Le principe est le même pour les suites (mais étudiées toujours uniquement en $n \to +\infty$).

Attention - Selon le point

Il n'est jamais trop tôt pour insister : la fonction (polynomiale - par exemple) plus simple qui décrit f **dépend du point** auprès duquel on est amené à faire l'étude.
Le résultat au voisinage de 0, n'a rien à voir avec celui au voisinage de $+\pi$! (par exemple)

2. Vocabulaire et opérations pour des développements asymptotiques de fonctions

2.1. Rappel : le cas des suites

Définition - Définition généralisée
Soient $(u_n),(v_n)\in\mathbb{R}^{\mathbb{N}}$. On dit que
— (u_n) est négligeable devant (v_n), notée $u_n{=}o(v_n)$ si

$$\forall\epsilon>0,\exists N\in\mathbb{N}\text{tel que}\forall n\geqslant N,|u_n|\leqslant\epsilon|v_n|.$$

— (u_n) est équivalente à (v_n), notée $u_n\sim v_n$ si $u_n-v_n=o(v_n)$.
— (u_n) est dominée par (v_n), notée $u_n=O(v_n)$ si

$$\exists C>0,\exists N\in\mathbb{N}\text{tel que}\forall n\geqslant N,|u_n|\leqslant C|v_n|.$$

Savoir faire - Etude de négligeabilité/équivalence/domination… d'une suite.
Deux cas fréquents pour étudier une suite (u_n) :
— si la suite $(u_n)=f(n)$, alors en fait on étudie directement la fonction f…
Très souvent, on se *ramène* à cette situation.
— si la suite est définie implicitement ou par récurrence, on étudie la limite de $\frac{u_n}{v_n}$, où v_n est le candidat pour être respectivement : le facteur de négligeabilité / d'équivalence / de domination (dans ce cas la limite vaut respectivement 0 / 1 / est bornée.

Remarque - Rappels
On rappelle également que l'on a vu
— $n!\underset{n\to+\infty}{\sim}n^ne^{-n}\sqrt{2\pi n}$ (formule de Stirling)
— $\sum_{k=1}^{n}\frac{1}{k}\underset{n\to+\infty}{\sim}\ln n$

2.2. Définitions

Définition - Définition généralisée
Soient $f,g:I\to\mathbb{R}$ et $a\in\overline{\mathbb{R}}$, point ou borne de I. On dit que
— f est négligeable devant g au voisinage de a, notée $f\underset{a}{=}o(g)$ si

$$\forall\epsilon>0,\exists V\in\mathcal{V}_a\,|\,\forall x\in V,|f(x)|\leqslant\epsilon|g(x)|.$$

— f est équivalente à g au voisinage de a, notée $f\sim_a g$ si $f-g\underset{a}{=}o(g)$.
— f est dominée par g au voisinage de a, notée $f\underset{a}{=}O(g)$ si

$$\exists C>0,\exists V\in\mathcal{V}_a\,|\,\forall x\in V,|f(x)|\leqslant C|g(x)|.$$

Remarque - Ensemble $g^{-1}(\{0\})$
Si $g(x)=0$ pour $x\in V$, alors nécessairement, pour les trois cas précédent : $f(x)=0$.
Donc $g^{-1}(\{0\})\cap V\subset f^{-1}(\{0\}$, autrement écrit : $\mathcal{Z}(g)\cap V\subset\mathcal{Z}(f)$.

Proposition - Caractérisation avec une fonction auxiliaire
Soient $f,g:I\to\mathbb{R}$ et $a\in\overline{\mathbb{R}}$, point ou borne de I.
Alors, on a $f=_a o(g)$ si et seulement si
il existe une fonction h telle que $h\underset{a}{\to}0$ et $f=hg$ au voisinage de a.
Alors, on a $f\sim_a g$ si et seulement si
il existe une fonction h telle que $h\underset{a}{\to}1$ et $f=hg$ au voisinage de a.
Alors, on a $f=_a O(g)$ si et seulement si
il existe une fonction h telle que h est bornée au voisinage de a et

$f=hg$ au voisinage de a.

Démonstration
• Supposons que $f=_a o(g)$.
Soit $h=\frac{f}{g}$ sur $\mathbb{R}\setminus\mathcal{Z}_g$ et $h=0$ dès que $g(x)=0$.
$\forall\epsilon>0,\exists V\in\mathcal{V}_a\,|\,\forall x\in V_a\setminus\mathcal{Z}_g,|h(x)|=\left|\frac{f(x)}{g(x)}\right|\leqslant\epsilon$ ou bien $h(x)=0$.
Réciproquement, s'il existe une fonction h telle que $h\underset{a}{\to}0$ et $f=hg$ au voisinage de a.
Alors pour tout $\epsilon>0$, il existe un voisinage V tel que $|h|\leqslant\epsilon$ sur V.
Sur l'intersection des deux voisinages : $|f(x)|\leqslant\epsilon|g(x)|$ donc $f=_a o(g)$.
• On a les équivalences :
$f\sim_a g\iff f-g=o_a(g)\iff\exists\,h_1$ telle que $f-g=h_1g$ au voisinage de a et $h_1\to_a 0$
$f\sim_a g\iff\exists\,h=(h_1+1)$ telle que $f=(h_1+1)g=hg$ au voisinage de a et $h\to_a 1$
• Supposons que $f=_a O(g)$.
Soit $h=\frac{f}{g}$ sur $\mathbb{R}\setminus\mathcal{Z}_g$ et $h=0$ dès que $g(x)=0$.
$\exists C>0,\exists V\in\mathcal{V}_a\,|\,\forall x\in V_a\setminus\mathcal{Z}_g,|h(x)|=\left|\frac{f(x)}{g(x)}\right|\leqslant C$ ou bien $h(x)=0$.
Donc h est bornée au voisinage de a et $f=hg$ au voisinage de a.
Réciproquement, s'il existe une fonction h bornée au voisinage de a et telle que $f=hg$ au voisinage de a.
Alors il existe $C>0$, il existe un voisinage V tel que $|h|\leqslant\epsilon$ sur V.
Sur l'intersection des deux voisinages : $|f(x)|\leqslant C|g(x)|$ donc $f=_a O(g)$.
□

Proposition - Domination, négligeabilité, équivalence pour les fonctions
Soient $f,g:I\to\mathbb{R}$ et $a\in\overline{\mathbb{R}}$, point ou borne de I ($a\in\overline{I}$).
— f est négligeable devant g au voisinage de a si et seulement si
$\frac{f(x)}{g(x)}\underset{x\to a,x\notin g^{-1}(\{0\})}{\longrightarrow}0$ et $\exists\,V\in\mathrm{V}_a$ tel que $g^{-1}(\{0\})\cap V\subset f^{-1}(\{0\}$
— f est équivalente à g au voisinage de a si et seulement si
$\frac{f(x)}{g(x)}\underset{x\to a}{\longrightarrow}1$et $\exists\,V\in\mathrm{V}_a$ tel que $g^{-1}(\{0\})\cap V\subset f^{-1}(\{0\}$
— f est dominée par g au voisinage de a ssi la fonction $\frac{f}{g}$ est bornée sur un voisinage de a et $g^{-1}(\{0\})\subset f^{-1}(\{0\}$, au voisinage de a.

Attention - Insistons bien
Pour les fonctions, il s'agit bien d'une relation LOCALE (au voisinage de a).
On peut avoir $f=o(g)$ au voisinage de a ET $g=o(f)$ au voisinage de b…
Donc « $f=o(g)$, sans précision supplémentaire » NE SIGNIFIE RIEN

Démonstration
On a vu que si $f\underset{a}{=}o(g)$, alors $\exists\,V\in\mathrm{V}_a$ tel que $g^{-1}(\{0\})\cap V\subset f^{-1}(\{0\}$.
Et par ailleurs, pour tout ϵ, $\exists\,V\in\mathrm{V}_a$ tel que $\forall\,x\in V\,|f(x)|\leqslant\epsilon|g(x)|$,
donc pour $x\notin g^{-1}(\{0\}$, $\frac{|f(x)|}{|g(x)|}\leqslant\epsilon$ et donc $\frac{f(x)}{g(x)}\underset{x\to a,x\notin g^{-1}(\{0\})}{\longrightarrow}0$.
Réciproquement, en pour tout ϵ, $\exists\,V\in\mathrm{V}_a$ tel que $\forall\,x\in V$, $\frac{f(x)}{g(x)}\underset{x\to a,x\notin g^{-1}(\{0\})}{\longrightarrow}0$, donc $|f(x)|\leqslant\epsilon|g(x)|$,
Puis il existe V' tel que $g^{-1}(\{0\})\cap V'\subset f^{-1}(\{0\}$, donc pour $x\in V'$, $f(x)=0\leqslant\epsilon g(x)=0$.
, pour $x\in V'\cap V$, $|f(x)|\leqslant\epsilon|g(x)|$, donc $f\underset{a}{=}o(g)$ □

Exercice
Faire les autres démonstrations

Correction

Savoir faire - Avec une fonction « relative »

Notons, pour tout $x \in I$, $h(x) = \dfrac{f(x)}{g(x)}$. Alors

- f est dominée par g au voisinage de a ssi h est bornée au voisinage de a.
- f est négligeable devant g au voisinage de a ssi $h \xrightarrow[x\to a]{} 0$.
- f est équivalente à g au voisinage de a ssi $h \xrightarrow[x\to a]{} 1$.

Avec $g = 1$, on trouve directement :

Proposition - Comparaison à une fonction constante
Soit f définie au voisinage de a. On a

$$f \underset{a}{=} O(1) \quad \Leftrightarrow f \text{ est bornée au voisinage de } a.$$
$$f \underset{a}{=} o(1) \quad \Leftrightarrow f(x) \xrightarrow[x\to a]{} 0$$

2.3. Relations d'équivalence. Relation de préordre

Pour les propositions suivantes, les démonstrations sont simplifiées par le fait que les fonctions ne s'annulent pas au voisinage de a, donc on peut considérer $h = \frac{f}{g}$ avec g non nul sur un voisinage de a .

Proposition - Equivalence : relation d'équivalence
Soient f, g, h trois fonctions définies et ne s'annulant pas sur un voisinage de a (ou juste en a). On a

- $f \underset{a}{\sim} f$ (réflexivité).
- Si $f \underset{a}{\sim} g$ alors $g \underset{a}{\sim} f$ (symétrie).
- Si $f \underset{a}{\sim} g$ et $g \underset{a}{\sim} h$ alors $f \underset{a}{\sim} h$ (transitivité).

La relation d'équivalence $\sim$ est donc une relation d'équivalence

Démonstration

- $\frac{f}{f} = 1 \to 1$, donc $f \sim_a f$.
- Si $f \sim_a g$, alors $h := \frac{f}{g} \underset{a}{\to} 1$ et donc $(f \neq 0)$ alors $\frac{g}{f} \underset{a}{\to} \frac{1}{1}$ et donc $g \sim_a f$
- Si $f \sim_a g$ et $g \sim_a h$, alors $\frac{f}{h} = \frac{f}{g} \times \frac{g}{h} \to 1 \times 1$ donc $f \underset{a}{\sim} h$.

□

Proposition - Relation de préordre
Soient f, g, h trois fonctions définies et ne s'annulant pas sur un voisinage de a. On a

- $f = O(f)$ au voisinage de a (réflexivité)
- Si $f = O(g)$ et $g = O(h)$ au voisinage de a alors $f = O(h)$ au voisinage de a. (transitivité)

Pour aller plus loin - Relation : même ordre de grandeur
Pour avoir une relation d'ordre, il faut associer la propriété d'antisymétrie.
Donc définir une égalité $\asymp$ entre fonctions par :

$$f \underset{a}{=} O(g) \text{ et } g \underset{a}{=} O(f) \Longrightarrow f \asymp g$$

Démonstration

- $f \sim f$, donc $\frac{f}{f} \leqslant \frac{3}{2}$, au voisinage de a
- $\exists\, C_1, C_2 \in \mathbb{R}_+$ et $V \in \mathcal{V}_a$ (quitte à intersecter) tels que $\frac{f}{h} = \frac{f}{g}\frac{g}{h} \leqslant C_1 C_2$.
  Donc $f =_a O(h)$

□

Proposition - Liens entre les relations
Soient f, g, h trois fonctions définies et ne s'annulant pas sur un voisinage de a. On a

- Si $f \underset{a}{=} o(g)$ alors $f \underset{a}{=} O(g)$
- On a : $f \underset{a}{\sim} g \Leftrightarrow f - g \underset{a}{=} o(g)$ (ou encore noté : $f = g + o(g)$).
- Si $f \underset{a}{\sim} g$ alors $f \underset{a}{=} O(g)$ et $g \underset{a}{=} O(f)$.
- Si $f \underset{a}{\sim} g$ alors $h \underset{a}{=} o(f) \Leftrightarrow h \underset{a}{=} o(g)$.

Démonstration

- Si $\frac{f}{g} \underset{a}{\to} 0$, alors $\frac{f}{g}$ est bornée.
- C'est la définition. Attention, le « = » n'est pas classique, il ne s'agit pas juste de faire passer le g de l'autre côté.
- Si $f \sim_a g$, alors $\frac{f}{g} \leqslant \frac{3}{2}$ au voisinage de a et de même $\frac{g}{f} \leqslant \frac{3}{2}$ au voisinage de a
- Supposons que $f \sim_a g$ et donc $g \sim_a f$.
  Si $h =_a o(f)$, alors $\frac{h}{g} = \frac{h}{f} \times \frac{f}{g} \underset{a}{\to} 0 \times 1 = 0$, donc $h =_a o(g)$.
  Ainsi $h =_a o(f) \Longrightarrow h =_a o(g)$. Les rôles de f et g sont interchangeables donc on a également $h =_a o(g) \Longrightarrow h =_a o(f)$.

□

2.4. Echelle de comparaison

Les résultats suivants sont tout simplement une réécriture des formules de croissances comparées bien connues.

Proposition - Comparaisons usuelles
Pour $\alpha > 0, \beta > 0$ on a

$$(\ln x)^\beta \underset{+\infty}{=} o(x^\alpha), \quad x^\alpha \underset{+\infty}{=} o(e^{\beta x}),$$
$$|\ln x|^\beta \underset{0}{=} o(\frac{1}{x^\alpha},)$$
$$e^{\beta x} \underset{-\infty}{=} o(\frac{1}{|x|^\alpha}).$$

On a également pour $0 < p < q$:

$$x^p \underset{+\infty}{=} o(x^q)$$
$$x^q \underset{0}{=} o(x^p) \text{ et } (x-a)^q \underset{a}{=} o((x-a)^p).$$

En d'autres termes, aux bornes des intervalles de définition, "l'exponentielle domine(=*« l'emporte sur »*) la puissance, la puissance domine(=*« l'emporte sur »*) le logarithme" (croissances comparées).

Proposition - Taux d'accroissement réinterprété
En utilisant les limites classiques (taux d'accroissement), on a

1. $\sin x \underset{0}{=} x + o(x)$ ou encore $\sin x \underset{0}{\sim} x$
2. $\tan x \underset{0}{=} x + o(x)$ ou encore $\tan x \underset{0}{\sim} x$
3. $\ln(1+x) \underset{0}{=} x + o(x)$ ou encore $\ln(1+x) \underset{0}{\sim} x$
4. $e^x \underset{0}{=} 1 + x + o(x)$ ou encore $e^x - 1 \underset{0}{\sim} x$
5. $(1+x)^\alpha \underset{0}{=} 1 + \alpha x + o(x)$ $(\alpha \in \mathbb{R}^*)$ ou encore $(1+x)^\alpha - 1 \underset{0}{\sim} \alpha x$

Démonstration
Cette proposition est originale.

$$\lim \frac{\sin x}{x} = \lim \frac{\sin x - \sin 0}{x-0} = \sin'(0) = \cos(0) = 1 \Rightarrow \sin x \underset{x\to 0}{\sim} x \Leftrightarrow \sin x \underset{0}{=} x + o(x)$$

$$\lim \frac{\tan x}{x} = \lim \frac{\tan x - \tan 0}{x-0} = \tan'(0) = \frac{1}{\cos^2(0)} = 1 \Rightarrow \tan x \underset{x\to 0}{\sim} x \Leftrightarrow \tan x \underset{0}{=} x + o(x)$$

$$\lim \frac{\ln(1+x)}{x} = \lim \frac{\ln(1+x) - \ln(1+0)}{x-0} = \ln'(1+0) = \frac{1}{1} = 1 \Rightarrow \ln(1+x) \underset{x\to 0}{\sim} x \Leftrightarrow \ln(1+x) \underset{0}{=} x + o(x)$$

$$\lim \frac{e^x - 1}{x} = \lim \frac{e^x - e^0}{x-0} = \exp'(0) = e^0 = 1 \Rightarrow e^x - 1 \underset{x\to 0}{\sim} x \Leftrightarrow e^x \underset{0}{=} 1 + x + o(x)$$

Toujours avec α constant, $f_\alpha(x) = (1+x)^\alpha$, dérivable en 0 :

$$\lim \frac{f_\alpha(x) - f_\alpha(0)}{x} = \lim \frac{(1+x)^\alpha - 1}{x} = f'_\alpha(0) = \alpha(1+0)^{\alpha-1} = \alpha \Rightarrow (1+x)^\alpha - 1 \underset{x\to 0}{\sim} \alpha x \Leftrightarrow (1+x)^\alpha \underset{0}{=} 1 + \alpha x + o(x)$$

□

2.5. Algèbre des relations de comparaison

Proposition - Opérations avec o ou O
Soient f, g, h, k quatre fonctions définies au voisinage de a. On a
- Si $f \underset{a}{=} o(g)$ et $g \underset{a}{=} o(h)$ alors $f \underset{a}{=} o(h)$.
- Si $f \underset{a}{=} o(h)$ et $g \underset{a}{=} o(h)$ alors $f + g \underset{a}{=} o(h)$.
- Si $f \underset{a}{=} o(g)$, $\lambda \in \mathbb{R}^*$ alors $\lambda f \underset{a}{=} o(g)$
- Si f et g ne s'annulent pas au voisinage de a et si $f \underset{a}{=} o(g)$ alors $\frac{1}{g} \underset{a}{=} o(\frac{1}{f})$.
- Si $f \underset{a}{=} o(g)$ et $h \underset{a}{=} o(k)$ alors $fh \underset{a}{=} o(gk)$.
- Si les fonctions f et g sont > 0 avec $f \underset{a}{=} o(g)$, alors pour $\alpha > 0$ on a $f^\alpha \underset{a}{=} o(g^\alpha)$.
- Si $f \underset{a}{=} o(g)$ alors $hf \underset{a}{=} o(hg)$

Les propriétés sont encore vraies en remplaçant les « o » par des « O ».

Démonstration

- Soit $\epsilon > 0$,
  il existe $V_1 \in \mathcal{V}_a$ tel que $\forall\, x \in V_1, |f(x)| \leqslant \epsilon |g(x)|$.
  il existe $V_2 \in \mathcal{V}_a$ tel que $\forall\, x \in V_2, |g(x)| \leqslant 1 |h(x)|$. Il existe $V = V_1 \cap V_2 \in \mathcal{V}_a$ tel que $\forall\, x \in V, |f(x)| \leqslant \epsilon 1 |h(x)|$. Ceci est vrai pour tout $\epsilon > 0$, quelconque (et fixé).
- Soit $\epsilon > 0$,
  il existe $V_1 \in \mathcal{V}_a$ tel que $\forall\, x \in V_1, |f(x)| \leqslant \frac{\epsilon}{2} |h(x)|$.
  il existe $V_2 \in \mathcal{V}_a$ tel que $\forall\, x \in V_2, |g(x)| \leqslant \frac{\epsilon}{2} |h(x)|$. Il existe $V = V_1 \cap V_2 \in \mathcal{V}_a$ tel que $\forall\, x \in V, |f(x) + g(x)| \leqslant |f(x)| + |g(x)| \leqslant \epsilon h(x)$. Ceci est vrai pour tout $\epsilon > 0$, quelconque (et fixé).
- Soit $\lambda \neq 0$. Soit $\epsilon > 0$,
  il existe $V \in \mathcal{V}_a$ tel que $\forall\, x \in V, |f(x)| \leqslant \frac{\epsilon}{|\lambda|} |g(x)|$, donc $|\lambda f(x)| \leqslant \epsilon |g(x)|$.
- Supposons que f et g soient non nulles au voisinage de a. Soit $\epsilon > 0$,
  il existe $V \in \mathcal{V}_a$ tel que $\forall\, x \in V, g(x) \neq 0$, $f(x) \neq 0$ et $|f(x)| \leqslant \epsilon |g(x)|$,
  ainsi $\frac{1}{|f(x)|} \geqslant \frac{1}{\epsilon} \frac{1}{|g(x)|}$, et donc $\frac{1}{|g(x)|} \leqslant \epsilon \frac{1}{|f(x)|}$
- Soit $\epsilon > 0$,
  il existe $V_1 \in \mathcal{V}_a$ tel que $\forall\, x \in V_1, |f(x)| \leqslant \epsilon |g(x)|$.
  il existe $V_2 \in \mathcal{V}_a$ tel que $\forall\, x \in V_2, |h(x)| \leqslant 1 |k(x)|$. Il existe $V = V_1 \cap V_2 \in \mathcal{V}_a$ tel que $\forall\, x \in V, |f(x)h(x)| = |f(x)| \times |h(x)| \leqslant \epsilon 1 |g(x)||k(x)| = \epsilon |g(x)k(x)|$.
- Supposons que $f, g > 0$ au voisinage de a. Soit $\epsilon > 0$, $\alpha > 0$, donc $\sqrt[\alpha]{\epsilon} \in \mathbb{R}_+^*$,
  il existe $V \in \mathcal{V}_a$ tel que $\forall\, x \in V, |f(x)| \leqslant \sqrt[\alpha]{\epsilon} |g(x)|$.
  il existe $V \in \mathcal{V}_a$ tel que $\forall\, x \in V, |f(x)^\alpha| = |f(x)|^\alpha \leqslant \epsilon |g(x)|^\alpha = \epsilon |g(x)^\alpha|$.
- Si $h = 0$, infiniment souvent au voisinage de a, c'est un peu pénible.
  Sinon, cela ne pose pas trop de problème…

□

Remarque - Où avons-nous besoin de $f, g > 0$?
Pour la démonstration du sixième résultat

Théorème - Signe d'une fonction
Si f est équivalente à g en a, alors il existe V voisinage de a, tel que f et g sont de même signe sur $V \setminus \{a\}$.

Exercice
Faire la démonstration

Correction

Prenons $\epsilon = \frac{1}{2}$, il existe V voisinage de a tel que pour tout $x \in V$, $\frac{1}{2} \leqslant \frac{f(x)}{g(x)} \leqslant \frac{3}{2}$.
Soit $x \in V$.
- Si $g(x) > 0$, alors $0 < \frac{1}{2} g(x) \leqslant f(x)$, donc $f(x) > 0$.
- Si $g(x) < 0$, alors $0 > \frac{1}{2} g(x) \geqslant f(x)$ donc $f(x) < 0$.

Dans tous les cas f et g sont de même signe sur V.

Théorème - Equivalents et limite
Soient $f, g : I \to \mathbb{R}$ et $a \in \overline{I}$.
- Si $\ell \in \mathbb{R}$, $\ell \neq 0$, alors $f(x) \underset{x\to a}{\longrightarrow} \ell$, si et seulement si $f \underset{a}{\sim} \ell$;
- Si $f \underset{a}{\sim} g$ et $g(x) \underset{x\to a}{\longrightarrow} \ell \in \overline{\mathbb{R}}$ alors $f(x) \underset{x\to a}{\longrightarrow} \ell$.

Démonstration
La division par ℓ est problématique si $\ell \neq 0$…
- Puisque $\ell \in \mathbb{R}^*$, alors $\frac{f}{\ell} \to 1 \Longleftrightarrow f \sim_a \ell$.
- Si $\ell \in \mathbb{R}^*$, alors $g \sim_a \ell$ et par transitivité : $f \sim_a \ell$ donc $f \to_a \ell$.
  Supposons que $\ell = 0$.
  Alors $|f(x)| \leqslant |f(x) + g(x)| + |g(x)| \leqslant (\epsilon + 1)|g(x)| \to 0$. Donc $f \to 0$.
  Supposons que $\ell = +\infty$. Soit $X > 0$.
  Il existe un voisinage V de a tel que pour $x \in V$, $g(x) \geqslant 2X$, et $|f(x) - g(x)| \leqslant \frac{1}{2}|g(x)| = \frac{1}{2} g(x)$.
  On a, pour tout $x \in V$, $f(x) = f(x) - g(x) + g(x) \geqslant -\frac{1}{2} g(x) + g(x) = \frac{1}{2} g(x) \geqslant X$.
  Par conséquent $f \to +\infty$. De même pour $\ell = -\infty$.

□

Proposition - Opérations
Soient f, g, h trois fonctions définies sur un voisinage de a. On a
- Si $f \underset{a}{\sim} g$ et $h \underset{a}{\sim} k$ alors $fh \underset{a}{\sim} gk$ (et $\frac{f}{h} \underset{a}{\sim} \frac{g}{k}$ si h ne s'annule pas)
- Soit $\alpha \in \mathbb{R}$. Si $f \underset{a}{\sim} g$, f ou g strictement positives (une suffit...) alors $f^\alpha \underset{a}{\sim} g^\alpha$

Démonstration
Il existe deux fonctions $u \to_a 1$, $v \to_a 1$ telles que $f = u \times g$ et $h = v \times k$.
Par produit, $fh = (uv)gk$ et donc il existe $w = uv \to_a 1$ telle que $fh = wgk$.
Si f est strictement positive, il en est de même de g, puisque $f \sim_a g$.
Il existe $u \to_a 1$ telle que $f = u \times g$.
En prenant la puissance α-ième ($\alpha > 0$), alors $f^\alpha = u^\alpha g^\alpha$.
Et on a alors $u^\alpha \to_a 1$. □

En appliquant le théorème de composition des limites, nous avons un nouveau résultat :

Proposition - Substitution dans les relations de comparaison
Soient ϕ définie sur un voisinage de a telle que $\lim_{t\to a} \phi(t) = b$, f, g définies sur un voisinage de b. Alors :

$$f \underset{b}{=} O(g) \Rightarrow f \circ \phi \underset{a}{=} O(g \circ \phi)$$

$$f \underset{b}{=} o(g) \Rightarrow f \circ \phi \underset{a}{=} o(g \circ \phi)$$

$$f \underset{b}{\sim} g \Rightarrow f \circ \phi \underset{a}{\sim} g \circ \phi$$

Démonstration
Faisons la seconde démonstration.
Il existe une voisinage V de b et Il existe une fonction $h \to_b 0$ telle que pour tout $x \in V$: $f(x) = h(x) \times g(x)$.
En composant par Φ : $f(\Phi(t)) = h(\Phi(t)) \times g(\Phi(t))$.
Notons $k = h \circ \Phi$, on a alors $f \circ \Phi = k \times g \circ \Phi$, avec par composition $\lim_{t \to a} k(t) = \lim_{t \to a} h(\Phi(t)) = \lim_{x \to b} h(x) = 1$. □

Attention - Ce qui ne marche pas
D'une manière générale, les équivalents ne passent ni aux sommes, ni aux exponentielles, ni aux logarithmes.
— Somme : en 0 avec $f_1(t) = t$, $f_2(t) = t + t^2$, $g_1(t) = g_2(t) = -t$
on a $f_1 \underset{0}{\sim} f_2$ mais $f_1 + g_1 \underset{0}{\not\sim} f_2 + g_2$.

— Exponentielle : en $+\infty$ avec $f(t) = t^2$ et $g(t) = t^2 + t$
on a $f \underset{+\infty}{\sim} g$ mais $e^f \underset{+\infty}{\not\sim} e^g$.

Exercice
Déterminer un équivalent de $\ln(\sin x)$ en 0.

Correction
Au voisinage de 0 :
$\sin x = x + o(x)$, donc $\ln(\sin(x)) = \ln(x + o(x)) = \ln(x(1 + o(1))) = \ln x + \ln(1 + o(1)) = \ln x + o(1)$.
C'est même mieux. . ..
$\ln(\sin x) \sim \ln x$

Attention - Rien de plus TERRIBLE. . .
Ne pas écrire $f \sim 0$, cela n'a pas de sens avec la définition précédente, et avec la définition générale qui suit, cela signifie que f est nulle dans un voisinage de a (ce qui est bien rare...)

Attention - Confusion fréquente
Ne pas confondre $f \sim g$ et $f(x) - g(x) \xrightarrow[x \to a]{} 0$.
Par exemple $x + 1 \underset{+\infty}{\sim} x$ mais $x + 1 - x = 1$ ne tend pas vers 0 en $+\infty$.

3. Développements limités

3.1. Définitions

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. $n \in \mathbb{N}$.

Définition - DL en un point réel
Soit I un intervalle contenant a ou d'extrémité a. Soit f une fonction définie sur I sauf éventuellement en a, à valeurs dans $\mathbb{K}$. On dit que f admet un développement limité d'ordre n au voisinage de a (en abrégé DL_n en a ou $DL_n(a)$) s'il existe un polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}_n[X]$ tel que

$$\forall x \in I, f(x) \underset{a}{=} P(x-a) + o((x-a)^n)$$
$$\underset{a}{=} a_0 + a_1(x-a) + \cdots + a_n(x-a)^n + o((x-a)^n)$$

ce qui peut aussi s'écrire

$$\forall x \in I, f(x) = a_0 + a_1(x-a) + \cdots + a_n(x-a)^n + (x-a)^n \epsilon(x) \text{ où } \epsilon(x) \xrightarrow[x \to a]{} 0$$

ou

$$f(a+h) \underset{h \to 0}{=} a_0 + a_1 h + \cdots + a_n h^n + o(h^n)$$

$P(x-a)$ s'appelle la partie régulière du DL_n de f en a.

Pour aller plus loin - Linéarisation d'une équation différentielle
Supposons que l'on doit résoudre une équation différentielle d'inconnue y mais qui n'est pas linéaire.
On peut l'écrire sous la forme $F(y, y', \ldots y^{(n)}) = 0$ si elle est d'ordre n.
Imaginons qu'on connait une solution $\tilde{y}$ du problème.
*On chercher alors une autre solution dans son voisinage : $y(t) = \tilde{y}(t) + \epsilon(t)$. On a alors : $F(\tilde{y} + \epsilon, \tilde{y}' + \epsilon', \ldots \tilde{y}^{(n)} + \epsilon^{(n)}) = 0$. Or cette équation peut **se linéariser** : on fait un DL_1 de F au voisinage de $\tilde{y}$, cela conduit à une équation différentielle **linéaire** d'ordre n.*
On connait des méthodes de résolution. . .

Définition - DL en ∞
Soit f une fonction définie sur $I = [a, +\infty[$. On dit que f admet un développement limité d'ordre n au voisinage de $\pm\infty$ s'il existe un polynôme $P = \sum_{k=0}^{n} a_k X^k \in K_n[X]$ tel que

$$\forall x \in I, f(x) = P\left(\frac{1}{x}\right) + o\left(\frac{1}{x^n}\right)$$
$$= a_0 + \frac{a_1}{x} + \cdots + \frac{a_n}{x^n} + o\left(\frac{1}{x^n}\right).$$

Remarque - Ecriture
Par convention, les termes d'un développement limité sont toujours écrits dans l'ordre croissant des puissances (de $(x-a)$ ou $1/x$). Ainsi chaque terme est négligeable devant ceux qui le précèdent et chaque nouveau terme apporte une précision par rapport à ceux qui le précède.

3.2. Propriétés

Théorème - Unicité
— Si f admet un DL_n en $a \in \mathbb{R}$ (ou en ∞), il est unique.
— Si f admet un DL_n en a, alors f admet un DL_p en $a \in \mathbb{R}$ (ou en ∞) pour tout $p \leqslant n$ obtenu en tronquant la partie régulière à la puissance p (c'est-à-dire en enlevant les monômes de degré $> p$ du polynôme).

Pour aller plus loin - Linéarisation d'une équation différentielle (suite)
Considérons (par hasard. . .) le problème : $y'' + a\sin(y) = 0$.
Une solution est $\tilde{y} : t \mapsto 0$. Une solution approchée est $y = \tilde{y} + \epsilon$.
On a donc $\sin(y) = \sin(0 + \epsilon) = \epsilon - \frac{\epsilon^3}{6} + o(\epsilon^4)$.
Donc si ϵ reste proche de 0 : $y'' - ay = o(y)$ et donc une solution approchée est $y = A\sin(\sqrt{a}t + \varphi)$.
Les solutions sont de la forme : $t \mapsto A\sin(\sqrt{a}t + \varphi) + o(t)$ . . .

Démonstration
Rappelons d'abord que si $m > n$, alors $\lambda(x-a)^m = o((x-a)^n)$, au voisinage de 0. Au voisinage de a, supposons que $f(x) = \sum_{k=0}^{p} a_k(x-a)^k + o((x-a)^p) = \sum_{h=0}^{n} b_h(x-a)^h + o((x-a)^n)$.
Nous avons donc :

$$\sum_{k=0}^{\min(p,n)} (a_k - b_k)(x-a)^k + o((x-a)^{\min(n,p)}) = 0$$

Si il existe $i \leqslant \min(n,p)$ tel que $a_i \neq b_i$.
Notons $i_0 = \min\{i \mid a_i \neq b_i\}$, on a donc :

$$(a_{i_0} - b_{i_0})(x-a)^{i_0} + o((x-a)^{i_0}) = 0 \Rightarrow (a_{i_0} - b_{i_0})(x-a)^{i_0} = o((x-a)^{i_0}) \Rightarrow \lim \frac{(a_{i_0} - b_{i_0})(x-a)^{i_0}}{(x-a)^{i_0}} = 0$$

Et donc $a_{i_0} = b_{i_0}$, ce qui est contradictoire.
Donc pour tout $i \leqslant \min(n,p)$, $a_i = b_i$ □

Corollaire - Lien avec la parité
Soit f définie sur un voisinage de 0.
— Si f admet en 0 un DL_n, $f(x) = P(x) + o(x^n)$, alors $g : x \mapsto f(-x)$ admet en 0 le DL_n

$$g(x) = P(-x) + o(x^n).$$

— Si f admet un DL_n en 0 et f paire (resp. f impaire) alors le DL ne

contient que des puissances paires (resp. impaires).

Démonstration
$g(x) = f(-x) = P(-x) + o((-x)^n) = P(-x) + o(x^n)$ et par unicité…
Si f est paire, alors $f(x) = P(x) + o(x^n) = f(-x) = P(-x) + o(x^n)$.
Par unicité : $P(-x) = P(x)$, donc P est paire.
(attention, il faut bien voir P en tant que forme polynomiale et non fonction) □

Proposition - Limites et équivalents
- Si f admet un DL_n en $a \in \mathbb{R}$ alors f est continue ou prolongeable par continuité en a, avec $f(a) = a_0$.
- Si $n \geqslant 1$, f (ou son prolongement) est dérivable en a, de dérivée a_1.
- Le premier (si les puissances sont « rangées » comme il faut!) terme non nul d'un DL de f en a fournit un équivalent en a, ou encore si on a la **forme normalisée** d'un DL

$$f(a+h) \underset{h\to 0}{=} h^p(a_p + a_{p+1}h + \cdots + a_n h^{n-p} + o(h^{n-p})) \text{ avec } a_p \neq 0 \text{ et } n \geqslant p$$

alors $f(a+h) \underset{h\to 0}{\sim} a_p h^p$.

Remarque - Généralisation en $+\infty$
En ∞, si f admet un DL_n alors f admet a_0 pour limite et le premier (si les puissances sont « rangées » comme il faut!) terme non nul d'un DL de f en ∞ fournit un équivalent.

Démonstration
Supposons, qu'au voisinage de a :
$$f(a+h) \underset{h\to 0}{=} h^p(a_p + a_{p+1}h + \cdots + a_n h^{n-p} + o(h^{n-p})) \text{ avec } a_p \neq 0 \text{ et } n \geqslant p$$
Donc
$$\frac{f(a+h)}{a_p h^p} = 1 + h(a_{p+1} + \cdots + a_n h^{n-1} + o(h^{n-1})) \underset{h\to 0}{\longrightarrow} 1$$
Ainsi $f(a+h) \underset{h\to 0}{\sim} a_p h^p$. En particulier $\lim_{h\to 0} f(a+h) = a_0$ (que celui-ci soit nul ou non).
Et si f admet un DL_1, en a :
$$\frac{f(a+h) - f(a)}{h} = \frac{a_0 + a_1 h + o(h) - a_0}{h} = a_1 + o(1) \underset{h\to 0}{\longrightarrow} a_1$$
□

Attention - A ne pas généraliser pour $f^{(2)}(a)$
Cela ne se généralise pas aux dérivées suivantes.
Contre-exemple : Soit f la fonction définie sur $\mathbb{R}$ par $f(x) = \begin{cases} x^{100}\sin\frac{1}{x^{100}} \text{ si } x \neq 0 \\ 0 \text{ sinon} \end{cases}$ Alors f admet un DL_{99} en 0 ($f(x) = 0 + o(x^{99})$) mais n'est pas deux fois dérivable en 0.

Savoir faire - Obtenir un $DL_n(a)$ d'une fonction f
On se ramène usuellemenent en 0 :
- Pour obtenir un DL_n en a de f, on pose $h = x - a$, on effectue un DL_n en 0 de $g(h) = f(a+h)$ puis on remplace h par $x - a$.
- Pour obtenir un DL_n en ∞ de f, on pose $t = 1/x$, on effectue un DL_n en 0 de $g(t) = f(1/t)$ puis on remplace t par $1/x$.

Il suffit donc de savoir obtenir les $DL_n(0)$

3.3. Existence de développements limités

On cherche maintenant les $DL_n(0)$ des fonctions usuelles.

Théorème - Premières formules
Les fonctions $\frac{1}{1-x}$ et $\frac{1}{1+x}$ admettent des DL_n en 0 pour tout $n \in \mathbb{N}$ donnés par :
$$\frac{1}{1-x} \underset{x\to 0}{=} 1 + x + x^2 + \cdots + x^n + o(x^n)$$
$$\frac{1}{1+x} \underset{x\to 0}{=} 1 - x + x^2 - x^3 + \ldots + (-1)^n x^n + o(x^n)$$

Démonstration
$$\forall x \neq 1,\ \frac{1}{1-x} = 1 + x + x^2 + \cdots + x^n + \frac{x^{n+1}}{1-x}$$
□

Proposition - Primitivation
Soient I un intervalle de $\mathbb{R}$ contenant 0 et $F : I \to \mathbb{R}$ dérivable. On suppose que F' admet un DL_n en 0
$$F'(x) \underset{x\to 0}{=} a_0 + a_1 x + \cdots + a_n x^n + o(x^n).$$
Alors F admet en 0 le DL_{n+1} (obtenu en primitivant celui de F)
$$F(x) \underset{x\to 0}{=} F(0) + a_0 x + \frac{a_1}{2}x^2 + \cdots + \frac{a_n}{n+1}x^{n+1} + o(x^{n+1}).$$

Exercice
Donner le $DL_n(0)$ de $x \mapsto \ln(1+x)$

Correction
On intègre le $DL_{n-1}(0)$ de $x \mapsto \frac{1}{1+x}$.
On a donc $\ln(1+x) \underset{x\to 0}{=} \ln 1 + \sum_{k=1}^{n} (-1)^{n-1}\frac{x^n}{n} + o(x^n)$

Démonstration
Soit $\varphi : x \mapsto F(x) - F(0) - \sum_{k=0}^{n} \frac{a_k}{k+1}x^{k+1}$.
Il existe $\epsilon : I \to \mathbb{R}$ et un voisinage V de 0 tels que $F'(x) = a_0 + a_1 x + \cdots + a_n x^n + x^n\epsilon(x)$ et $\epsilon(x) \to_0 0$.
On applique l'inégalité des accroissements finis :
$$|\varphi(x) - \varphi(0)| \leqslant \sup_{t\in[0,x]} |\varphi'(t)||x-0|$$
Or $\forall\, x \in V$, $|\varphi'(x)| = \left|F'(x) - \sum_{k=0}^{n} a_k x^k\right| \leqslant |x^n\epsilon(x)|$.
Donc pour tout $x \in V$, $|\varphi(x)| \leqslant x^{n+1}\epsilon(x)$. □

Corollaire -
$$\operatorname{Arctan} x \underset{x\to 0}{=} x - \frac{x^3}{3} + \frac{x^5}{5} - \cdots + (-1)^n \frac{x^{2n+1}}{2n+1} + o(x^{2n+2})$$

Démonstration
Au voisinage de 0, $\arctan'(x) = \frac{1}{1+x^2} = \sum_{k=0}^{n} (-1)^n x^2 n + o(x^{2n})$.
On intégre le DL
$$\arctan(x) = \arctan(0) + \sum_{k=0}^{n} \frac{(-1)^n}{2n+1}x^{2n+1} + o(x^{2n+1})$$
□

Attention - Mais on ne peut pas dériver!!

Si f est dérivable, l'existence d'un DL_n pour f n'implique pas l'existence d'un DL_{n-1} pour f'.

Soit f la fonction définie sur $\mathbb{R}$ par $f(x) = \begin{cases} x^{100}\sin\frac{1}{x^{100}} \text{ si } x \neq 0 \\ 0 \text{ sinon} \end{cases}$ Alors f admet un DL_{99} en 0, mais n'est pas deux fois dérivable en 0.

Remarque - Mais tout n'est pas perdu...

En revanche si f est de classe $\mathscr{C}^n$, alors f' est de classe $\mathscr{C}^{n-1}$ et le DL_{n-1} de f' est obtenu par dérivation du DL_n de f.
(son intégration doit correspondre avec celui de f (unicité))

Théorème - Formule de Taylor-Young

Soient I un intervalle de $\mathbb{R}$, f une application de I dans K, n fois dérivable en $a \in I$.
Alors il existe $\epsilon : I \to \mathbb{R}$ tel que pour tout $x \in I$ on a

$$f(x) = \sum_{k=0}^{n} \frac{(x-a)^k}{k!} f^{(k)}(a) + \frac{(x-a)^n}{n!}\epsilon(x) \text{ avec } \lim_{x\to a}\epsilon(x) = 0.$$

Démonstration

On démontre le résultat par récurrence sur n.

— Si f est (1 fois) dérivable en a,

$$\epsilon(x) = \frac{f(x)-f(a)}{x-a} - f'(a) \underset{x\to a}{\longrightarrow} 0$$

En multipliant par $x-a$, on trouve $\mathscr{P}_1$.

— Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}_n$ est vraie.
Soit f dérivable $n+1$ fois en a. Alors f' est n fois dérivable en a.
On peut lui appliquer $\mathscr{P}_n$

$$f'(x) = \sum_{k=0}^{n} \frac{(x-a)^k}{k!} f^{(k+1)}(a) + \frac{(x-a)^n}{n!}\epsilon(x) \text{ avec } \lim_{x\to a}\epsilon(x) = 0.$$

Si on intègre ce DL d'ordre n (une primitive de $\mapsto (x-a)^k$ est $x \mapsto \frac{1}{k+1}(x-a)^{k+1}$, même pour $k=0$) :

$$f(x) = f(a) + \sum_{k=0}^{n} \frac{(x-a)^{k+1}}{(k+1)!} f^{(k+1)}(a) + \frac{(x-a)^{n+1}}{(n+1)!}\epsilon(x) \text{ avec } \lim_{x\to a}\epsilon(x) = 0.$$

Et donc $\mathscr{P}_{n+1}$ est vraie.

□

Attention - Ne pas en dire trop

Cette formule donne uniquement un résultat **local**, elle NE sert donc QU'à préciser la fonction f au voisinage de a.

Corollaire - Condition suffisante simple

Toute fonction n fois dérivable en a admet un DL_n en a, donné par la formule de Taylor-Young.

Ce résultat permet de retrouver les DL précédemment obtenus, mais également ceux d'autres fonctions usuelles :

Proposition - Développements limités usuels en 0

On a les résultats suivants (à connaître parfaitement)

$$e^x \underset{x\to0}{=} 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + o(x^n)$$

$$\cos x \underset{x\to0}{=} 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots + (-1)^p \frac{x^{2p}}{(2p)!} + o(x^{2p}) (\text{ ou } o(x^{2p+1}))$$

$$\sin x \underset{x\to0}{=} x - \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots + (-1)^p \frac{x^{2p+1}}{(2p+1)!} + o(x^{2p+1}) (\text{ ou } o(x^{2p+2}))$$

$$\operatorname{ch} x \underset{x\to0}{=} 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots + \frac{x^{2p}}{(2p)!} + o(x^{2p}) (\text{ ou } o(x^{2p+1}))$$

$$\operatorname{sh} x \underset{x\to0}{=} x + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots + \frac{x^{2p+1}}{(2p+1)!} + o(x^{2p+1}) (\text{ ou } o(x^{2p+2}))$$

$$(1+x)^\alpha \underset{x\to0}{=} 1 + \alpha x + \alpha(\alpha-1)\frac{x^2}{2!} + \ldots + \alpha(\alpha-1)\ldots(\alpha-n+1)\frac{x^n}{n!} + o(x^n)$$

$$\frac{1}{1+x} \underset{x\to0}{=} 1 - x + x^2 - x^3 + \ldots + (-1)^n x^n + o(x^n)$$

$$\ln(1+x) \underset{x\to0}{=} x - \frac{x^2}{2} + \frac{x^3}{3} + \ldots + (-1)^{n-1}\frac{x^n}{n} + o(x^n)$$

$$\sqrt{1+x} \underset{x\to0}{=} 1 + \frac{x}{2} - \frac{x^2}{8} + o(x^2) \quad (\alpha = \frac{1}{2})$$

$$\frac{1}{\sqrt{1+x}} \underset{x\to0}{=} 1 - \frac{x}{2} + \frac{3}{8}x^2 + o(x^2) \quad (\alpha = -\frac{1}{2})$$

Démonstration

On va démontrer le résultat fonction par fonction.

— $\exp : x \mapsto e^x$ est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$ et pour tout $k \in \mathbb{N}$, $\exp^{(k)} = \exp$ (récurrence).
On a donc $\forall\, k \in \mathbb{N}$, $\exp^{(k)}(0) = e^0 = 1$. On applique la formule de Taylor-Young :

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + o(x^n)$$

— De même $\exp i : x \mapsto e^{ix}$ est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$ (à valeurs dans $\mathbb{C}$) et pour tout $k \in \mathbb{N}$, $\exp i^{(k)} = i^k \exp i$ (récurrence).
On a donc $\forall\, k \in \mathbb{N}$, $\exp i^{(k)}(0) = i^k e^0 = i^k$. On applique la formule de Taylor-Young :

$$e^{ix} = 1 + ix - \frac{x^2}{2!} - i\frac{x^3}{3!} + \ldots + \frac{i^n x^n}{n!} + o(x^n)$$

En prenant les parties réelles et imaginaires :

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots + (-1)^p \frac{x^{2p}}{(2p)!} + o(x^{2p}) (\text{ ou } o(x^{2p+1}))$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots + (-1)^p \frac{x^{2p+1}}{(2p+1)!} + o(x^{2p+1}) (\text{ ou } o(x^{2p+2}))$$

— ch est la partie paire de e^x et sh sa partie impaire :

$$\operatorname{ch} x = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots + \frac{x^{2p}}{(2p)!} + o(x^{2p}) (\text{ ou } o(x^{2p+1}))$$

$$\operatorname{sh} x = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots + \frac{x^{2p+1}}{(2p+1)!} + o(x^{2p+1}) (\text{ ou } o(x^{2p+2}))$$

— On peut aussi démontrer par récurrence que si $f_\alpha : x \mapsto (1+x)^\alpha$, alors pour tout $k \in \mathbb{N}^*$,

$$\forall\, x > -1, \qquad f_\alpha^{(k)}(x) = \alpha(\alpha-1)\ldots(\alpha-k+1)(1+x)^{\alpha-k} \Rightarrow f_\alpha^{(k)}(0) = \alpha(\alpha-1)\ldots(\alpha-k+1)$$

Donc

$$(1+x)^\alpha = \sum_{k=0}^{n} \frac{\alpha(\alpha-1)\ldots(\alpha-k+1)}{k!}x^k + o(x^n) = 1 + \alpha x + \alpha(\alpha-1)\frac{x^2}{2!} + \ldots + \alpha(\alpha-1)\ldots(\alpha-n+1)\frac{x^n}{n!} + o(x^n)$$

On notera qu'avec $\alpha \in \mathbb{N}$, on retrouve la formule du binôme de Newton.

— On a vu la fonction $x \mapsto \frac{1}{1+x}$ (ou prendre $\alpha = -1$ dans le développement précédent)

— On pourrait primitiver le DL précédent pour obtenir celui de $x \mapsto \ln(1+x)$ (voir un théorème plus loin).
On peut aussi démontrer par récurrence que si $f : x \mapsto \ln(1+x)$, alors pour tout $k \in \mathbb{N}^*$,

$$\forall\, x \neq -1, \qquad f^{(k)}(x) = \frac{(-1)^{k-1}(k-1)!}{(1+x)^k} \Rightarrow f^{(k)}(0) = (-1)^{k-1}(k-1)!$$

Donc

$$\ln(1+x) = f(0) + \sum_{k=1}^{n} \frac{(-1)^{k-1}(k-1)!}{k!}x^k + o(x^n) = x - \frac{x^2}{2} + \frac{x^3}{3} + \ldots + (-1)^{n-1}\frac{x^n}{n} + o(x^n)$$

— On prend $\alpha = \frac{1}{2}$ ou $\alpha = -\frac{1}{2}$, pour les deux derniers

□

Remarque - Composition de DL = composition de polynômes
En fait, on remarque que dans plusieurs cas, l'enjeu des composés des développements limités, il s'agit donc d'appliquer des formules de composition de polynômes.
Or, on a vu que cela n'était pas vraiment une choses facile…
On reviendra sur cette remarque un peu plus loin…

Exercice
Terminer la démonstration pour obtenir le DL d'ordre 4 de $x \mapsto \frac{1}{\sqrt{1+x}}$

Correction
On prend $\alpha = -\frac{1}{2}$, donc

$$\frac{1}{\sqrt{1+x}} \underset{x\to 0}{=} 1+\frac{-1}{2}x+\frac{\frac{-1}{2}\frac{-3}{2}}{2}x^2+\frac{\frac{-1}{2}\frac{-3}{2}\frac{-5}{2}}{6}x^3+\frac{\frac{-1}{2}\frac{-3}{2}\frac{-5}{2}\frac{-7}{2}}{24}x^4+o(x^4) = 1-\frac{1}{2}x+\frac{3}{8}x^2-\frac{5}{16}x^3+\frac{35}{128}x^4+o(x^4)$$

Savoir faire - DL des fonctions de référence en une autre valeur
Supposons que $x \to a$ pour $x \to a$. Alors $h = x - a \to 0$. On a respectivement :
— $\exp(x) = \exp(a+h) = e^a \times \exp(h) = e^a(1+h+\frac{h}{2}+\dots)$
— $\ln(x) = \ln(a+h) = \ln\left(a(1+\frac{h}{a})\right) = \ln a + \frac{h}{a} - \frac{h^2}{2a^2}+\dots)$
— $\cos(x) = \cos(a+h) = \cos a\cos h - \sin a \sin h = \cos a(1-\frac{h^2}{2}+\dots) - \sin a(h-\frac{h^3}{6}+\dots)$
— $\mathrm{sh}(x) = \mathrm{sh}(a+h) = \mathrm{sh}(a)\,\mathrm{ch}\,h + \mathrm{ch}\,a\,\mathrm{sh}\,a\dots$ (à démontrer)
— $x^\alpha = (a+h)^\alpha = a^\alpha \times (1+\frac{h}{a})^\alpha = a^\alpha(1+\alpha\frac{h}{a}+\frac{\alpha(\alpha-1)}{2}\frac{h^2}{a^2}+\dots$

3.4. Opérations

Proposition - Combinaison linéaire
Si f et g admettent en a des DL_n alors pour $\lambda, \mu \in K$, $\lambda f + \mu g$ admet un DL_n en a, obtenu en faisant la combinaison linéaire correspondante des DL_n.
(résultat encore valable en ∞)

Démonstration
Il s'agit d'une simple addition, puis d'une identification (par unicité du DL) □

Exercice
Donner un DL_3 en 0 de $\cos x + 2\sin(-x)$.

Correction
$\cos(x) \underset{x\to 0}{=} 1-\frac{x^2}{2}+o(x^3)$ et $\sin(x) = x - \frac{x^3}{6}+o(x^3)$ au voisinage de 0.
Donc $\cos x + 2\sin(-x) \underset{x\to 0}{=} 1-2x-\frac{x^2}{2}+\frac{x^3}{3}+o(x^3)$ au voisinage de 0

Proposition - Produit
Si f et g admettent des DL_n en a alors fg admet un DL_n en a obtenu en multipliant les DL_n de f et de g et en supprimant les termes de degré $> n$ (termes non significatifs).
(résultat encore valable en ∞)

Démonstration
Supposons qu'au voisinage de 0, $f(x) = \sum_{k=0}^{n} a_k x^k + o(x^n) = P_n(x) + o(x^n)$ et $g(x) = \sum_{k=0}^{n} b_k x^k + o(x^n) = Q_n(x) + o(x^n)$.
Alors (il s(agit bien d'une égalité) :
Au voisinage de 0,

$$f(x)g(x) = \left(\sum_{k=0}^{n} a_k x^k + o(x^n)\right)\left(\sum_{k=0}^{n} b_k x^k + o(x^n)\right) = P_n(x)\times Q_n(x) + o(x^n(P_n(x)+Q_n(x)+x^n))$$

Or on peut imagine que $a_0 \neq 0$ ou $b_0 \neq 0$, donc dans ce cas (le « pire »), on peut seulement affirmer :

$$o(x^n(P_n(x)+Q_n(x)+x^n)) = o(x^n)$$

Auquel cas dans le produit $P_n(x)Q_n(x)$, il ne sert à rien de considérer les termes de degré supérieur à n (comme par exemple $a_1 b_n x^{n+1}\dots$). Il faut donc faire une troncature.
Finalement, on obtient :

$$f(x)g(x) = \sum_{k=0}^{n}\left(\sum_{h=0}^{k} a_h b_{k-h}\right)x^k + o(x^n)$$

□

Remarque - Multiplication de polynôme
Si les parties régulières des DL_n de f et g sont des polynômes de valuation strictement positive, le produit des DL_n de f et g donne un DL d'un ordre strictement supérieur à n, mais dont on ne peut rien dire pour $k > n$.
Il s'agit d'une multiplication polynomiale.

Exercice
Donner le DL_3 en 0 de $e^x\sqrt{1+x}$ et le DL_4 en 0 de $\sin^2 x$.

Correction
Il faut donc anticiper l'ordre du $DL(0)$ à chercher a priori pour chacune des fonctions.

$$e^x \underset{x\to 0}{=} 1+x+\frac{x^2}{2}+\frac{x^3}{6}+o(x^3) \qquad \sqrt{1+x} = 1+\frac{x}{2}-\frac{x^2}{8}+\frac{x^3}{16}+o(x^3)$$

$$e^x\sqrt{1+x} \underset{x\to 0}{=} 1+\left(1+\frac{1}{2}\right)x+\left(\frac{1}{2}+\frac{1}{2}-\frac{1}{8}\right)x^2+\left(\frac{1}{6}+\frac{1}{4}-\frac{1}{8}+\frac{1}{16}\right)x^3+o(x^3) = 1+\frac{3}{2}x+\frac{7}{8}x^2+\frac{17}{48}x^3+o(x^3)$$

et on ne va pas plus loin…
De même, au voisinage de 0

$$\sin(x) \underset{x\to 0}{=} x-\frac{1}{6}x^3+o(x^4) \quad \Rightarrow \quad \sin^2(x) \underset{x\to 0}{=} x^2-\frac{1}{3}x^4+o(x^4)$$

Proposition - Composition
Soient $f : I \to K$ où I est un intervalle de $\mathbb{R}$ contenant 0 et $\phi : J \to \mathbb{R}$ tel que $\phi(J) \subset I$ et $\lim_{x\to 0}\phi(x) = 0$.
On suppose que f admet un DL_n en 0, $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + o(x^n)$, et que ϕ admet un DL_n en 0, $\phi(x) = b_1 x + \dots + b_n x^n + o(x^n)$. Alors $f\circ\phi$ admet un DL_n en 0, obtenu en écrivant

$$\begin{aligned} f\circ\phi(x) &= a_0 + a_1(b_1 x+\dots+b_n x^n+o(x^n)) + a_2(b_1 x+\dots+b_n x^n+o(x^n))^2 \\ &\quad +\dots+a_n(b_1 x+\dots+b_n x^n+o(x^n))^n + o(x^n) \end{aligned}$$

en développant et en supprimant les termes de degré $> n$ (termes non significatifs).

Pour aller plus loin - Intérêt des polynômes
En début d'année, on a vu que l'intérêt des fonctions polynomiales n'était pas dans le fait que la somme ou le produit de fonctions polynomiales donne une fonction polynomiale, mais bien dans la stabilité par composition.

Remarque - Comment s'y prendre
En fait il s'agit, là aussi, des opérations sur les polynômes (en l'occurence la composition), puis une troncature.
Il faut bien prendre initialement des DL d'ordre n de f et ϕ pour obtenir un DL_n de $f\circ\phi$.
Il s'agit encore d'une composition de polynômes, ce qui donne bien un polynôme!

Démonstration
Comme pour l'addition, on prend d'abord l'égalité (qui est une VRAIE égalité). Puis on tronque.
□

Exercice
Donner un DL_4 en 0 de $\ln(\cos x)$.

Correction
Au voisinage de 0 :

$$\cos x \underset{x\to 0}{=} \underbrace{1-\frac{1}{2}x^2+\frac{1}{24}x^4+o(x^4)}_{u} \qquad \ln(1+u)=u-\frac{1}{2}u^2+\frac{1}{3}u^3-\frac{1}{4}u^4+o(u^4)$$

Donc (il faut vraiment anticiper !!)

$$\ln(\cos(x)) \underset{x\to 0}{=} \left(-\frac{1}{2}x^2+\frac{1}{24}x^4\right)-\frac{1}{2}\left(-\frac{1}{2}x^2\right)^2+\frac{1}{3}(0)+o(x^4)=-\frac{1}{2}x^2-\frac{1}{12}x^4+o(x^4)$$

Proposition - Inverse
Si f admet un DL_n en 0, $f(x) \underset{x\to 0}{=} a_0+a_1x+\cdots+a_nx^n+o(x^n)$, et $f(0)=a_0\neq 0$ alors $\frac{1}{f}$ admet un DL_n en 0 obtenu en écrivant

$$\begin{aligned}\frac{1}{f(x)} &\underset{x\to 0}{=} \frac{1}{f(0)}\times\frac{1}{1+\frac{a_1}{a_0}x+\frac{a_2}{a_0}x^2+\cdots+\frac{a_n}{a_0}x^n+o(x^n)}\\ &\underset{x\to 0}{=} \frac{1}{f(0)}\times\left(1-u(x)+u(x)^2+\cdots+(-1)^nu(x)^n+o(u(x)^n)\right)\\ &\text{où } u(x)\underset{x\to 0}{=}\frac{a_1}{a_0}x+\frac{a_2}{a_0}x^2+\cdots+\frac{a_n}{a_0}x^n+o(x^n),\end{aligned}$$

en développant et en supprimant les termes de degré $> n$ (termes non significatifs).

En fait, il s'agit d'un corollaire de la proposition précédente. Il faut plus le prendre comme un savoir-faire.
Exercice
Donner le DL_5 en 0 de $\tan x$.

Correction
Au voisinage de 0,

$$\begin{aligned}\tan(x) &\underset{x\to 0}{=} \frac{\sin x}{\cos x}\\ &= \frac{x-\frac{1}{6}x^3+\frac{1}{120}x^5+o(x^5)}{1-\underbrace{\left(\frac{1}{2}x^2-\frac{1}{24}x^4+o(x^5)\right)}_{=u}} \underset{x\to 0}{=} \left(x-\tfrac{1}{6}x^3+\tfrac{1}{120}x^5+o(x^5)\right)\times(1+u+u^2+u^3+u^4+u^5+o(u^5))\\ &\underset{x\to 0}{=} \left(x-\tfrac{1}{6}x^3+\tfrac{1}{120}x^5+o(x^5)\right)\left(1+\tfrac{1}{2}x^2-\tfrac{1}{24}x^4+\tfrac{1}{4}x^4+o(x^5)\right)\\ &\underset{x\to 0}{=} x+\left(\tfrac{1}{2}-\tfrac{1}{6}\right)x^3+\left(\tfrac{5}{24}-\tfrac{1}{12}+\tfrac{1}{120}\right)x^5+o(x^5)\\ &\underset{x\to 0}{=} x+\tfrac{1}{3}x^3+\tfrac{2}{15}x^5+o(x^5)\end{aligned}$$

Corollaire - $DL_3(0)$ de tan

$$\tan x \underset{0}{=} x+\frac{x^3}{3}+o(x^3)$$

Truc & Astuce pour le calcul - Méthode (Bilan)
Pour faire le $DL_n(a)$ de f.

1. On évalue (rapidement) la valeur numérique de $f(a)$ (elle peut être nulle ou non).
   On garde le résultat auprès de soi.
2. On fait le changement de variable
   — $x=a+h$ avec $x\to a$ ssi $h\to 0$ pour $a\in\mathbb{R}$
   — $x=\frac{1}{y}$ avec $x\to\infty$ ssi $y\to 0$ pour $a=\pm\infty$
3. On factorise par $f(a)$.
   Selon la nature de f, il peut y avoir des simplification.
   Normalement, on retrouve nécessairement des $DL_n(0)$ connus de fonctions de référence.

4. Il peut y avoir des compositions : $(1+U)^n$ ou $\frac{1}{1+U}$, $\ln(1+U)\ldots$ avec $U(h)\underset{h\to 0}{\longrightarrow}0$.
   On exploite les résultats de composition, avec U, dans un premier temps, remplacé ensuite par sa valeur.
5. Beaucoup de développements. On fait comme d'habitude : on n'écrit pas trop, et on associe directement les coefficients associés au même monôme h^k.

3.5. Généralisation

Définition - Développement limité généralisé
On dit que f admet un développement limité généralisé à l'ordre n s'il existe $Q,R\in K[X]$, $P,S\in K_n[X]$ tels que :

$$\begin{aligned}&\text{en } 0,\ f(x)=Q\left(\frac{1}{x}\right)+P(x)+o(x^n)\\ &\text{en } \pm\infty,\ f(x)=R(x)+S\left(\frac{1}{x}\right)+o\left(\frac{1}{x^n}\right)\end{aligned}$$

c'est-à-dire s'il existe $p\in\mathbb{N}^*$ (= $\deg Q$ ou $\deg R$) tel que, $x^pf(x)$ en 0, $\frac{1}{x^p}f(x)$ en $\pm\infty$, admette un DL_{n+p}

Exemple - Retour sur l'exemple original : $\frac{e^x-1}{\sin x}$ autour de $x=-\pi$
On note $u=x+\pi$, ainsi $x\to-\pi\iff u\to 0$. On s'intéresse à

$$\begin{aligned}\frac{e^{u-\pi}-1}{\sin(u-\pi)} &\underset{x\to\pi}{=} \frac{e^{-\pi}e^u-1}{-\sin(u)}=\frac{e^{-\pi}(1+u+\frac{u^2}{2}+o(u^2))-1}{-u+\frac{u^3}{6}+o(u^3)}\\ &\underset{x\to\pi}{=} \frac{(e^{-\pi}-1)+e^{-\pi}u+\frac{e^{-\pi}}{2}u^2+o(u^2)}{-u(1-\frac{1}{6}u^2+o(u^2))}\\ &\underset{x\to\pi}{=} \frac{-1}{u}\times\frac{(e^{-\pi}-1)+e^{-\pi}u+\frac{e^{-\pi}}{2}u^2+o(u^2)}{(1-\frac{1}{6}u^2+o(u^2))}\\ &\underset{x\to\pi}{=} \frac{-1}{u}\times\left(e^{-\pi}-1+e^{-\pi}u+\tfrac{e^{-\pi}}{2}u^2+o(u^2)\right)\left(1+\tfrac{1}{6}u^2+o(u^2)\right)\\ &\underset{x\to\pi}{=} \frac{-1}{u}\times\left(e^{-\pi}-1\right)+e^{-\pi}u+\left(\tfrac{e^{-\pi}}{2}+\tfrac{e^{-\pi}-1}{6}\right)u^2+o(u^2)\\ &\underset{x\to\pi}{=} \frac{1-e^{-\pi}}{u}-e^{-\pi}+\tfrac{1-4e^{-\pi}}{6}u+o(u)\end{aligned}$$

On a un développement limité généralisé

Définition - Développement asymptotique
On dit que f admet un développement aymptotique en $a\in\overline{\mathbb{R}}$ si f peut s'écrire

$$f(x)=f_0(x)+f_1(x)+\cdots+f_n(x)+o(f_n(x))$$

où pour tout k, $f_k(x)\underset{a}{=}o(f_{k-1}(x))$.
On peut par exemple avoir $f_k(x)=g(x)^k$ où $g(x)$ est une fonction qui tend vers 0 en a ($g(x)=x^\alpha$ en 0 ($\alpha>0$), $g(x)=e^{-x}$ en $+\infty$...).
$f_n(x)$ s'appelle la précision du DA.

Exercice
Déterminer un DA en 0 de $\left(1+\frac{1}{x}\right)^x$ à la précision $x\ln x$, puis à la précision x^3.

Correction
On exploite toujours la fonction exponentielle :

$$\left(1+\frac{1}{x}\right)^x=\exp\left(x\ln(1+\tfrac{1}{x})\right)=\exp\left(x\ln(1+x)-x\ln x\right)$$

Au voisinage de 0, comme $x\ln x \to 0$,

$$\left(1+\frac{1}{x}\right)^x = \exp(-x\ln x)\times\exp(x\ln(1+x)) = (1-x\ln x+\frac{1}{2}x^2\ln^2 x-\frac{1}{6}x^3\ln^3 x+o(x^3\ln^3 x))\times\exp(x^2-\frac{1}{2}x^3+o(x^3))$$

$$= (1-x\ln x+\frac{1}{2}x^2\ln^2 x-\frac{1}{6}x^3\ln^3 x+o(x^3\ln^3 x))\times(1+x^2-\frac{1}{2}x^3+o(x^3))$$

$$= 1-x\ln x+\frac{1}{2}x^2\ln^2 x+x^2-\frac{1}{6}x^3\ln^3(x)-x^3\ln x-\frac{1}{2}x^3+o(x^3)$$

4. Applications des DL

4.1. Recherche de limites et d'équivalents (suite ou fonction)

Savoir faire - La force des développements limités

Les DL permettent d'avoir un équivalent (premier terme non nul) et, contrairement aux équivalents, ils peuvent être additionnés. C'est donc un outil "plus sûr" dans son maniement. L'équivalent permet ensuite d'avoir la limite.

On commence toujours par se ramener en 0 pour utiliser les DL usuels.

Exercice

Déterminer $\lim\limits_{x\to 0}\left(\frac{1}{1+x^2}-\cos x\right)\frac{1}{x^2}$.

Correction

Assez simplement :

$$\frac{1}{1+x^2}-\cos x = (1-x^2)-(1-\frac{1}{2}x^2)+o(x^2)$$

Donc $\lim\limits_{x\to 0}\left(\frac{1}{1+x^2}-\cos x\right)\frac{1}{x^2} = -\frac{1}{2}$

Exercice

Déterminer un équivalent de la suite (u_n) définie par $u_n = \left(1+\frac{1}{n}\right)^n - e$.

Correction

Par composition,

$$\left(1+\frac{1}{n}\right)^n = \exp\left(n\ln(1+\frac{1}{n})\right) = \exp\left(1-\frac{1}{2n}+o(\frac{1}{n})\right) = e(1-\frac{1}{2n}+o(\frac{1}{n}))$$

Donc $u_n \sim \frac{-e}{2n}$

Exercice

Déterminer $\lim\limits_{x\to\frac{\pi}{6}}\left(\tan\frac{3x}{2}\right)^{\frac{1}{\cos 3x}}$.

Correction

On commence par faire le changement de variable $h = x-\frac{\pi}{6}$, donc $x = h+\frac{\pi}{6}$.

$\cos(3x) = \cos(3h+\frac{\pi}{2}) = -\sin(3h)$ et $\tan\frac{3x}{2} = \tan\left(\frac{3}{2}h+\frac{\pi}{4}\right) = \frac{\tan\frac{3}{2}h+1}{1-\tan\frac{3}{2}h}$ On exploite la fonction exponentielle :

$$\left(\tan\frac{3x}{2}\right)^{\frac{1}{\cos 3x}} = \exp\left(\frac{-1}{\sin 3h}\left(\ln(1+\tan\frac{3}{2}h)-\ln(1-\tan\frac{3}{2}h)\right)\right)$$

$$= \exp\frac{-(3h+o(h))}{3h+o(h)} = \frac{1}{e}(1+o(h))$$

Donc $\lim\limits_{x\to\frac{\pi}{6}}\left(\tan\frac{3x}{2}\right)^{\frac{1}{\cos 3x}} = \frac{1}{e}$

4.2. Etude locale d'une fonction

Savoir faire - Etude locale d'une courbe au voisinage d'un point

Les DL permettent d'avoir directement des résultats sur le comportement local d'une fonction plus précis que la limite ou l'équivalent en un point.

Tangentes et position, extremum local

Proposition - Exploitation graphique d'un DL en a

Si f admet en a un DL_k ($k\geqslant 2$) de la forme

$$f(x) = a_0+a_1(x-a)+a_k(x-a)^k+o((x-a)^k)$$

alors f est prolongeable par continuité en a, de prolongement dérivable en a, l'équation de la tangente à $\mathscr{C}_f$ en a est $y = a_0+a_1(x-a)$, le signe de a_k et la parité de k donnent, localement, au voisinage de a, les positions relatives de la tangente et de la courbe, des conditions pour avoir un extremum local.

Remarque - « Seulement » un DL d'ordre 1

Un DL_1 donne le prolongement par continuité, la dérivabilité et l'équation de la tangente, mais ne permet pas d'avoir les positions relatives de la tangente et de la courbe car le signe de $o(x-a)$ est inconnu.

Exercice

Soit f la fonction définie par $f(x) = \frac{x^2-1}{x\ln x}$. Quel est son domaine de définition ?

Montrer qu'elle se prolonge de manière continue et dérivable en 1. Donner l'équation de la tangente ainsi que les positions relatives de la tangente et de la courbe.

Préciser également le comportement de f aux autres bornes du domaine de définition.

Correction

$\mathscr{D}_f = \mathbb{R}_+^*\setminus\{1\}$, on pose $x = 1+h$, On cherche à obtenir un DL d'ordre 2. Puisqu'il y aura une factorisation par h, on prend un DL_3 au dénominateur :

$$f(x) = f(1+h) = \frac{2h+h^2}{(1+h)\ln(1+h)} = \frac{2h+h^2}{(1+h)(h-\frac{h^2}{2}+\frac{h^3}{3}+o(h^3))} = \frac{2+h}{1+\frac{1}{2}h-\frac{1}{6}h^2+o(h^2)}$$

$$= (2+h)(1-\frac{1}{2}h+\frac{1}{6}h^2+\frac{1}{4}h^2+o(h^2)) = 2+\frac{5}{6}h^2-\frac{1}{2}h^2+o(h^2) = 2-\frac{1}{3}h^2+o(h^2)$$

Donc f est prolongeable en 1 et $f(1) = 2$, $f'(1) = 0$ et f au-dessous la tangente ($y = 2$) pour $x > 1$ et au-dessous pour $x < 1$ *On aurait pu aussi exploiter la règle de L'hopital :* $\lim\limits_1 f = \lim\limits_{x\to 1}\frac{2x}{1+\ln x} = 2$.

Asymptotes et position

Proposition - Exploitation graphique d'un DL en ∞

Si f admet en ∞ un développement limité généralisé d'ordre k ($k\geqslant 1$) de la forme

$$f(x) = ax+b+\frac{c}{x^k}+o\left(\frac{1}{x^k}\right)$$

alors $\mathscr{C}_f$ admet une asymptote d'équation $y = ax+b$, le signe de c et la parité de k donnent, localement, au voisinage de $+(-)\infty$, les positions relatives de l'asymptote et de la courbe.

Remarque - « Seulement » un DL d'ordre 0

Un développement limité généralisé à l'ordre 0 donne l'asymptote, mais ne permet pas d'avoir les positions relatives de la tangente et de la courbe.

Exercice

Soit f la fonction définie par $f(x) = (x^2-1)\ln\frac{x-1}{x+1}$.

Quel est son domaine de définition ?

Montrer que $\mathscr{C}_f$ admet une asymptote en $+\infty$ dont on donnera l'équation ainsi que la position relative par rapport à la courbe.

Correction

$\mathscr{D}_f =]-\infty,-1[\cup]1,+\infty[$.

On pose $h = \frac{1}{x}$, on a

$$f(x) = (\frac{1}{h^2}-1)\ln\frac{1-h}{1+h} = \frac{1-h^2}{h^2}(\ln(1-h)-\ln(1+h))$$

$$= \frac{1-h^2}{h^2}\left(-h-\frac{1}{2}h^2-\frac{1}{3}h^3-h+\frac{1}{2}h^2-\frac{1}{3}h^3+o(h^3)\right)$$

$$= \frac{1}{h}(1-h^2)(-2-\frac{2}{3}h^2+o(h^2)) = \frac{1}{h}(-2+\frac{4}{3}h^2+o(h^2))$$
$$= -2x+\frac{4}{3x}+o\frac{1}{x}$$

$\mathscr{C}_f$ admet une asymptote d'équation $y=-2x$.
La courbe se trouve au-dessus de l'asymptote.

5. Bilan

Synthèse

⇝ Nous apprenons ici à remplacer localement une fonction par une expression plus simple (polynomiale la plupart du temps) et facile à étudier.
Cela est assez technique et calculatoire, mais également très puissant!
On commence toujours par se demander où est-ce qu'on se trouve!

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Avec une fonction « relative »
- Savoir-faire - Etude de négligeabilité/équivalence/domination... d'une suite.
- Savoir-faire - Obtenir un $DL_n(a)$ d'une fonction f
- Savoir-faire - DL des fonctions de références en d'autres points (que 0)
- Truc & Astuce pour le calcul - Méthode (Bilan)
- Savoir-faire - La force des développements limités
- Savoir-faire - Etude locale d'une courbe au voisinage d'un point

Notations

	Propriétés	*Remarques*
es racine de g	$\mathcal{Z}(g)=g^{-1}(\{0\})=[g=0]=\{x \mid g(x)=0\}$	
eable devant g au voisinage de	$\forall \epsilon>0, \exists V\in\mathcal{V}_a \mid \forall x\geqslant V, \lvert f(x)\rvert\leqslant\epsilon\lvert g(x)\rvert$	si $\mathcal{Z}(g)\cap V\subset\mathcal{Z}(f)$, équivalent à $\lim\limits_{x\to a, x\notin\mathcal{Z}(g)}\frac{f(x)}{g(x)}=0$
ılente à g au voisinage de a	$\forall \epsilon>0, \exists V\in\mathcal{V}_a \mid \forall x\geqslant V, \lvert f(x)+g(x)\rvert\leqslant\epsilon\lvert g(x)\rvert$	si $\mathcal{Z}(g)\cap V\subset\mathcal{Z}(f)$, équivalent à $\lim\limits_{x\to a, x\notin\mathcal{Z}(g)}\frac{f(x)}{g(x)}=1$
ıée par g au voisinage de a	$\exists M>0, \exists V\in\mathcal{V}_a \mid \forall x\geqslant V, \lvert f(x)\rvert\leqslant M\lvert g(x)\rvert$	si $\mathcal{Z}(g)\cap V\subset\mathcal{Z}(f)$, équivalent à $\frac{f(x)}{g(x)}$ bornée sur $\mathcal{Z}(g)\cap V$
nent limité d'ordre n de f au e a	$\exists P\in\mathbb{R}_n[X] \mid f(x)\underset{a}{=}P(x-a)+o((x-a)^n)$	

Retour sur les problèmes

147. $f(x)=\dfrac{e^x-1}{\sin x}$.
Au voisinage de 0 : $e^x-1=x+\frac{1}{2}x^2+\frac{1}{6}x^3+\frac{1}{24}x^4+o(x^4)$ et $\sin x=x-\frac{x^3}{6}+o(x^4)$. On simplifie par x.
$$f(x)=\frac{1+\frac{1}{2}x+\frac{1}{6}x^2+\frac{1}{24}x^3+o(x^3)}{1-\frac{1}{6}x^2+o(x^3)}$$
$$=(1+\tfrac{1}{2}x+\tfrac{1}{6}x^2+\tfrac{1}{24}x^3+o(x^3))(1+\tfrac{1}{6}x^2+o(x^3))$$
$$=1+\tfrac{1}{2}x+\tfrac{1}{2}x^2+\tfrac{1}{8}x^3+o(x^2).$$
Au voisinage de $-\pi$: $\sin(x)=\sin(-\pi+h)=-\sin h=-h+\frac{1}{6}h^3+o(h^4)$.
$$e^x-1=e^{-\pi+h}-1=e^{-\pi}e^h-1=e^{-\pi}(1+h+\tfrac{1}{2}h^2+\tfrac{1}{6}h^3+o(h^3))-1.$$
$$f(x)=\frac{-1}{h}\frac{e^{-\pi}-1+e^{-\pi}h+\frac{e^{-\pi}}{2}h^2+\frac{e^{-\pi}}{6}h^3+o(h^3)}{1-\frac{1}{6}h^2+o(h^3)}$$
$$=\frac{1-e^{-\pi}}{h}-e^{-\pi}+\frac{1-4e^{-\pi}}{6}h+o(h)$$

Cinquième partie

Algèbre linéaire & bilinéaire

Chapitre 24

Espaces vectoriels

Résumé -

Les espaces vectoriels sont aujourd'hui la structure principale (ou première) de tout cours de mathématiques spéciales dans le monde. Il y a (au moins deux raisons) : la première est historique : c'est le lien qu'ils jouent naturellement avec la géométrie (en toute dimension). Mais pour nous c'est la seconde raison qui est prioritaire : c'est le lieu de la linéarité. Or la science physique (actuelle) est la science de la linéarité. Les espaces vectoriels sont donc parfaitement adaptés au co-développement maths/physique.

Dans l'ensemble de ce chapitre : on opère sur ces structures ou les sous-espaces induits (image par application linéaire, addition et intersection) ou sur ces objets (combinaison linéaire, génératrice et/ou indépendante)…

Sommaire

1. Problèmes 464
2. Structure d'espace vectoriel 465
2.1. Loi de composition externe 465
2.2. Exemples fondamentaux d'espaces vectoriels 466
2.3. Combinaisons linéaires 467
3. Sous-espaces vectoriels 468
3.1. Définition et caractérisation 468
3.2. Exemples 469
3.3. Sous-espace vectoriel engendré par une partie . . . 470
3.4. Somme de sous-espaces vectoriels 472
4. Applications linéaires 475
4.1. Définitions et exemples 475
4.2. Cas général : structure de $\mathscr{L}(E,F)$ 477
4.3. Cas particulier de $\mathscr{L}(E)$ 478
4.4. Projecteurs et symétries 480
5. Familles de vecteurs 482
5.1. Sur-famille, sous-famille 482
5.2. Familles génératrices de E 482
5.3. Familles libres, liées 484
5.4. Image d'une famille de vecteurs par une application linéaire 486
6. Bilan 487

1. Problèmes

Problème 101 - Structure de la géométrie vectorielle

En physique, on travaille beaucoup avec des vecteurs (forces, positions…). Ces vecteurs peuvent être de dimension 2, 3, voire 6 (dans l'espace des phases…).
En mathématiques, on aime dégager les objets de leur histoire pour retenir que la structure sous-jacente.
Si on appelle espace vectoriel, un ensemble de vecteurs et les opérations que l'on peut poser sur cet ensemble, que peut être (que doit être) un espace vectoriel?
Puis existe-t-il d'autres problèmes physiques ou mathématiques dans lesquels les espaces vectoriels peuvent être les bons cadres d'étude?

Problème 102 - Sous-espaces vectoriels

On suppose que F et G sont des espaces vectoriels (inclus dans un même espace vectoriel). Ils sont donc stables par combinaison linéaire.
A quelle condition, l'ensemble $F \cap G$ est un espace vectoriel?
A quelle condition, l'ensemble $F \cup G$ est un espace vectoriel?

Problème 103 - Anneau de sous-espaces vectoriels

Si L, M, N sont des sous-espaces vectoriels d'un espace E, a-t-on

$$L \cap (M + (L \cap N)) = (L \cap M) + (L \cap N)$$

$$L \cap (M + N) = (L \cap M) + (L \cap N)$$

Problème 104 - Application qui conserve la structure

On considère $f : E \to F$, une application f d'un espace vectoriel E dans un espace vectoriel F.
E, comme F, sont des structures assez rigides (espace vectoriel) dont la particularité est la stabilité par la combinaison linéaire.
Quelles propriétés donner à f, pour que la structure rigide se transporte de E à F par f?
A quelle condition simple nécessaire et/ou suffisante peut-on affirmer que f est surjective, resp. injective?

Problème 105 - Projection

En début d'année, nous avons vu qu'il est pratique d'avoir pour une décomposition $E = F \uplus G$, des applications $\mathbf{1}_F$ et $\mathbf{1}_G$, ainsi, on peut décomposer tout x de F en $x = \mathbf{1}_F(x) \times x + \mathbf{1}_G(x) \times x$ et éviter d'étudier des sous-cas… Pour les espaces vectoriels, nous voyons que les ensembles (espaces) se décomposent plutôt en somme qu'en réunion : $E = F \oplus G$. Il faudrait pouvoir alors, envoyer la partie sur F et celle sur G. Comment définir proprement deux applications $f : E \to F$ et $g : E \to G$, telles que $\forall\, x \in E,\ x = f(x) + g(x)$? Unique(s)?

2. Structure d'espace vectoriel

2.1. Loi de composition externe

Définition - Loi de composition externe
Soit $\mathbb{K}$ un corps. Une **loi de composition externe sur** E à domaine d'opérateurs $\mathbb{K}$ est une application de $\mathbb{K} \times E$ dans E (on la note généralement par un point) :

$$\begin{array}{ll} \mathbb{K} \times E & \to E \\ (\lambda, x) & \mapsto \lambda \cdot x \end{array}$$

Définition - Espace vectoriel
Soit $\mathbb{K}$ un corps commutatif. On appelle **$\mathbb{K}$-espace vectoriel** (notation $\mathbb{K}$-e.v.) ou **espace vectoriel sur** $\mathbb{K}$ tout triplet $(E, +, \cdot)$ formé d'un ensemble E, d'une loi interne $+$ sur E et d'une loi externe $\cdot$ sur E à domaine d'opérateurs $\mathbb{K}$ tel que :
• $(E, +)$ est un groupe commutatif
• Et on a les quatre propriétés suivantes :
$\forall (\alpha, \beta) \in \mathbb{K}^2$, $\forall (x, y) \in E^2$,

$$\begin{array}{l} \alpha \cdot (\beta \cdot x) = (\alpha\beta) \cdot x \\ (\alpha + \beta) \cdot x = (\alpha \cdot x) + (\beta \cdot x) \\ \alpha \cdot (x + y) = (\alpha \cdot x) + (\alpha \cdot y) \\ 1 \cdot x = x \end{array}$$

Les éléments de E s'appellent des vecteurs.
Les éléments de $\mathbb{K}$ s'appellent des scalaires.
L'élément neutre de E pour $+$ s'appelle le vecteur nul, il est noté 0_E ou $\vec{0_E}$.
Par abus de langage on dira que E est un $\mathbb{K}$-e.v. (à la place de $(E, +, \cdot)$ est un $\mathbb{K}$-e.v.)

Pour aller plus loin - Notation et point de vue géométrique
Jusqu'à maintenant les vecteurs rencontrés en mathématiques (et souvent en physique) s'écrivent plutôt $\vec{AB}$ ou $\vec{x}$. Cela permet de bien faire la différence avec la notation des nombres (scalaire) $k \in \mathbb{K}$ dans l'écriture $k \cdot \vec{x}$.
On peut plaider pour conserver cette notation :
- *C'est visuel : on ne confond pas les deux types d'objets*
- *Cela donne un vrai sens géométrique à ce cours d'algèbre linéaire*

Mais malheureusement, comme cela est un peu réducteur (le point de vue géométrique), on préférera l'écriture sans flèche. On notera plutôt en lettres grecs les scalaires et en lettres latines les vecteurs : $\lambda \cdot x$ (en science physique, on note souvent en gras les vecteurs : $k \cdot \mathbf{x}$)…
Le point de vue géométrique n'est néanmoins pas à bannir. Il s'agit « seulement » d'une forme particulière incarnation des espaces vectoriels (mais il permet aussi de voir les choses).

Remarque - Corps $\mathbb{K}$
Dans la suite on s'intéressera presqu'exclusivement au cas où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Ce sont les cas figurants au programme, mais la définition peut s'étendre à d'autres cas, par exemple $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K} = \mathbb{F}_p (= \frac{\mathbb{Z}}{p\mathbb{Z}})$.

Proposition - Premières propriétés
Soit E un $\mathbb{K}$-espace vectoriel. Pour $x \in E$ et $\lambda \in \mathbb{K}$ on a :

$$\begin{array}{l} 0 \cdot x = 0_E \\ (-1) \cdot x = -x \\ \lambda \cdot (-x) = (-\lambda) \cdot x = -(\lambda \cdot x) \\ \lambda \cdot 0_E = 0_E \\ \lambda \cdot x = 0_E \Leftrightarrow \lambda = 0 \text{ ou } x = 0_E \end{array}$$

Pour aller plus loin - Module
On appelle A-module, un ensemble $(F, +, \cdot)$ muni des mêmes propriétés que E, espace vectoriel, à la différence que A est un anneau et non un corps.
Cela n'est pas sans conséquence sur la question des bases, dont nous reparlerons plus loin. A part cela, il y a beaucoup de points communs

Démonstration
Pour tout $x \in E$, on notera que $1 \cdot x = x$.
- $x = 1 \cdot x = (0 + 1) \cdot x = 0 \cdot x + 1 \cdot x = 0 \cdot x + x$ donc $0 \cdot x = 0_E$, nécessairement
- $0_E = 0 \cdot x = (1 + (-1)) \cdot x = x + (-1) \cdot x$, donc $(-1) \cdot x = -x$.
- De même : $0_E = 0 \cdot x = (\lambda + (-\lambda)) \cdot x = \lambda x + (-\lambda) \cdot x$, donc $(-\lambda) \cdot x = -\lambda \cdots x$.
- $\lambda \cdot (-x) = [\lambda \cdot (-1)] \cdot x = (-\lambda) \cdot x$
- Et donc Et $0_E = \lambda \cdot x + \lambda \cdot (-x) = \lambda \cdot (x - x) = \lambda \cdot 0_E$

- Supposons que $\lambda \cdot x = 0_E$.
  Si $\lambda \neq 0$, on a donc $0_E = \lambda^{-1} \cdot 0_E = (\lambda^{-1}) \cdot \lambda \cdot x = 1 \cdot x = x$,
  car $\lambda \in \mathbb{K}$, corps, donc λ inversible.
  Et par conséquent, $x = 0_E$.
  Donc ou bien $\lambda = 0_{\mathbb{K}}$ ou bien $x = 0_E$.

□

2.2. Exemples fondamentaux d'espaces vectoriels

Proposition - Espace vectoriel des matrices
$\mathcal{M}_{n,p}(\mathbb{K}), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Démonstration
Vu dans le cours sur les matrices □

Proposition - Espace vectoriel des polynômes
$\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel.

Démonstration
$\mathbb{K}[X]$ a été construit pour cela, c'est même mieux : une algèbre (un mélange d'espace vectoriel et anneau). □

Proposition - Espaces produits
Soient $E_1, \ldots, E_n$ des $\mathbb{K}$-e.v. (avec le même corps $\mathbb{K}$). On définit sur $E = E_1 \times E_2 \times \cdots \times E_n$ les lois $+$ et $\cdot$ par :

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 \underset{E_1}{+} y_1, x_2 \underset{E_2}{+} y_2, \ldots, x_n \underset{E_n}{+} y_n)$$

$$\lambda \cdot (x_1, \ldots, x_n) = (\lambda \underset{E_1}{\cdot} x_1, \ldots, \lambda \underset{E_n}{\cdot} x_n)$$

Alors $(E, +, \cdot)$ est un $\mathbb{K}$-e.v., de vecteur nul $(0_{E_1}, \ldots, 0_{E_n})$.

Remarque - Application classique
On utilise généralement ce résultat avec des E_i sous-espaces vectoriels (cf paragraphe suivant) d'un même espace vectoriel E, voire égaux, mais ce n'est pas obligatoire.
Exercice
A démontrer

Correction
Il s'agit d'un « jeu » d'écriture.
$\mathbb{K}$ muni de la loi interne $+$ et de la loi $\times$ comme loi externe à domaine d'opérateurs $\mathbb{K}$ étant un $\mathbb{K}$-e.v. on en déduit que

Corollaire - Exemple crucial!
$\mathbb{K}^n$ est un $\mathbb{K}$-e.v de vecteur nul $(0, \ldots, 0)$: $\mathbb{R}^n$ est un $\mathbb{R}$-e.v. et $\mathbb{C}^n$ est un $\mathbb{C}$-e.v.

Exercice
Montrer que $\mathbb{C}^n$ est également un $\mathbb{R}$-e.v.

Correction
On a :

$$\mathbb{R} \times \mathbb{C}^n \to \mathbb{C}^n, \qquad (\lambda, x) \mapsto \lambda \times x$$

Définition - Famille presque nulle
On considère un espace vectoriel E défini sur un corps $\mathbb{K}$ ($\mathbb{K}$ lui-même par exemple).
On dit qu'une famille $(y_i)_{i \in I}$ d'éléments de E est presque nulle, si $\{i \in I \mid y_i \neq 0\}$ est fini.

On note alors $E^{(I)}$ cet ensemble (des familles de E presque nulle).
Alors $(E^{(I)},+,\cdot)$ est un espace vectoriel

Exercice
On a $(y_i)+(z_i)=(y_i+z_i)$. A démontrer

Correction

Exemple - $\mathbb{K}^{(\mathbb{N})}$
L'ensemble des familles presque nulles de $\mathbb{K}$ indexés sur $\mathbb{N}$ est isomorphe à l'ensemble des polynômes $\mathbb{K}[X]$.

Proposition - Espaces de fonctions
Soit E un $\mathbb{K}$-e.v. et X un ensemble quelconque. On munit $\mathscr{F}(X,E)$ des lois $+$ et $\cdot$ définies par :

$$f+g:\ \begin{array}{l}X\to E\\ x\mapsto f(x)\underset{E}{+}g(x)\end{array} \quad\text{et}\quad \lambda\cdot f:\ \begin{array}{l}X\to E\\ x\mapsto \lambda\underset{E}{\cdot} f(x)\end{array}$$

Alors : $(\mathscr{F}(X,E),+,\cdot)$ est un $\mathbb{K}$-e.v. (pour E $\mathbb{K}$-e.v.) d'élément neutre l'application nulle (application constante égale à 0_E).

Démonstration
$(\mathscr{F}(X,E),+)$ est un groupe commutatif d'élément neutre l'application nulle. De plus :
$\forall(\alpha,\beta)\in\mathbb{K}^2$, $\forall(f,g)\in\mathscr{F}^2=\mathscr{F}(X,E)^2$, on a pour tout $x\in X$:

$$\begin{aligned}
\big(\alpha\underset{\mathscr{F}}{\cdot}(\beta\underset{\mathscr{F}}{\cdot}f)\big)(x)&=\alpha\underset{E}{\cdot}(\beta\underset{E}{\cdot}f(x)) \text{ par définition (appliquée deux fois) de } \underset{\mathscr{F}}{\cdot}\\
&=(\alpha\beta)\underset{E}{\cdot}f(x) \text{ car } E \text{ est un } \mathbb{K}-e.v.\\
&=\big((\alpha\beta)\underset{\mathscr{F}}{\cdot}f\big)(x) \text{ par définition de } \underset{\mathscr{F}}{\cdot}\\
\big((\alpha\underset{\mathbb{K}}{+}\beta)\underset{\mathscr{F}}{\cdot}f\big)(x)&=(\alpha\underset{\mathbb{K}}{+}\beta)\underset{E}{\cdot}f(x) \text{ par définition de } \underset{\mathscr{F}}{\cdot}\\
&=\alpha\underset{E}{\cdot}f(x)\underset{E}{+}\beta\underset{E}{\cdot}f(x) \text{ car } E \text{ est un } \mathbb{K}-e.v.\\
&=(\alpha\underset{\mathscr{F}}{\cdot}f)(x)\underset{E}{+}(\beta\underset{\mathscr{F}}{\cdot}f)(x) \text{ par définition de } \underset{\mathscr{F}}{+}\\
&=\big(\alpha\underset{\mathscr{F}}{\cdot}f\underset{\mathscr{F}}{+}\beta\underset{\mathscr{F}}{\cdot}f\big)(x) \text{ par définition de } \underset{\mathscr{F}}{+}
\end{aligned}$$

Ces résultats étant vrais pour tout élément de X, ensemble de départ commun aux applications $\alpha\underset{\mathscr{F}}{\cdot}(\beta\underset{\mathscr{F}}{\cdot}f)$ et $(\alpha\beta)\underset{\mathscr{F}}{\cdot}f$ d'une part, et $(\alpha\underset{\mathbb{K}}{+}\beta)\underset{\mathscr{F}}{\cdot}f$ et $\alpha\underset{\mathscr{F}}{\cdot}f\underset{\mathscr{F}}{+}\beta\underset{\mathscr{F}}{\cdot}f$ d'autre part (qui ont même ensemble d'arrivée E), on en déduit que

$$\alpha\underset{\mathscr{F}}{\cdot}(\beta\underset{\mathscr{F}}{\cdot}f)=(\alpha\beta)\underset{\mathscr{F}}{\cdot}f$$

$$(\alpha\underset{\mathbb{K}}{+}\beta)\underset{\mathscr{F}}{\cdot}f=\alpha\underset{\mathscr{F}}{\cdot}f\underset{\mathscr{F}}{+}\beta\underset{\mathscr{F}}{\cdot}f$$

On démontre de même que $\alpha\underset{\mathscr{F}}{\cdot}(f\underset{\mathscr{F}}{+}g)=\alpha\underset{\mathscr{F}}{\cdot}f\underset{\mathscr{F}}{+}\alpha\underset{\mathscr{F}}{\cdot}g$ et que $1\underset{\mathscr{F}}{\cdot}f=f$.
On en déduit que $(\mathscr{F}(X,E),+,\cdot)$ est un $\mathbb{K}$-e.v. □

Analyse - Cas particuliers
Pour $X=I$ intervalle de $\mathbb{R}$ on obtient que $\mathscr{F}(I,\mathbb{R})$ est un $\mathbb{R}$-e.v. (on peut remplacer $\mathbb{R}$ par $\mathbb{C}$)
Pour $X=\mathbb{N}$ on obtient que $\mathbb{R}^{\mathbb{N}}$ est un $\mathbb{R}$-e.v. (on peut remplacer $\mathbb{R}$ par $\mathbb{C}$)
Pour $X=E$ $\mathbb{K}$-e.v. on obtient que $\mathscr{F}(E,E)$ est un $\mathbb{K}$-e.v.

Corollaire - Exemples multiples
$\mathscr{F}(I,\mathbb{K})$ (I intervalle de $\mathbb{R}$), $\mathbb{K}^{\mathbb{N}}$ sont des $\mathbb{K}$-espaces vectoriels.

2.3. Combinaisons linéaires

Soit E un $\mathbb{K}$-e.v.

Histoire - Du sens (physique) de $\mathbb{R}^n$ ***avec*** $n\geqslant 4$
Cela a-t-il un sens « physique » de s'intéresser à un espace vectoriel de dimension $n>5$? La relativité nous fait voir l'espace-temps comme un ensemble à 4 dimensions et ensuite ?
Pour le mathématicien la question ne se pose pas…
Et pourtant, la mathématique et la physique ont partie liée ; l'histoire montre que les coups l'un de l'autre ne conduit que vers un assèchement (même si les acteurs ont souvent un penchant pour l'une ou pour l'autre).
Alors nous répondrons à la question : l'espace des phases d'un objet de N molécules n'est-il pas de dimension $6N$?

Définition - Combinaison linéaire
On dit que $x\in E$ est combinaison linéaire de la famille finie $(x_1,\dots,x_n)$ d'éléments de E s'il existe $(\lambda_1,\dots,\lambda_n)\in\mathbb{K}^n$ tel que

$$x=\lambda_1\cdot x_1+\lambda_2\cdot x_2+\dots+\lambda_n\cdot x_n$$

Proposition - Stabilité linéaire
Si x et y sont combinaisons linéaires de la famille $(x_1,\dots,x_n)$
alors pour tout $(\lambda,\mu)\in\mathbb{K}^2$, $\lambda\cdot x+\mu\cdot y$ est combinaison linéaire de la famille $(x_1,\dots,x_n)$.
Plus généralement, toute combinaison linéaire de vecteurs qui sont des combinaisons linéaires de la famille $(x_1,\dots,x_n)$ est une combinaison linéaire de la famille $(x_1,\dots,x_n)$.

Histoire - Grassmann



C'est à Hermann Grassmann (1809-1877), mathématicien d'origine allemande que l'on doit la formalisation des espaces vectoriels (ainsi que la plupart des résultats de ce cours). Ces idées datent de 1844 : Théorie de l'extension linéaire. Mais il a totalement été oublié par la postérité mathématique avant de réapparaitre au milieu du XX^e siècle. Sa vie, à lui également, pourrait faire l'objet d'un biopic…

Démonstration
On a $x=\sum_{i=1}^{n}\lambda_i\cdot x_i$ et $y=\sum_{i=1}^{n}\mu_i\cdot x_i$, donc par propriété des lois $+$ et $\cdot$ on obtient

$$\lambda\cdot x+\mu\cdot y=\lambda\cdot\sum_{i=1}^{n}\lambda_i\cdot x_i+\mu\cdot\sum_{i=1}^{n}\mu_i\cdot x_i=\sum_{i=1}^{n}(\lambda\lambda_i+\mu\mu_i)\cdot x_i$$

et donc $\lambda\cdot x+\mu\cdot y$ est combinaison linéaire de la famille $(x_1,\dots,x_n)$.
Par récurrence, on généralise à une combinaison linéaire d'un nombre quelconque de vecteurs.
□

Définition - Généralisation : combinaison linéaire de famille
Soit I un ensemble infini et $(x_i)_{i\in I}$ une famille d'éléments de E.
On dit que $x\in E$ est combinaison linéaire de la famille $(x_i)_{i\in I}$ s'il est combinaison linéaire d'un nombre **fini** d'éléments de cette famille.
Ce qui peut aussi s'écrire : il existe une famille presque nulle (ou à support compact) $(\lambda_i)_{i\in I}$ (c'est-à-dire comportant seulement un nombre fini de λ_i non nuls) telle que $x=\sum_{i\in I}\lambda_i\cdot x_i$. Ou encore, il existe $J\subset I$, fini et $(\lambda_i)_{i\in J}$ tel que $x=\sum_{i\in J}\lambda_i\cdot x_j$.

3. Sous-espaces vectoriels

3.1. Définition et caractérisation

Soit $(E,+,\cdot)$ un $\mathbb{K}$-e.v.

Définition - Sous-espace vectoriel
Soit F une partie non vide de E.
On dit que F est un sous-espace vectoriel de E
si F est stable pour les deux lois $+$ et $\cdot$
et si F muni des lois induites est un $\mathbb{K}$-e.v.

Exemple - Triviaux
$\{0_E\}$ et E sont des s.e.v de E.

Proposition - Caractérisation
Soit $F\subset E$. F est un sous-espace vectoriel de E si et seulement si

(1) $F\neq\emptyset$
(2) $\forall(\lambda,\mu)\in\mathbb{K}^2,\quad\forall(x,y)\in F^2,\quad\lambda\cdot x+\mu\cdot y\in F$

La deuxième condition se traduit par « F est stable par combinaison linéaire ».

Démonstration
Si F est un sev de E, alors
F est non vide
et F est stable pour les deux lois induites,
Donc nécessairement $\forall(\lambda,\mu)\in\mathbb{K}^2, \forall(x,y)\in F^2, \underbrace{\in F}\ \underbrace{\in F}\ \lambda\cdot x+\underbrace{\in F}\ \mu\cdot y\in F$
Réciproquement,
Si F est non vide et stable par combinaison linéaire,
F est non vide, stable par addition ($\lambda=\mu=1$),
F est stable par $\cdot$ (avec $\mu=0_{\mathbb{K}}$, $y=0_E$)
Les éléments de F sont aussi des éléments de E et donc F est un $\mathbb{K}$ev. □

Remarque - Elément vide et 0_E
Si F est un sev de E, alors F est non vide est contient nécessairement 0_E.
Réciproquement, si $0_E\in F$, alors F est non vide.
Donc on peut faire évoluer « la recherche de F est-il non vide? » en « F contient-il 0_E? »
En outre, si la réponse est non, on peut affirmer que F n'est pas un sev de E (ce que ne permet pas la réponse négative à la première question).

Savoir faire - Démontrer que F est un (s.)ev (de E)
Soit $F\subset E$. F est un sous-espace vectoriel de E si et seulement si

$(1')\quad 0_E\in F$

$(2)\quad \forall(\lambda,\mu)\in\mathbb{K}^2,\quad \forall(x,y)\in F^2,\quad \lambda.x+\mu.y\in F$

Exercice
Soit $F\subset E$. Montrer que F est un sous-espace vectoriel de E si et seulement si

$(1)\quad F\neq\emptyset$

$(2)\quad \forall\lambda\in\mathbb{K},\quad \forall(x,y)\in F^2,\quad \lambda.x+y\in F$

Correction
La condition est nécessaire (on prend $\mu=1$).
La condition est également suffisante.
Soient $\lambda,\mu\in\mathbb{K}$, $x,y\in E$, alors $Y=\mu\cdot y+0_E\in F$, puis $\lambda\cdot x+Y=\lambda\cdot x+\mu\cdot y\in F$

Histoire - Petite citation
« J'ai la confiance la plus ferme que le travail que j'ai consacré à la science exposée ici et qui m'a accaparé une période importante de ma vie, réclamant une mise sous tension extrême de toutes mes forces, ne sera pas perdu.[…] je sais que même si ce travail devait rester en sommeil pendant encore dix-sept ans ou plus, sans emprise sur la Science vivante, il n'en viendra pas moins un temps où il sera tiré de la poussière de l'oubli et où les idées qu'il recèle porteront leurs fruits. […] Car la vérité est éternelle et divine, et aucune phase du développement de la vérité, si petit que soit le domaine qu'elle comprend, ne peut passer sans laisser de trace; elle perdure, même si l'habit dont des hommes faibles la revêtent tombe en poussière »
Grassmann, Théorie de l'Extension *(1862)*

3.2. Exemples

Proposition - Sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$
L'ensemble des matrices scalaire, l'ensemble des matrices diagonales, l'ensemble des matrices symétriques, l'ensemble des matrices antisymétriques, l'ensemble des matrices triangulaires supérieures, l'ensemble des matrices triangulaires inférieures sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$ (ou $\mathcal{M}_{n,p}(\mathbb{K})$).

Exercice
A démontrer

Correction

Proposition - $\mathbb{K}_n[X]$
Pour tout $n\in\mathbb{N}$, $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.

Démonstration
$0\in\mathbb{K}_n[X]$.
Si $P_1,P_2\in\mathbb{K}_n[X]$ et $\lambda_1,\lambda_2\in\mathbb{K}$, alors $\deg(\lambda_1P_1+\lambda_2P_2)\leqslant n$.
Donc $\lambda_1P_1+\lambda_2P_2\in\mathbb{K}_n[X]$ □

Proposition - Vision géométrique
Dans $\mathbb{R}^2$: $\{(x,y)\in\mathbb{R}^2\,|\,ax+by=0\}$ est un s.e.v de $\mathbb{R}^2$ (a,b réels fixés, $(a,b)\neq(0,0)$) (droite vectorielle).
Dans $\mathbb{R}^3$: $\{(x,y,z)\in\mathbb{R}^3\,|\,ax+by+cz=0\}$ est un s.e.v de $\mathbb{R}^3$ (a,b,c réels fixés, $(a,b,c)\neq(0,0,0)$) (plan vectoriel). Il y a aussi des droites vectorielles dans $\mathbb{R}^3$.

Proposition - Sev de $\mathscr{F}(I,\mathbb{R})$
$\mathscr{C}(I,\mathbb{R})$, $\mathscr{D}(I,\mathbb{R})$, $\mathscr{C}^1(I,\mathbb{R})$ sont des s.e.v de $\mathscr{F}(I,\mathbb{R})$.

Démonstration
La fonction nulle $0: I\to\mathbb{R}$, $x\mapsto 0$ est dans chacun de ces ensembles.
Ils sont stables par combinaison linéaire. □

Exercice
Les ensemble suivants sont-ils des s.e.v de $\mathscr{F}(\mathbb{R},\mathbb{R})$?
— $\mathscr{P}$: ensembles des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ paires ;
— $\mathscr{I}$: ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ impaires ;
— $F_1=\{f\in\mathscr{F}(\mathbb{R},\mathbb{R})\,|\,f(1)=2f(0)\}$;
— $F_2=\{f\in\mathscr{F}(\mathbb{R},\mathbb{R})\,|\,f(0)=f(1)+1\}$;
— $F_3=\{f\in\mathscr{F}(\mathbb{R},\mathbb{R})\,|\,\lim_{x\to-\infty}f(x)=0\}$.

Correction
Oui, oui, oui, non, oui
Et pour l'espace vectoriel des suites numériques :
Exercice
Les ensemble suivants sont-ils des s.e.v de $\mathbb{R}^{\mathbb{N}}$?
— ensemble des suites géométriques de raison q (réel fixé) ;
— ensemble des suites géométriques ;
— ensemble des suites arithmétiques ;
— ensemble des suites convergentes ;
— ensemble des suites convergeant vers 0.

Correction
Oui, non, oui, oui, oui

3.3. Sous-espace vectoriel engendré par une partie

Heuristique - Comme pour les groupes : 2 points de vue
Le nom de sous-espace engendré par une partie A de E donne l'idée du plus petit sous-espace vectoriel de E que l'on peut obtenir en ne prenant que des éléments de A. Un espace strictement plus grand (pour l'inclusion) contient nécessairement des éléments qui ne sont obtenables à partir de combinaison linéaire de A. Ce point de vue correspond bien au nom donné, mais ce n'est pas le point de vue simple mathématiquement qui permet de prouver l'existence.
Le second point de vue consiste à considérer tous les espaces vectoriels qui contiennent la partie A et de prendre parmi ceux-ci le plus petit. Or on sait, qu'en faisant l'intersection des espaces, on obtient nécessairement un ensemble qui contient A (qui est dans tous) et qui est le plus petit. C'est bien le même point de vue choisi que pour les groupes engendrés

Soit $(E,+,.)$ un $\mathbb{K}$-e.v.

Théorème - Intersection de s.e.v
Soient F_1 et F_2 deux s.e.v de E. Alors $F_1 \cap F_2$ est un s.e.v de E.
Plus généralement, soit $(F_i)_{i\in I}$ une famille de s.e.v de E (I fini ou infini).
Alors $\bigcap_{i\in I} F_i$ est un s.e.v de E.

Démonstration
Pour tout $i \in I$, $0 \in F_i$, donc $0 \in \bigcap_{i\in I} F_i$.
Soient $\lambda, \mu \in \mathbb{K}$, $x, y \in \bigcap_{i\in I} F_i$,
alors pour tout $i \in I$, $x \in F_i$ $y \in F_i$ et donc $\lambda x + \mu y \in F_i$ car F_i sev.
Ainsi $\lambda x + \mu y \in \bigcap_{i\in I} F_i$. □

Si $A \subset E$, $\mathscr{A} = \{B \text{ sev de } E \mid A \subset B\}$ est non vide et admet un plus petit élément :

Définition - Sous espace engendré par une partie
Soit $A \subset E$. L'ensemble des s.e.v de E contenant A admet un plus petit élément pour l'inclusion que l'on appelle sous-espace vectoriel engendré par A, noté vect(A). C'est l'intersection de tous les s.e.v contenant A.

Démonstration
Il faut montrer l'existence, il s'agit de $< A >:= \bigcap_{B\in\mathscr{A}} B$.
1. En effet, cet inclusion donne bien un sous-espace vectoriel de E.
2. $< A >$ contient A, car tous les B intersectés contiennent A.
3. Si C est un sous-espace contenant A, alors $C \in \mathscr{A}$, donc $< A > \subset C$. C'est le plus petit
□

Remarque - Si A est déjà un espace vectoriel
Si A est un s.e.v de E alors vect(A) = A.

Théorème - Caractérisation
Soit $A \subset E$, $A \neq \emptyset$.
vect(A) est l'ensemble des combinaisons linéaires d'éléments de A :

$$\text{vect}(A) = \{\lambda_1 \cdot a_1 + \cdots + \lambda_n \cdot a_n;\ n \in \mathbb{N}^*,\ (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n,\ (a_1, \ldots, a_n) \in A^n\}.$$

Démonstration
Notons momentanément $C = \{\lambda_1.a_1 + \cdots + \lambda_n.a_n;\ n \in \mathbb{N}^*, (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n, (a_1, \ldots, a_n) \in A^n\}$.
On veut montrer que vect(A) = C.
• C contient le vecteur nul (pour $n = 1, a_1 \in A, \lambda_1 = 0$), et est stable par combinaison linéaire
(une combinaison linéaire de deux éléments eux même combinaison linéaire d'éléments de A est une combinaison linéaire d'éléments de A)
et $A \subset C$ ($n = 1, a_1 \in A, \lambda_1 = 1$) :
C est un s.e.v. de E contenant A, donc par définition vect(A) $\subset C$.
• D'autre part si $(a_1, \ldots, a_n) \in A^n$, alors $(a_1, \ldots, a_n) \in \text{vect}(A)^n$
et comme vect(A) s.e.v. toute combinaison linéaire des a_i appartient à vect(A)
et donc $C \subset$ vect(A).
Finalement on a bien vect(A) = C.
□

Définition - Sous espace vectoriel engendré par une famille
On appelle sous-espace vectoriel engendré par la famille $(x_i)_{i\in I}$ d'éléments de E le s.e.v engendré par $\{x_i;\ i \in I\}$. C'est donc l'ensemble des combinaisons linéaires (finies) des x_i.

Exemple - Dans le $\mathbb{R}$ev $\mathbb{C}$
Par exemple, dans le $\mathbb{R}$-e.v $\mathbb{C}$, vect(1) = $\mathbb{R}$, vect(i) = $i\mathbb{R}$, vect(1, i) = $\mathbb{C}$.

Pour aller plus loin - Pas de stabilité par réunion. mais une nouvelle opération à la place
La réunion de deux espaces vectoriels n'est pas (en général) un espace vectoriel.
Par contre, certains auteurs notent $A \vee B$, l'opération vect(A, B) *définie un peu plus bas.*
Cette notation est très compatible avec la suite du cours. On peut la garder en tête pour la suite…

Savoir faire - Montrer un espace vectoriel par famille génératrice
Cela peut servir à prouver qu'un ensemble est un espace vectoriel; par exemple

$$\{(x, y, z) \in \mathbb{R}^3 \mid \exists(\lambda, \mu) \in \mathbb{R}^2,\ (x, y, z) = \lambda(1, 0, 1) + \mu(2, 2, 1)\}$$
$$= \text{vect}\big((1, 0, 1), (2, 2, 1)\big)$$

est un s.e.v de $\mathbb{R}^3$.

L'exercice suivant est à savoir faire :
Exercice
Caractériser par une équation le s.e.v de $\mathbb{R}^3$ engendré par $A = \{(1, 1, 1), (1, 0, 1)\}$.

Correction
$x \in \text{vect}A \iff \exists\, a, b \in \mathbb{R}$ tel que $x = a(1, 1, 1) + b(1, 0, 1) = (a + b, a, a + b)$.
On cherche à exprimer une condition nécessaire et suffisante sur les coordonnées de x.

$$x = (x_1, x_2, x_3) \in \text{vect}A \iff \exists\, a, b \in \mathbb{R} \text{ tel que } \begin{cases} a & +b & = & x_1 \\ a & & = & x_2 \\ a & +b & = & x_3 \end{cases}$$

$$x = (x_1, x_2, x_3) \in \text{vect}A \iff \exists\, a, b \in \mathbb{R} \text{ tel que } \begin{cases} a & & = & x_2 \\ & b & = & x_1 - x_2 \\ \hline & x_1 & = & x_3 \end{cases}$$

Donc vect$A = \{x = (x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 = x_3\}$
(et dans ce cas $x = x_2 \cdot a + (x_1 - x_2) \cdot b$)

3.4. Somme de sous-espaces vectoriels

$F + G =$ **vect**$(F \cup G)$

Soit $(E, +, .)$ un $\mathbb{K}$-e.v.

Définition - Somme d'espaces vectoriels
Soient $F_1, \ldots, F_n$ des s.e.v de E ($n \in \mathbb{N}^*$). On appelle somme des s.e.v F_i l'ensemble

$$F_1 + F_2 + \cdots + F_n = \{x_1 + x_2 + \cdots + x_n \mid \forall i \in [\![1, n]\!],\ x_i \in F_i\}$$

Pour aller plus loin - Moins loin
Voici la définition exacte de la réunion vectorielle : $A + B = A \vee B$

Théorème - Addition et partie engendrée
$F_1 + F_2 + \cdots + F_n$ est un s.e.v de E et on a $F_1 + F_2 + \cdots + F_n = \text{vect}(F_1 \cup \ldots \cup F_n)$
(c'est le plus petit s.e.v de E qui contienne $F_1 \cup \ldots \cup F_n$.)

Démonstration

- Montrons d'abord que $F_1 + F_2 + \cdots + F_n$ est un s.e.v de E :
Comme $0_E = 0_E + \cdots + 0_E$ et que $0_E \in F_i$ pour tout i, on a $0_E \in F_1 + F_2 + \cdots + F_n$.
D'autre part si $x = \sum_{i=1}^n x_i$, $y = \sum_{i=1}^n y_i$ avec $x_i, y_i \in F_i$ et $(\lambda, \mu) \in \mathbb{K}^2$, alors
$$\lambda.x + \mu.y = \sum_{i=1}^{n} \lambda.x_i + \mu.y_i \in F_1 + F_2 + \cdots + F_n \text{ car } \lambda.x_i + \mu.y_i \in F_i \text{ (s.e.v.)}$$
- On note momentanément $F = F_1 + F_2 + \cdots + F_n$. Montrons que $F = \text{vect}(F_1 \cup \ldots \cup F_n)$ par double inclusion.
$\boxed{\subset}$ Soit $x = \sum_{i=1}^n x_i \in F$ ($x_i \in F_i$). On a $\forall i, x_i \in F_1 \cup \ldots \cup F_n$ et vect$(F_1 \cup \ldots \cup F_n)$ est, par caractérisation, l'ensemble des C.L. des éléments de $F_1 \cup \ldots \cup F_n$, donc $x \in$ vect$(F_1 \cup \ldots \cup F_n)$ et on a la première inclusion.
$\boxed{\supset}$ $\forall i \in I, F_i \subset F$ car $x_i \in F_i$ s'écrit $x_i = 0_E + \cdots + x_i + \cdots + 0_E$ où $0_E \in F_j$ avec $j \neq i$, d'où $x_i \in F$.
Donc $F_1 \cup \ldots \cup F_n \subset F$ et par définition de vect$(F_1 \cup \ldots \cup F_n)$, on a donc vect$(F_1 \cup \ldots \cup F_n) \subset F$, d'où la deuxième inclusion.

□

Exercice
Dans $\mathbb{R}^3$, vérifier que $F = \{(x, 0, 0);\ x \in \mathbb{R}\}$ et $G = \{(x, x, 0);\ x \in \mathbb{R}\}$ sont des s.e.v de $\mathbb{R}^3$ et déterminer $F + G$.

Correction
$F = \text{vect}\big((1,0,0)\big)$ et $G = \text{vect}\big((1,1,0)\big)$, ce sont bien des espaces vectoriels de $\mathbb{R}^3$.
Et $F+G = \text{vect}\big((1,0,0),(1,1,0)\big) = \{(a+b,b,0) \mid a,b,\in\mathbb{R}\} = \{(x,y,0) \mid x,y\in\mathbb{R}\} = \text{vect}\big((1,0,0),(0,1,0)\big)$
Nous avons vu que $F\cap G$ est un sev. Il n'en est pas de tout du même de $F\cup G$.
Cette notion est remplacée dans le cadre des espaces vectoriels par $F+G$.

Savoir faire - Caractérisations. $x\in F\cap G$, $x\in F+G$
On a alors
$x\in F\cap G \iff x\in F$ et $x\in G$,
$x\in F+G \iff \exists\, a\in F, b\in G$ tels que $x=a+b$.

Attention - Deux erreurs classiques qui en découlent
- Si $x\in F+G$ et $x\notin G \not\Rightarrow x\in F$.
- $E=F\oplus G = F\oplus H \not\Rightarrow G=H$.

Ecrire cela serait confondre les notions de supplémentarité et de complémentarité!

Somme directe

Proposition - Somme directe
Soient $F_1,\dots,F_n$ des s.e.v de E ($n\in\mathbb{N}^*$). Il y a équivalence de :

(i) tout élément x de $F_1+F_2+\dots+F_n$ s'écrit de manière unique sous la forme
$x = x_1+x_2+\dots+x_n$ avec $\forall i, x_i\in F_i$
(ii) $\forall (x_1,x_2,\dots,x_n)\in F_1\times F_2\times\dots\times F_n$, $x_1+x_2+\dots+x_n=0_E \Rightarrow \forall i, x_i=0_E$

Si ces propriétés sont vérifiées, on dit que les F_i sont en somme directe et on note leur somme
$$F_1\oplus F_2\oplus\dots\oplus F_n = \bigoplus_{i=1}^{n} F_i.$$

Démonstration
On note $G=F_1+F_2+\dots F_n$. On peut encore raisonner avec l'application :
$$\Psi : F_1\times F_2\times\dots\times F_n \longrightarrow G, \qquad (x_1,x_2,\dots x_n)\longmapsto x_1+x_2+\dots+x_n$$
Il est affirmé que les F_i sont en somme directe si Ψ est injective (1ere proposition).
Et que celle-ci est équivalent à l'injectivité sur 0.
En effet :
$$\Psi(x)=\Psi(y) \Leftrightarrow x_1+x_2+\dots+x_n = y_1+y_2+\dots y_n \Leftrightarrow (x_1-y_1)+(x_2-y_2)+\dots(x_n-y_n)=0$$
L'injectivité en 0 assure alors $\forall\, i\in\mathbb{N}_n$, $x_i-y_i=0$, donc $x=y$ et Ψ est injective.
La réciproque est triviale □

Pour aller plus loin - Vision physicienne
En science physique, un excellent réflexe fréquent est celui qui affirme : un vecteur est nul si et seulement si ses coordonnées sont nulles.
On passe ainsi aisément d'une équation (vectorielle) à n équation scalaire.
Il arrive de faire la transformation dans les deux sens…

Corollaire - Cas de 2 s.e.v
Soient F_1 et F_2 deux s.e.v de E. F_1 et F_2 sont en somme directe si et seulement si $F_1\cap F_2=\{0_E\}$.

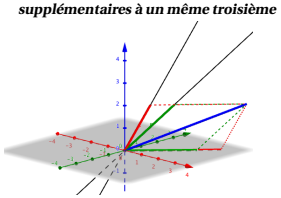
Définition - Espaces supplémentaires
F_1 et F_2 deux s.e.v de E sont dits supplémentaires si $E=F_1\oplus F_2$,
ce qui équivaut à :
1. $E=F_1+F_2$
2. $F_1\cap F_2=\{0_E\}$

ou à
tout vecteur de E se décompose de manière unique comme somme d'un

vecteur de F_1 et d'un vecteur de F_2.

Attention - Notation piégée
Lorsqu'on écrit : $E=F_1\oplus F_2$, il y a bien DEUX affirmations (deux propositions ou deux verbes) :
— $E=F_1+F_2$
— La somme est directe : $F_1\oplus F_2$ ou $F_1\cap F_2=\{0_E\}$

Représentation - Deux espaces différents supplémentaires à un même troisième



Les deux droites vectoriels sont toutes les deux supplémentaires au plan $z=0$ dans $\mathbb{R}^3$.
On peut y voir la décomposition unique de $z=x_1+y_1=x_2+y_2$ pour ces deux espaces supplémentaires. Même si y_1 et $y_2\in\mathscr{P}$ (même plan), ce sont néanmoins des vecteurs différents.

Exemple - Dans le $\mathbb{R}$-e.v $\mathbb{C}$
$\mathbb{C}=\mathbb{R}+i\mathbb{R}$.

Remarque - Autour de la notion de supplémentaire
- On dit aussi que F_2 est un supplémentaire de F_1 (dans E).
- Ne pas confondre supplémentaire et complémentaire, le complémentaire d'un s.e.v n'est jamais un s.e.v
- E admet un seul supplémentaire, c'est $\{0_E\}$ (et réciproquement).
- Il existe, en général, une infinité de supplémentaires d'un s.e.v (voir l'illustration dans la marge)

Savoir faire - Montrer que deux espaces vectoriels sont supplémentaires
Montrer que $E=F\oplus G$, c'est montrer que $E=F+G$ et $F\cap G=\{0\}$.
Très souvent on procède par analyse-synthèse :
— L'analyse : *Supposons que $E=F+G$.*
Soit $x\in E$, il existe $(y,z)\in F\times G$ tel que $x=y+z$.
Le problème : pour UN x donné, il y a DEUX vecteurs y et z, ce qui est trop de *liberté* Il faut découpler ces vecteurs. Ainsi, après analyse (lié aux conditions du problème), on trouve y défini explicitement en fonction de x (uniquement : i.e. plus de z) et également on trouve z défini explicitement en fonction de x (uniquement : i.e. plus de y).
Fin de l'analyse. On ne sait pas si le couple (y,z) existe bien, mais s'il existe il est unique.

— La synthèse. On fixe $x\in E$ et on reprend le couple (y,z) défini comme à la fin de l'analyse.
On vérifie tour à tour que :
— $y\in F$
— $z\in G$
— $x=y+z$.
Fin de la synthèse. On a bien, pour tout $x\in E$, $\exists\,(y,z)\in F\times G$ tel que $x=y+z$, ie. $E\subset F+G$.
(L'inclusion réciproque est donné par $F\subset E$, $G\subset E$, E espace vectoriel.)

Dans ce genre d'exercice, on exploite souvent le raisonnement en analyse-synthèse.
Exercice
Montrer que $\mathscr{P}$ (ensembles des fonctions paires) et $\mathscr{I}$ (ensemble des fonctions impaires) sont des s.e.v supplémentaires de $\mathscr{F}(\mathbb{R},\mathbb{R})$.

Correction
Soit $f\in\mathscr{F}(\mathbb{R},\mathbb{R})$.
Supposons que $f=p+i$, avec p paire et i impaire.
Alors pour tout $x\in\mathbb{R}$, $f(-x)=p(-x)+i(-x)=p(x)-i(x)$.
Donc $p(x)=\frac{f(x)+f(-x)}{2}$ et $i(x)=\frac{f(x)-f(-x)}{2}$.
Cela assure l'UNICITE de la décomposition.
Maintenant, étant donné f, considérons $p: x\mapsto \frac{f(x)+f(-x)}{2}$ et $i: x\mapsto \frac{f(x)-f(-x)}{2}$.
On a alors, pour tout $x\in\mathbb{R}$, $p(x)+i(x)=f(x)$, donc $p+i=f$.
Et pour tout $x\in\mathbb{R}$, $p(-x)=\frac{f(-x)+f(x)}{2}=p(x)$ et $i(-x)=\frac{f(-x)-f(x)}{2}=i(x)$ ainsi $p\in\mathscr{P}$ et $i\in\mathscr{I}$.
Cela démontre bien l'EXISTENCE de la décomposition. Finalement : $\mathscr{F}(\mathbb{R},\mathbb{R})=\mathscr{P}\oplus\mathscr{I}$

4. Applications linéaires

4.1. Définitions et exemples

Définition - Application linéaire
Soit u une application de E dans F. On dit que u est linéaire si

(1) $\forall (x,y)\in E^2, u(x\underset{E}{+}y)=u(x)\underset{F}{+}u(y)$

(2) $\forall x\in E, \forall \lambda\in\mathbb{K}, u(\lambda\underset{E}{.}x)=\lambda\underset{F}{.}u(x)$

Histoire - Introduction des espaces vectoriels et des applications linéaires
Les applications linéaires (et les espaces vectoriels associés) se sont imposées petit à petits dans les manuel de mathématiques supérieures au début du XX^e siècle… Elles étaient initialement considérée avec beaucoup d'attention, le domaine semblait difficile (à l'inverse des groupes…). Aujourd'hui, cela se fait vite dès les premiers mois dans les études supérieures, partout dans le monde.
Cette universalité est étonnante : la définition des espaces vectoriels était loin d'être uniforme dans chaque pays. Il semble que ce soit la multiplication des espaces vectoriels de fonctions (et en particulier leurs exploitation par Stefan Banach) qui ait justifié cette introduction de plus en plus précoce.

Savoir faire - Montrer qu'une application est linéaire
$u:E\to F$ est linéaire si et seulement si

$$\forall (x,y)\in E^2, \forall(\lambda,\mu)\in\mathbb{K}^2, u(\lambda.x+\mu.y)=\lambda.u(x)+\mu.u(y)$$

Démontrons qu'on a bien cette équivalence.

Démonstration
$\Rightarrow$ évident
$\Leftarrow$ en prenant $\lambda=\mu=1$ on a $u(x+y)=u(x)+u(y)$ et en prenant $\mu=0$ on a $u(\lambda.x)=\lambda.u(x)$ □

Proposition - Image par une application linéaire
Soit $u:E\to F$ une application linéaire. Alors

(1) $u(0_E)=0_F$

(2) $\forall n\in\mathbb{N}^*, \forall (x_i)_{1\leqslant i\leqslant n}\in E^n, \forall(\lambda_i)_{1\leqslant i\leqslant n}\in\mathbb{K}^n, u\left(\sum_{i=1}^n \lambda_i.x_i\right)=\sum_{i=1}^n \lambda_i.u(x_i)$

Dans le cas d'une famille infinie $(x_i)_{i\in I}$, si $(\lambda_i)_{i\in I}$ est une famille presque nulle, on a aussi

$$u\left(\sum_{i\in I}\lambda_i.x_i\right)=\sum_{i\in I}\lambda_i.u(x_i).$$

L'image d'une combinaison linéaire est donc la combinaison linéaire des images (avec les mêmes coefficients).

Définition - endo/iso/auto -morphisme
On appelle
- isomorphisme de E dans F toute application linéaire bijective de E dans F ;
- endomorphisme de E toute application linéaire de E dans E ;
- automorphisme de E un isomorphisme de E dans E ;
- forme linéaire sur E toute application linéaire de E dans $\mathbb{K}$.

On note
- $\mathscr{L}(E,F)$ l'ensemble des applications linéaires de E dans F (éventuellement $\mathscr{L}_{\mathbb{K}}(E,F)$ s'il y a une ambiguité sur le corps $\mathbb{K}$) ;
- $\mathscr{L}(E,\mathbb{K})$ ou E^* l'ensemble des formes linéaires sur E, aussi appelé dual de E ;
- $\mathscr{L}(E)$ l'ensemble des endomorphismes de E (i.e. $\mathscr{L}(E,E)$).

Remarque - Eléments neutres
$Id_E\in\mathscr{L}(E)$ (élément neutre pour $\circ$) ;
l'application nulle de E dans F est linéaire (élément neutre pour $+$).

Exemple - Donner des exemples
- endomorphismes de $\mathbb{R}$
- homothéties de E

Pour aller plus loin - Pourquoi s'intéresser aux applications linéaires
Ce que nous apprend Newton des lois de la physique (démontré d'une certaine façon par les formules de Taylor) : le monde est en première approximation linéaire.
Une application quelconque vérifie toujours au voisinage d'un point $M_0(x_0,y_0,z_0)$:

$$f(M)=f(M_0)+\overrightarrow{u_{f,M_0}}(x-x_0,y-y_0,z-z_0)$$
$$+o(\|(x-x_0,y-y_0,z-z_0)\|)$$

avec $\overrightarrow{u_{f,M_0}}$, une application linéaire!

- endomorphisme du $\mathbb{R}$-e.v. $\mathbb{C}$
- applications linéaires du $\mathbb{R}$-e.v. $\mathbb{C}$ dans $\mathbb{R}$
- dans $\mathscr{C}^1(\mathbb{R},\mathbb{R})$ ou $\mathscr{C}^1(\mathbb{R},\mathbb{C})$
- dans $\mathbb{K}[X]$

Exercice
Soit $E=C^\infty(\mathbb{R},\mathbb{R})$ le sous-espace vectoriel de $\mathscr{F}(\mathbb{R},\mathbb{R})$ constitué des fonctions indéfiniment dérivables sur $\mathbb{R}$. Soit D l'application qui à une fonction de E associe sa dérivée et I l'application qui à une fonction f associe la primitive de f qui s'annule en 0.
Vérifier que D et I sont des endomorphismes de E. S'agit-il d'isomorphismes ? Que peut on dire de $D\circ I$ et de $I\circ D$?

Correction
$D:E\mapsto E$. Pour tout $f,g\in E, \lambda,\mu\in\mathbb{K}$,
$D(\lambda f+\mu g)=\lambda f'+\mu g'=\lambda D(f)+\mu D(g)$.
$I:E\mapsto E$. Pour tout $f,g\in E, \lambda,\mu\in\mathbb{K}$,
$I(\lambda f+\mu g)=\lambda(F-F(0))+\mu(G-G(0))=\lambda I(f)+\mu I(g)$.
donc D et I sont bien des endomorphismes.
D n'est pas injective : $f_1=f+K$, alors $D(f_1)=f'=D(f)$, alors que $f_1\neq f$.
Donc D n'est pas un isomorphisme.
I n'est pas surjective. Les fonctions qui ne s'annulent pas en 0 n'ont pas d'antécédents par I.
Donc I n'est pas un isomorphisme.
$(D\circ I)(f)=f$, alors que $(I\circ D)(f)=f-f(0)$.

Attention - Montrer la bijectivité
L'exemple précédent montrer qu'il faut bien les deux conditions $f\circ g=id$ ET $g\circ f=id$, pour pouvoir affirmer que f (ou g) est bijective…

Exercice
Soient F et G deux sous-espaces vectoriels d'un $\mathbb{K}$-e.v. E. On considère l'application

$$\begin{array}{rccc}\phi: & F\times G & \to & E\\ & (x,y) & \mapsto & x+y.\end{array}$$

Montrer que ϕ est linéaire. A quelle condition sur F et G est-ce un isomorphisme ? Quel est alors l'isomorphisme réciproque ?

Correction
Il ne faut pas aller trop vite…

$$\phi\big(\lambda_1(x_1,y_1)+\lambda_2(x_2,y_2)\big)=\phi(\lambda_1x_1+\lambda_2x_2,\lambda_1y_1+\lambda_2y_2)=\lambda_1x_1+\lambda_2x_2+\lambda_1y_1+\lambda_2y_2$$
$$=\lambda_1(x_1+y_1)+\lambda_2(x_2+y_2)=\lambda_1\phi(x_1,y_1)+\lambda_2\phi(x_2,y_2)$$

Donc ϕ est bien linéaire. On a vu que ϕ est bijective ssi $E=F\oplus G$.
L'application réciproque jouera un rôle important par la suite du cours : c'est la combinaison des deux projections de E sur F (de direction G) et respectivement de E sur G (de direction F)

Définition - Image et noyau
Soit $u\in\mathscr{L}(E,F)$. On appelle
- noyau de u, l'ensemble $\operatorname{Ker}u=\{x\in E\,|\,u(x)=0_F\}=u^{-1}(\{0_F\})$
- image de u, l'ensemble $\operatorname{Im}u=\{y\in F\,|\,\exists x\in E, y=u(x)\}=u(E)$

Théorème - Transformation par u linéaire, en sev
Soit $u\in\mathscr{L}(E,F)$.
- $\operatorname{Ker}u$ est un s.e.v de E, $\operatorname{Im}u$ est une s.e.v de F
- Plus généralement, si V est un s.e.v de E et W un s.e.v de F, alors $u^{-1}(W)$ est s.e.v de E et $u(V)$ est un s.e.v de F.

On rappelle que $u(V)=\{u(x),x\in V\}$ et $u^{-1}(W)=\{x\in E\,|\,u(x)\in W\}$

Démonstration
On démontre le second cas, avec $V=E$ et $W=\{0\}$, on en déduira le résultat pour $\operatorname{Im}u$ et $\operatorname{Ker}u$ respectivement.
Soient $\lambda,\mu\in\mathbb{K}, x,y\in u(V)$.
Il existe $a,b\in V$ tel que $x=u(a)$ et $y=u(b)$,
Donc $\lambda x+\mu y=u(\lambda a+\mu b)\in u(V)$, car u est linéaire.

Donc $u(V)$ est un sev de F.
Soient $\lambda,\mu\in\mathbb{K}$, $x,y\in u^{-1}(W)$.
Donc $u(\lambda x+\mu y)=\lambda u(x)+\mu u(y)$, car u est linéaire.
Comme W est un espace vectoriel, $\lambda u(x)+\mu u(y)\in W$,
ainsi $\lambda x+\mu y\in u^{-1}(W)$. Donc $u^{-1}(W)$ est un sev de E. □

Exercice
Montrer que l'application

$$\begin{array}{rccc} u: & \mathbb{R}^3 & \to & \mathbb{R}^2 \\ & (x,y,z) & \mapsto & (x+y-z,x-y+2z) \end{array}$$

est une application linéaire de $\mathbb{R}^3$ dans $\mathbb{R}^2$ et déterminer son noyau et son image.

Correction

$$u(\lambda_1\cdot(x_1,y_1,z_1)+\lambda_2\cdot(x_2,y_2,z_2))=u\big((\lambda_1x_1+\lambda_2x_2,\lambda_1y_1+\lambda_2y_2,\lambda_1z_1+\lambda_2z_2)\big)$$
$$=(\lambda_1x_1+\lambda_2x_2+\lambda_1y_1+\lambda_2y_2-\lambda_1z_1-\lambda_2z_2,\lambda_1x_1+\lambda_2x_2-\lambda_1y_1-\lambda_2y_2+2\lambda_1z_1+2\lambda_2z_2)$$
$$=\lambda_1(x_1+y_1-z_1,x_1-y_1+2z_1)+\lambda_2(x_2+y_2-z_2,x_2-y_2+2z_2)=\lambda_1u(x_1,y_1,z_1)+\lambda_2u(x_2,y_2,z_2)$$

Donc u est une application linéaire de $\mathbb{R}^3$ dans $\mathbb{R}^2$.
Puis $\operatorname{Ker}u=\{(x,y,z)\mid(x+y-z,x-y+2z)=(0,0)\}=\{(x,y,z)\mid x=-\frac{1}{2}z,y=\frac{3}{2}z\}=\{z(\frac{-1}{2},\frac{3}{2},1),z\in\mathbb{R}\}=\operatorname{vect}(-1,3,2)$.
Et $\operatorname{Im}u=\{(x+y-z,x-y+2z),x,y,z\in\mathbb{R}\}=\mathbb{R}^2\}$

Théorème - Critère d'injectivité et de surjectivité
Soit $u\in\mathscr{L}(E,F)$.

$$u \text{ est injective } \Leftrightarrow \operatorname{Ker}u=\{0_E\}$$
$$u \text{ est surjective } \Leftrightarrow \operatorname{Im}u=F$$

Pour aller plus loin - Rappel
Ces théorèmes ainsi que les définitions associées nous rappelle les résultat vu sur les morphismes de groupes

Démonstration
Par linéarité de u, $u(x)=u(y)\Leftrightarrow u(x-y)=0$
u est injective $\Longleftrightarrow[\forall\,x,y\in E,\,u(x)=u(y)\Rightarrow x=y]$
$\Longleftrightarrow[\forall\,x,y\in E,\,x-y\in\operatorname{Ker}u\Rightarrow x-y=0]$
$\Longleftrightarrow[\forall\,z\in E,\,z\in\operatorname{Ker}u\Rightarrow z=0]$
$\Longleftrightarrow\operatorname{Ker}u=\{0\}$
u est surjective $\Longleftrightarrow[\forall\,y\in F,\,\exists\,x\in E$ tel que $y=u(x)]$
$\Longleftrightarrow[\forall\,y\in F,\,y\in\operatorname{Im}F]\Longleftrightarrow F\subset\operatorname{Im}u$
L'inclusion réciproque étant toujours vraie :
u est surjective $\Longleftrightarrow\operatorname{Im}u=F$ □

Exercice
L'application linéaire D qui à $P\in\mathbb{K}[X]$ associe P' est-elle injective ? surjective ?

Correction
$\operatorname{Ker}D=\mathbb{K}_0[X]$, l'ensemble des polynômes constants, donc D n'est pas injective.
$\operatorname{Im}D=\mathbb{K}[X]$, donc D est surjective.

4.2. Cas général : structure de $\mathscr{L}(E,F)$

Théorème - Structure d'espace vectoriel
$(\mathscr{L}(E,F),+,.)$ est un $\mathbb{K}$-espace vectoriel.

Remarque - Interprétation
Cela signifie en particulier que la somme de deux applications linéaires est linéaire, ainsi que $\lambda.f$.
On ne fera pas de démonstration.

Théorème - Composition linéaire
Soient E,F,G trois $\mathbb{K}$-e.v. et $u\in\mathscr{L}(E,F)$, $v\in\mathscr{L}(F,G)$. Alors $v\circ u\in\mathscr{L}(E,G)$.

Démonstration
Soient $\lambda,\mu\in\mathbb{K}$ et $x,y\in E$.

$$(v\circ u)(\lambda x+\mu y)=v\big(u(\lambda x+\mu y)\big)=v(\lambda u(x)+\mu u(y))=\lambda v(u(x))+\mu v(u(y))$$
$$=\lambda(v\circ u)(x)+\mu(v\circ u)y$$

□

Théorème - u^{-1} ?
La réciproque d'un isomorphisme de E dans F est un isomorphisme de F dans E.

Démonstration
Soit u un isomorphisme de E sur F.
Alors u est bijective et admet une application réciproque u^{-1}, également bijective.
Et u^{-1} est un morphisme : Pour tout $\lambda_1\lambda_2\in\mathbb{K},\forall\,y_1,y_2\in F,x_1=u^{-1}(y_1),x_2=u^{-1}(y_2)$,

$$u^{-1}(\lambda_1y_1+\lambda_2y_2)=u^{-1}(\lambda_1u(x_1)+\lambda_2u(x_2))=u^{-1}(u(\lambda_1x_1+\lambda_2x_2))$$
$$=\lambda_1x_1+\lambda_2x_2=\lambda_1u^{-1}(y_1)+\lambda_2u^{-1}(y_2)$$

□

Définition - Espaces isomorphes
Deux $\mathbb{K}$-e.v. E et F tels qu'il existe un isomorphisme de E dans F sont dits isomorphes.

Théorème - Linéarité de la composition
Soit $u\in\mathscr{L}(E,F)$. Alors l' application

$$\begin{array}{ccc} \mathscr{L}(F,G) & \to & \mathscr{L}(E,G) \\ v & \mapsto & v\circ u \end{array}$$

est linéaire i.e

$$(\lambda.v_1+\mu.v_2)\circ u=\lambda.v_1\circ u+\mu.v_2\circ u$$

Soit $v\in\mathscr{L}(F,G)$. Alors l' application

$$\begin{array}{ccc} \mathscr{L}(E,F) & \to & \mathscr{L}(E,G) \\ u & \mapsto & v\circ u \end{array}$$

est linéaire i.e

$$v\circ(\lambda.u_1+\mu.u_2)=\lambda.v\circ u_1+\mu.v\circ u_2$$

Démonstration
Nous ferrons qu'un seul cas : la linéarité de

$$\Phi:\begin{array}{ccc} \mathscr{L}(F,G) & \to & \mathscr{L}(E,G) \\ v & \mapsto & v\circ u \end{array}$$

Pour tout $\lambda_1,\lambda_2\in\mathbb{K},v_1,v_2\in\mathscr{L}(E,F)$,

$$\Phi(\lambda_1v_1+\lambda_2v_2)=(\lambda_1v_1+\lambda_2v_2)\circ u=\lambda_1v_1(u(\cdot)+\lambda_2v_2(u(\cdot))=\lambda_1\Phi(v_1)+\lambda_2\Phi(v_2)$$

□

4.3. Cas particulier de $\mathscr{L}(E)$

Théorème - Structure de $\mathscr{L}(E)$
Soit E un $\mathbb{K}$-e.v.
— $(\mathscr{L}(E),+)$ est un groupe commutatif ;
— $(\mathscr{L}(E),+,.)$ est un $\mathbb{K}$-espace vectoriel ;
— $(\mathscr{L}(E),+,\circ)$ est un anneau non commutatif (sauf si E de dimension finie égale à 1), en particulier la composée de deux endomorphismes de E est un endomorphisme de E ;
— $\forall\lambda\in\mathbb{K},\forall(u,v)\in\mathscr{L}(E)^2,(\lambda.v)\circ u=\lambda.(v\circ u)=v\circ(\lambda.u)$
On résume ces propriétés en disant que $(\mathscr{L}(E),+,\circ,.)$ est une algèbre sur

$\mathbb{K}$.

Exercice
Donner un contre-exemple pour la commutativité.

Correction
$u : \mathbb{R}^2 \to \mathbb{R}^2$, $(x,y) \mapsto (2x,y)$ et $v : \mathbb{R}^2 \to \mathbb{R}^2$, $(x,y) \mapsto (y,x)$.
Alors $u \circ v(x,y) = (2y,x)$ et $v \circ u(x,y) = (y,2x)$.

Proposition - Règles de calcul dans $\mathscr{L}(E)$
Soit $u \in \mathscr{L}(E)$. On définit pour $n \in \mathbb{N}$ u^n par

$$u^0 = Id_E \text{ et } \forall n \geqslant 1, u^n = u \circ u^{n-1} = \underbrace{u \circ u \ldots \circ u}_{n facteurs}.$$

Pour u et v qui commutent ($u \circ v = v \circ u$) on a les formules suivantes :

$(u+v)^n = \sum_{k=0}^{n} \binom{n}{k} u^k \circ v^{n-k}$ (Formule du binôme)
$u^n - v^n = (u-v) \circ (u^{n-1} + u^{n-2} \circ v + \ldots + u \circ v^{n-2} + v^{n-1})$ (Factorisation)
$Id_E - v^n = (Id_E - v) \circ (Id_E + v + v^2 + \ldots + v^{n-2} + v^{n-1})$

On note parfois $u \circ v = uv$.

Attention - uv
En algèbre, uv n'est JAMAIS $u \times v$, cela n'a pas de sens.
(Il n'y a pas de produit dans les espaces vectoriels)

Application - A compléter
On obtient donc :

$(u+v)^2 =$, $u^2 - v^2 =$, $u^3 - v^3 =$

Remarque - Démonstration
Il s'agit toujours de la même démonstration, celle vu avec les polynômes.

Exercice
Soient E un $\mathbb{K}$-e.v. et $u \in \mathscr{L}(E)$. Montrer que si $v = \sum_{k=0}^{n} a_k u^k$ (avec $n \in \mathbb{N}$, $a_k \in \mathbb{K}$), alors v commute avec toute puissance de u, puis que v commute avec $w = \sum_{k=0}^{m} b_k u^k$ (avec $m \in \mathbb{N}$, $b_k \in \mathbb{K}$).

Correction
$u \circ v = \sum_{k=0}^{n} a_k u^{k+1} = v \circ u$.
$w \circ v = \sum_{h=0}^{n+m} (\sum_{k=0}^{n} a_k b_{h-k}) u^h = v \circ w$

Proposition - Groupe linéaire
La réciproque d'un automorphisme de E est un automorphisme de E.
L'ensemble des automorphismes de E muni de la loi $\circ$ est donc un groupe (en général non commutatif) appelé groupe linéaire et noté $GL(E)$.

Démonstration
Un automorphisme est un isomorphisme de E sur E.
On a vu que sa réciproque est également un isomorphisme de E sur E, donc un automorphisme.
□

Pour aller plus loin - Groupe des inverses
Puisque $(\mathscr{L}(E), +, \circ)$ est un anneau, l'ensemble $(\mathscr{L}(E), \circ)^\times$ des inverses de $\mathscr{L}(E)$, plutôt noté $(GL(E), \circ)$ est un groupe : le groupe linéaire.

Pour aller plus loin - Relation polynomiale
*Il faut **typiquement** interpréter ces relations avec des polynômes.*
Ici, on note $P = \sum_{k=0}^{n} a_k X^k$, $Q = X$ et $T = \sum_{k=0}^{m} b_k X^k$.
On a donc $v = P(u)$, $u = Q(u)$ et $w = T(u)$.
Puis $v \circ u = P(u) \circ Q(u) = (P \times Q)(u) = (Q \times P)(u) = u \circ v$.
De même $v \circ w = (P \times T)(u) = (T \times P)(u) = w \circ v$

Définition - Homothéties de E
Pour $\lambda \in \mathbb{K}$, l'endomorphisme $\lambda.Id_E : x \mapsto \lambda.x$ s'appelle l' homothétie de rapport λ.
Une homothétie de rapport non nul est un automorphisme.

4.4. Projecteurs et symétries

Projecteurs

Définition - Projecteur
Soient E_1 et E_2 deux sous-espaces vectoriels supplémentaires de E. On sait que tout $x \in E$ s'écrit de manière unique sous la forme $x = x_1 + x_2$ avec $x_1 \in E_1$ et $x_2 \in E_2$.
L'application

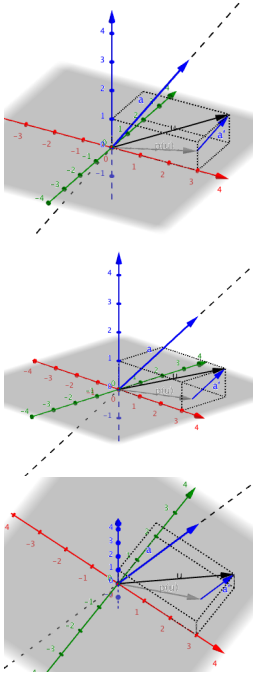
$$p : \begin{array}{l} E \to E \\ x \mapsto x_1 \end{array}$$

s'appelle le projecteur sur E_1 parallèlement à E_2 (ou de direction E_2) ;

$$q = Id_E - p : \begin{array}{l} E \to E \\ x \mapsto x_2 \end{array}$$

s'appelle le projecteur sur E_2 parallèlement à E_1 (ou de direction E_1).
On dit que p et q sont des projecteurs associés (car ils sont définis par la même décomposition de E en s.e.v supplémentaires).

Représentation - Représentation de la projection
Ici $\mathbb{R}^3 = \text{vect}(a) + \mathscr{P}$.
On projete u sur $\mathscr{P}$, on voit que $u = a' + p(u)$ avec a' et a colinéaires, alors que $p(u) \in \mathscr{P}$.



Remarque - Rappel (?) de la projection dans le plan
Le terme de projecteur généralise la notion de projection dans l'ensemble des vecteurs du plan ou de l'espace. Toutefois on parle également de projection sur E_1 parallèlement à E_2.

Remarque - A partir de l'analyse-synthèse
L'analyse-synthèse, conduit souvent à exprimer y (et z) explicitement en fonction de x.
Cette expression explicite est la définition explicite du projecteur.

Proposition - Propriétés premières d'un projecteur
On suppose que $E = E_1 \oplus E_2$. Soit p le projecteur sur E_1 parallèlement à E_2, alors :

- p est un endomorphisme de E;
- $E_1 = \{x \in E \mid p(x) = x\}$ (ensemble des invariants par p);
- $\text{Im } p = E_1$ et $\text{Ker } p = E_2$;
- $p \circ p = p$.

Démonstration
• Notons d'abord que $p : E \to E$.
Soient $x = x_1 + x_2$ et $y = y_1 + y_2$, deux vecteurs de E décomposés sur $E_1 \oplus E_2$.
Soient $\lambda, \mu \in \mathbb{K}$.

$$p(\lambda x + \mu y) = p(\underbrace{(\lambda x_1 + \mu y_1)}_{\in E_1} + \underbrace{(\lambda x_2 + \mu y_2)}_{\in E_2}) = \lambda x_1 + \mu y_1 = \lambda p(x) + \mu p(y)$$

Donc p est bien un endomorphisme de E.
• Si $x \in E_1$, $x = x + 0$ est la décomposition de x sur $E_1 \oplus E_2$, donc $p(x) = x$.
Réciproquement, si $p(x) = x$, comme $p(x) \in E$, alors $x \in E$
Par double inclusion $E = \{x \mid p(x) = x\}$. • $x \in E_1$, alors $x = p(x)$ donc $x \in \text{Im } p$.
Et réciproquement, par définition de p, $\text{Im } p \subset E_1$.
Si $x \in E_2$, alors la décomposition de x selon $E_1 \oplus E_2$ est $x = 0 + x$, donc $p(x) = 0$.
Réciproquement, comme $x - p(x) \in E_2$, si $p(x) = 0$, alors $x \in E_2$.
• Enfin, si $x = x_1 + x_2$, on a $p^2(x) = p(p(x)) = p(x_1) = x_1$, car $x_1 \in E_1$, donc $p^2(x) = p(x)$. □

Remarque - Relation entre les deux projecteurs
On a aussi $p \circ q = q \circ p = 0_{\mathscr{L}(E)}$.
En effet si $x = x_1 + x_2$, $p \circ q(x) = p(x_2) = 0 \dots$

Théorème - Caractérisation
Soit p un endomorphisme de E.
Alors p est un projecteur si et seulement si $p \circ p = p$.
On a alors $E = \text{Im } p \oplus \text{Ker } p$ et p est le projecteur sur Im p parallèlement à Ker p.

Démonstration
On a vu l'implication dans le sens direct.
Réciproquement, su $p^2 = p$.
Notons $E_1 = \text{Im } p$ et $E_2 = \text{Ker } p$.
Si $x \in E_1 \cap E_2$, alors il existe a tel que $x = p(a)$, donc $0 = p(x) = p^2(a) = p(a) = x$.
On a donc la somme directe $E_1 \oplus E_2$.
Si $x \in E$, alors $x = p(x) + (x - p(x))$.
Or $p(x) \in \text{Im } p$ et $p[(x - p(x))] = p(x) - p^2(x) = 0$, donc $x - p(x) \in \text{Ker } p$.
Les deux espaces sont supplémentaires : $E = E_1 \oplus E_2$.
Enfin, p est bien la projection sur $E_1 (= \text{Im } p)$ parallèlement à $E_2 (= \text{Ker } p)$ □

Symétries

Définition - Symétrie
Soient E_1 et E_2 deux sous-espaces vectoriels supplémentaires de E. On sait que tout $x \in E$ s'écrit de manière unique sous la forme $x = x_1 + x_2$ avec $x_1 \in E_1$ et $x_2 \in E_2$.
On appelle symétrie par rapport à E_1 parallèlement à E_2 (ou symétrie d'axe E_1 de direction E_2) l'application

$$\begin{array}{rccc} s: & E & \to & E \\ & x = x_1 + x_2 & \mapsto & x_1 - x_2 \end{array}$$

Proposition - Propriétés premières de s
On suppose que $E = E_1 \oplus E_2$.
Soit s la symétrie par rapport à E_1 parallèlement à E_2. Alors
— si p est le projecteur sur E_1 parallèlement à E_2 on a $s = 2p - Id_E$;
— s est un endomorphisme de E et $s \circ s = Id_E$ (on dit que s est une involution de E).

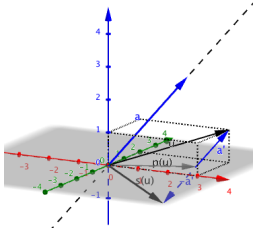
Démonstration
On garde les notations mises en place :
— $\forall x \in E$, $2p(x) - x = 2x_1 - (x_1 + x_2) = x_1 - x_2 = s(x)$ donc $s = 2p - Id_E$;
— $\mathscr{L}(E)$ est un $\mathbb{K}$-e.v. donc, comme $p \in \mathscr{L}(E)$, on a aussi $s = 2p - Id_E \in \mathscr{L}(E)$ et

$$s \circ s = (2p - Id_E) \circ (2p - Id_E) = 4p \circ p - 4p + Id_E = Id_E.$$

□

Théorème - Caractérisation
Soit $s \in \mathscr{L}(E)$.
Alors s est une symétrie si et seulement si $s \circ s = Id_E$.
On a alors $E = \text{Ker}(s - Id_E) \oplus \text{Ker}(s + Id_E)$ et s est la symétrie par rapport à Ker $(s - Id_E)$ parallèlement à Ker $(s + Id_E)$.

Représentation - Représentation des symétries
Toujours avec les mêmes espaces vectoriels



Démonstration
Il reste à prouver que $s \circ s = Id_E \Rightarrow s$ symétrie.
Pour cela on pose $p = \frac{1}{2}(s + Id_E)$ et on prouve que p est un projecteur.
On a $s \in \mathscr{L}(E) \Rightarrow p = \frac{1}{2}(s + Id_E) \in \mathscr{L}(E)$ et

$$p \circ p = \frac{1}{4}(s + Id_E) \circ (s + Id_E) = \frac{1}{4}(s \circ s + 2s + Id_E) = \frac{1}{2}(s + Id_E) = p$$

D'après la caractérisation des projecteurs, p est un projecteur (sur $\Im p$ parallèlement à Ker p) et d'après la proposition précédente, $2p - Id_E$, c'est-à-dire s, est la symétrie par rapport à $\Im p$ parallèlement à Ker p. De plus

$$x \in \Im p \Leftrightarrow p(x) = x \Leftrightarrow \frac{1}{2}(s + Id_E)(x) = x \Leftrightarrow s(x) - x = 0_E \Leftrightarrow x \in \text{Ker}(s - Id_E)$$

$$x \in \text{Ker } p \Leftrightarrow p(x) = 0_E \Leftrightarrow \frac{1}{2}(s + Id_E)(x) = 0_E \Leftrightarrow s(x) + x = 0_E \Leftrightarrow x \in \text{Ker}(s + Id_E)$$

et $E = \text{Ker}(s - Id_E) \oplus \text{Ker}(s + Id_E)$. □

Exercice
$E = \mathbb{R}^2$, on désigne par f l'endomorphisme de E défini par $f((x,y)) = (2x - y, 2x - y)$.
Montrer que f est un projecteur dont on précisera les éléments caractéristiques. On notera $E_1 = \text{Im } f$ et $E_2 = \text{Ker } f$.
Donner la détermination analytique de la symétrie par rapport à E_2 parallèlement à E_1.

Correction
$f^2(x,y) = f(2x - y, 2x - y) = (2(2x - y) - (2x - y), 2(2x - y) - (2x - y)) = (2x - y, 2x - y) = f(x,y)$.
Donc f est bien un projecteur.
$E_1 = \text{Im } f = \{(x,y) \mid (x,y) = f(x,y)\} = \{(x,y) \mid x = y = 2x - y\} = \text{vect}((1,1))$.
$E_2 = \text{Ker } f = \{(x,y) \mid f(x,y) = (0,0)\} = \{(x,y) \mid 2x - y = 0\} = \text{vect}(1,2)$.
Puis $s(x,y) = 2f(x,y) - id(x,y) = (3x - 2y, 2x - 3y)$ (1/5 ?)

5. Familles de vecteurs

E est un $\mathbb{K}$-espace vectoriel.

5.1. Sur-famille, sous-famille

Définition - Sur-famille et sous-famille
Soit $(x_i)_{i \in I}$ une famille d'éléments de E.
On appelle sur-famille de $(x_i)_{i \in I}$ toute famille $(x_j)_{j \in J}$ d'éléments de E telle que $I \subset J$.
On appelle sous-famille de $(x_i)_{i \in I}$ toute famille $(x_k)_{k \in K}$ d'éléments de E telle que $K \subset I$.

Exemple - Interprétation géométrique
Dans $\mathscr{V}$, $(\vec{i}, \vec{j}, \vec{i} + 2\vec{j})$ est une sur-famille de $(\vec{i}, \vec{i} + 2\vec{j})$; $(\vec{i}, \vec{j})$ est une sous-famille de $(\vec{i}, \vec{j}, \vec{i})$.

5.2. Familles génératrices de E

Définition - Famille génératrice de F, sev de E
Soient $x_1, \dots, x_n$ n éléments de E.
On dit que la famille $(x_1, \dots, x_n)$ est génératrice de F si $F = \text{vect}(x_1, \dots, x_n)$, c'est-à-dire si

$$\forall x \in F, \exists (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \mid x = \sum_{i=1}^{n} \lambda_i \cdot x_i \quad \text{et} \quad \forall\, i \in \mathbb{N}_n, x_i \in F$$

Démonstration
C'est bien équivalent.
Si $F = \text{vect}(x_1,\dots,x_n)$, alors pour tout $i \in \mathbb{N}_n$, $x_i \in \text{vect}(x_1,\dots,x_n) = F$,
et toute combinaison linéaire des x_i est dans F.
Réciproquement, si $\forall x \in F, \exists(\lambda_1,\dots,\lambda_n) \in \mathbb{K}^n \mid x = \sum_{i=1}^n \lambda_i \cdot x_i$, alors $x \in \text{vect}(x_1,\dots,x_n)$, donc $F \subset \text{vect}(x_1,\dots,x_n)$.
et, par ailleurs, tout $x_i \in F$, donc $\text{vect}(x_1,\dots,x_n) \subset F$, car F est un s.e.v. □

Remarque - Partie génératrice
On notera en particulier que si $F = E$, on a toujours $x_i \in E$ et donc la première caractéristique suffit.
Dans ce cas, on parle parfois de : partie $\{x_1,\dots,x_n\}$ génératrice de E.

Exercice
Donner des exemples de familles génératrices de :
- $\mathbb{R}^2$
- $\mathbb{R}^3$
- le $\mathbb{R}$-e.v $\mathbb{C}$
- $\mathbb{K}_n[X]$
- dans $\mathscr{F}(\mathbb{R},\mathbb{R})$, une famille génératrice de $\{y \in \mathscr{F}(\mathbb{R},\mathbb{R}) \mid y'' + y' - 2y = 0\}$ est

Correction

Attention - Ne pas s'emballer pour une famille génératrice
Parfois, en cherchant une famille génératrice de F, on se rend compte que tout vecteur de F s'écrit comme une c.l. des vecteurs $(f_1, f_2, \dots f_p)$.
L'erreur consisterait à écrire que $F = \text{vect}(f_1, f_2, \dots f_p)$.
La seule chose qu'on ait est une inclusion : $F \subset \text{vect}(f_1, f_2, \dots f_p)$.
Il faut donc vérifier l'inclusion réciproque : est-ce que tout $f_i \in F$ (si F est un bien un espace vectoriel, cela est suffisant) ?

Remarque - Permutation
L'image d'une famille génératrice de E par une permutation des vecteurs est encore génératrice.
(Une famille est une liste ou un n-uplet et non un ensemble.
Si la famille (x_i) est génératrice de E, ajouter d'autres vecteurs à la famille ne peut pas faire perdre le caractère générateur de la famille :

Proposition - (Directe)
Toute sur-famille d'une famille génératrice de E est encore génératrice de E.

Démonstration
Si $(x_i)_{i\in I}$ est génératrice de E et que $I \subset J$.
Alors tout élément de E est une combinaison de $(x_i)_{i\in I}$ et donc de la même combinaison de $(x_i)_{i\in J}$.
Donc $E \subset \text{vect}(x_i, i \in J)$. □

En revanche, enlever des vecteurs peut être problématique

Définition - Famille génératrice minimale de E
On dit que la famille $(x_i)_{i\in I}$ est une famille génératrice minimale de E,
si toute sous-famille stricte $(x_i)_{i\in H}$ n'est pas génératrice (avec $H \subset I$ et $H \neq I$)

Définition - Généralisation (I potentiellement infini)
La famille d'éléments de E $(x_i)_{i\in I}$ (I infini) est dite génératrice de E, si $\text{vect}((x_i)_{i\in I}) = E$,
c'est-à-dire si tout élément de E s'écrit comme une combinaison linéaire d'un nombre fini de x_i.

5.3. Familles libres, liées

Définition - Famille libre (ou vecteurs linéairement indépendants)
Soit $(x_1,\dots,x_n)$ une famille de vecteurs de E.
— On dit que cette famille est une famille libre (ou que $x_1,\dots,x_n$ sont des vecteurs linéairement indépendants) si

$$\forall(\lambda_1,\dots,\lambda_n) \in \mathbb{K}^n,\ \lambda_1.x_1 + \dots + \lambda_n.x_n = 0_E \Rightarrow \lambda_1 = \dots = \lambda_n = 0$$

— Si la famille n'est pas libre, on dit qu'elle est liée (ou que $x_1,\dots,x_n$ sont des vecteurs linéairement dépendants), c'est-à-dire qu'il existe $(\lambda_1,\dots,\lambda_n) \neq (0,\dots,0)$ (non tous nuls) tel que $\lambda_1.x_1 + \dots + \lambda_n.x_n = 0_E$.

Remarque - Interprétation importante!
On a donc qu'une famille est libre si la seule combinaison linéaire des éléments de cette famille qui est nulle est celle dont les coefficients sont égaux à 0.

Pour aller plus loin - Famille libre
Une famille libre est d'une certaine façon un ensemble de vecteurs qui n'a pas d'éléments superflus.

Proposition - Cas de famille liée
Soit $(x_1,\dots,x_n)$ une famille de vecteurs de E.
— Si $n = 1$, la famille est liée si et seulement si $x_1 = 0_E$.
— Si l'un des x_i est égal à 0_E, alors la famille est liée.
— Si $x_i = x_j$ pour $i \neq j$, alors la famille est liée.
— Si l'un des vecteurs est combinaison linéaire des autres alors la famille est liée.
— Réciproquement, si $n \geqslant 2$ et si la famille est liée, alors l'un des vecteurs au moins est combinaison linéaire des autres.

Pour aller plus loin - Module (2)
Pour les espaces vectoriels si il existe $\lambda_i \neq 0$, alors $x_i = \sum_{j\neq i} \frac{-\lambda_j}{\lambda_i} x_j$, i.e. x_i est une CL des x_j.
Ce raisonnement marche bien car $\mathbb{K}$ est un corps et donc λ_i est inversible (d'où la division par λ_i).
Pour les modules, les éléments de l'anneau ne sont pas (en règle générale) inversible. C'est essentiellement ici que commence la différence entre les modules et les espaces vectoriels.

Démonstration
— $1 \cdot 0_E = 0_E$, donc (0_E) est liée.
Réciproquement si (x) est liée, alors $\exists\, \lambda \neq 0$ tel que $\lambda x = 0$, donc $x = 0$.
— Alors $0 \cdot x_1 + 0 \cdot x_2 + \dots + 1 \cdot x_i + 0 \cdot x_{i+1} + \dots 0 \cdot x_n = 0$ avec $\lambda_i \neq 0$, donc $(x_1,\dots x_n)$ liée.
— De même avec $\lambda_i = 1$, $\lambda_j = -1$ et $\forall\, k \neq i, j$, $\lambda_k = 0$…
— Si $x_i = \sum_{j\neq i} \mu_j x_j$, alors avec $\lambda_i = -1$ et $\lambda_j = \mu_j$, on a $\sum_k \lambda_k x_k = 0$ alors que les λ_k ne sont pas tous nuls.
— Réciproquement, il existe i tel que $\lambda_i \neq 0$.
Alors avec $\mu_j = \frac{-\lambda_j}{\lambda_i}$ (pour $j \neq i$), on a $x_i = \sum_{j\neq i} \mu_j x_j$.
□

Remarque - Colinéarité (DEUX vecteurs)
(x_1, x_2) est une famille liée si et seulement si x_1 et x_2 sont colinéaires i.e.

$$\exists \alpha \in \mathbb{K} \mid x_2 = \alpha x_1 \text{ ou } x_1 = \alpha x_2$$

Exercice
Compléter :
- dans $\mathbb{R}^3$ avec $x_1 = (1,0,2), x_2 = (1,1,1) = x_3$
(x_1, x_2, x_3) est
$(x_1, x_2, 2x_3)$ est
(x_1, x_2) est
(x_1) est
- dans le $\mathbb{R}$-e.v $\mathbb{C}$
$(1, i)$ est
$(1, j)$ est
$(1, i, j)$ est
- dans $\mathbb{R}^2$, $\big((1,0),(0,1)\big)$ est
- dans $\mathbb{K}_n[X]$, $(1, X, X^2, \dots, X^n)$ est
- dans $\mathscr{F}(\mathbb{R},\mathbb{R})$, $(\cos, \sin)$ est

Correction
• liée, liée, libre, libre
• libre, libre, liée
• libre
• libre
• libre

Exercice classique :
Exercice
On note $f_k : x \mapsto e^{-kx}$. Montrer que pour tout $n \in \mathbb{N}$, la famille $(f_0, \dots, f_n)$ est une famille libre de $\mathscr{F}(\mathbb{R}, \mathbb{R})$.

Correction
Le mieux est d'exploiter le déterminant de Vandermonde. Mais on ne le peut pas encore…
Soient $\lambda_k \in \mathbb{R}$ tel que $\sum_{k=0}^{n} \lambda_k \cdot f_k = 0$ (la fonction nulle).
Remarquons d'abord :

$$e^{-mx} \underset{x\to+\infty}{=} o(e^{-nx}) \Leftrightarrow \lim_{x\to+\infty} e^{(n-m)x} = 0 \Leftrightarrow n - m < 0 \Leftrightarrow n < m$$

Si il existe i tel que $\lambda_i \neq 0$, on considère $i_0 = \min\{i \mid \lambda_i \neq 0\}$.
On a donc $0 = \lambda_{i_0} f_{i_0} + \sum_{j=i_0+1}^{n} \lambda_j f_j =_{+\infty} \lambda_{i_0} f_{i_0} + o(f_{i_0})$
Ce qui implique que $\lambda_{i_0} = 0$, contradiction.
Donc pour tout $i \in [\![0, n]\!]$, $\lambda_i = 0$

La proposition suivante découle des définitions :

Proposition - Manipulation des termes de la famille
Une permutation des vecteurs ne change pas le caractère libre ou lié d'une famille.
Toute sous-famille d'une famille libre est libre.
Toute sur-famille d'une famille liée est liée.

La démonstration, simple est néanmoins pédagogique.

Démonstration
Soit $(e_i)_{i\in I}$ une famille libre. Soit $J \subset I$.
Soient $(\lambda_j)_{j\in J}$ tel que $\sum_{j\in J} \lambda_j e_j = 0$.
alors quitte à considérer $\lambda_i = 0$ si $i \notin J$, on a $\sum_{i\in I} \lambda_i e_i = 0$, donc $\forall\ i \in I$, $\lambda_i = 0$.
Et donc pour tout $j \in J$, $\lambda_j = 0$.
Soit $(e_i)_{i\in I}$ une famille liée et K tel que $I \subset K$.
Si $(e_k)_{k\in K}$ est libre, alors toute sous-famille est libre.
Mais $(e_i)_{i\in I}$ est une sous-famille non libre, donc nécessairement $(e_k)_{k\in K}$ est liée. □

Définition - Famille libre maximale
On dit que la famille $(x_i)_{i\in I}$ est une famille libre maximale (dans E), si toute sur-famille stricte $(x_i)_{i\in J}$ n'est pas libre (avec $I \subset J$ et $I \neq J$)

Définition - Généralisation
Une famille infinie $(x_i)_{i\in I}$ d'éléments de E est dite libre si toute sous-famille finie est libre.

Exemple - Famille libre infinie…
Dans $\mathbb{K}[X]$, la famille $(X^k)_{k\in\mathbb{N}}$ est une famille libre (infinie) de $\mathbb{K}[X]$ Et plus généralement :

Théorème - Degrés echelonnés
Toute famille de polynômes non nuls à coefficients dans $\mathbb{K}$ de degrés échelonnés (distincts deux à deux...) est libre dans $\mathbb{K}[X]$.

Démonstration
Soit $(P_k)_{k\in I}$ une famille (finie ou infinie) de polynôme de degrés échelonnés.
Soit $J \subset I$, une famille finie d'éléments de I.
$(P_j)_{j\in J}$ est une famille finie de polynôme de degré échelonnée.
Soit $(\lambda_j) \in \mathbb{K}^J$ tel que $\sum_{j\in J} \lambda_j P_j = 0$ (polynôme nul).
Supposons qu'il existe $j_0 \in J$ tel que $\lambda_j \neq 0$.
$\{\deg P_j \mid \lambda_j \neq 0 \text{ et } j \in J\}$ est un ensemble fini de $\mathbb{N}$.
Il admet un plus grand élément d. On note également h, l'indice de P_j tel que $\deg P_j = d$.
On a donc $\lambda_h \neq 0$.
Si on dérive d fois le polynôme nul : $\sum_{j\in J} \lambda_j P_j$, on a

$$\lambda_h P_h^{(d)} + 0 = 0$$

Or $\deg P_h = d$, donc $P_h^{(d)}$ est une constante non nulle ($d! a_d$) et donc $\lambda_h = 0$.
On a donc une contradiction et ainsi pour tout j, $\lambda_j = 0$.
La famille $(P_j)_{j\in J}$ est une famille libre. Ceci est vrai pour tout $J \subset I$. □

Pour aller plu
Dans ce genre d
faire indifférem
l'absurde ou une

5.4. Image d'une famille de vecteurs par une application linéaire

Théorème - Application linéaire et familles de vecteurs
Soit $u \in \mathscr{L}(E, F)$.
— Si $(x_i)_{i\in I}$ est une famille de vecteurs de E alors

$$u\Big(\text{vect}(x_i, i \in I)\Big) = \text{vect}\Big(u(x_i), i \in I\Big).$$

— Si u est injective alors l'image par u d'une famille libre de E est une famille libre de F.
Réciproquement, si l'image par u de n'importe quelle famille libre de E est libre, alors u est injective.
— Si u est surjective alors l'image par u d'une famille génératrice de E (s'il en existe) est une famille génératrice de F.
— Si u est un isomorphisme, l'image par u d'une base de E (s'il en existe) est une base de F. Réciproquement, si il existe une base $\mathscr{B}$ de E telle que son image par u soit une base de F, alors u est un isomorphisme.

Démonstration

— $$y \in u\Big(\text{vect}(x_i, i \in I)\Big) \Leftrightarrow \exists\,(\lambda_i) \in \mathbb{K}^I \mid y = u\Big(\sum_{i\in I} \lambda_i x_i\Big) = \sum_{i\in I} \lambda_i u(x_i) \Leftrightarrow y \in \text{vect}\Big(u(x_i), i \in I\Big)$$

— Supposons que u soit injective. Considérons $(e_1, \dots e_p)$ une famille libre de E.
Soient $\lambda_1, \dots \lambda_p$ tels que $\sum_{i=1}^{p} \lambda_i u(e_i) = 0$.
Par linéarité, on a donc $\sum_{i=1}^{p} \lambda_i e_i \in \text{Ker}\, u = \{0\}$.
Donc pour tout $i \in \mathbb{N}_p$, $\lambda_i = 0$ car $(e_1, \dots e_p)$ est libre.
Par conséquent, la famille $\big(u(e_1), u(e_2), \dots u(e_p)\big)$ est libre.
Pour la réciproque, on fait un raisonnement par l'absurde.
Supposons qu'il existe une famille libre de E, dont l'image par u n'est pas libre.
Notons i tel que $u(e_i) = \sum_{k\neq i} \mu_k u(e_k)$, donc par linéarité $e_i - \sum_{k\neq i} \mu_k e_k \in \text{Ker}\, u$.
Or le vecteur $e_i - \sum_{k\neq i} \mu_k e_k \neq 0$ (sinon $(e_1, e_2, \dots e_p)$ liée) et $\text{Ker}\, u \neq \{0\}$, et u non injective.

— Supposons que u est surjective et que $(x_i)_{i\in I}$ est génératrice de E.
Pour tout $y \in F$, $\exists\, x \in E$ tel que $u(x) = y$ (surjectivité de u).
Or $\exists\,(\lambda_i) \in \mathbb{K}^I$ tel que $x = \sum_{i\in I} \lambda_i x_i$.
Donc pour tout $y \in F$, $\exists\,(\lambda_i) \in \mathbb{K}^I$ tel que $y = u\Big(\sum_{i\in I} \lambda_i x_i\Big) = \sum_{i\in I} \lambda_i u(x_i)$.

Donc $\left(u(x_i)\right)_{i\in I}$ est une famille génératrice de F.

— Si u est un isomorphisme, il est à la fois injectif est surjectif,
donc l'image d'une base est libre et génératrice donc est une base de F.
Réciproquement,
Si il existe une base $\mathscr{B}$ de E d'image par u égale à une base de F.
Alors, comme toute base est une famille libre, d'après un critère précédent : u est injectif.
Et Im $u = u(\overline{\mathscr{B}}) = \text{vect}(\mathscr{B}') = F$, donc u est surjective.

□

Remarque - Réciproque pour la surjectivité?
Cela donnerait : Si l'image par u d'une (de toute) famille génératrice de E est une famille génératrice de F alors u est surjective.
En fait, on n'a pas besoin du fait que la famille initiale soit génératrice de E. Donc des hypothèses moins fortes.

Exercice
Retrouver l'image de l'application linéaire

$$\begin{array}{rccc} u: & \mathbb{R}^3 & \to & \mathbb{R}^2 \\ & (x,y,z) & \mapsto & (x+y-z, x-y+2z) \end{array}$$

Correction
Im $(u) = \text{vect}(u(1,0,0), u(0,1,0), u(0,0,1)) = \text{vect}((1,1),(1,-1),(-1,2)) = \mathbb{R}^2$

6. Bilan

Synthèse

- ⇝ Les espaces vectoriels est le nom savant pour les ensembles dans lesquels les éléments (vecteurs) peuvent sans difficulté s'additionner et être multiplié par des constantes d'un corps $\mathbb{K}$. Une combinaison linéaire est par définition l'opération : $(\lambda,\mu,u,v) \in \mathbb{K}^2 \times E^2 \mapsto \lambda u + \mu v \in E$. E est donc le monde des combinaisons linéaires, ou plus rapidement de la linéarité.
- ⇝ Les éléments de E s'écrivent donc les uns à partir des autres par additions, ou multiplication par une constante. Les éléments se décrivent les uns par rapport aux autres de manières multiples. Nous reviendrons sur cette non-unicité au chapitre suivant
- ⇝ Les applications linéaires sont les applications de transcriptions de structure d'espaces, tout simplement. De nombreuses définitions se développent alors : automorphismes, formes linéaires, noyau et image…
Des propriétés se filent : l'injectivité de u est toujours associée à des familles libres, la surjectivité de u est associée à des familles génératrices.
- ⇝ Deux familles d'applications linéaires : les projecteurs et les symétries vectorielles nous intéressent. La première permet de se concentrer sur une partie de l'espace; on parle de la réduction de l'espace sur ces sous-espaces.
C'est une partie importante en seconde année.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Montrer que deux espaces vectoriels sont supplémentaires
— Savoir-faire - Démontrer que F est un (s.)ev (de E)
— Savoir-faire - Montrer un espace vectoriel par famille génératrice
— Savoir-faire - Caractérisations : $x \in F \cap G$ et $x \in F+G$
— Savoir-faire - Montrer qu'une application est linéaire

Notations

Notations	*Définitions*	*Propriétés*	*Remarq*
vect(A)(=< A >)	Sous-espace vectoriel de E engendré par A	vect$(A) = \{\sum_{i=1}^{k} \lambda_i a_i \; k \in \mathbb{N}, \lambda_i \in \mathbb{K}, a_i \in A\}$	C'est le nant A.
$E = F+G$	E est la somme des espaces F et G	$\forall\, x \in E, \exists\, (y,z) \in F \times G$ tels que $x = y+z$	$F+G=$
$E = F \cap G$	E est l'intersection des espaces F et G	$\forall\, x \in E,\, x \in F$ et $x \in G$	
$E = F \oplus G$	E est la somme directe des espaces F et G	$\forall\, x \in E, \exists\, !(y,z) \in F \times G$ tels que $x = y+z$	Deux in $F \cap G =$
$F = F_1 \oplus F_2 \cdots \oplus F_k$	E est la somme directe des espaces F_i	$\forall\, x \in F, \exists\, !(x_1, x_2, \ldots x_k) \in F_1 \times F_2 \cdots \times F_k$ tels que $x = \sum_{i=1}^{k} x_i$	Deux i $F_2 + \cdots$ unique $x_i = 0$
$\mathscr{L}(E,F)$	Ensemble des applications linéaires de E vers F		On note
$GL(E)$	Groupe (linéaire) des automorphismes de E		
Im (u)	Image de l'application u	Im $(u) = \{u(x); x \in E\} \subset F$	u surjec
Ker (u)	Noyau de l'application u	Ker $(u) = \{x \in E \mid u(x) = 0\} \subset E$	u inject

Retour sur les problèmes

117. Enormément! Il faut même souvent ajouter des hypothèses, ainsi en mécanique quantique les objets sont des vecteurs d'un espace vectoriel normé muni d'un produit sesquilinéaire (=scalaire sur $\mathbb{C}$) complet. Il espace d'un espace dit de Hilbert.
118. $F \cap G$ est toujours un sev de E. Ce n'est pas le cas de $E \cup G$.
$F \cup G$ est un sev de E ssi $F \subset G$ ou $G \subset F$
119. En prenant, dans $\mathbb{R}^2$, $L = \text{vect}(0,1)$, $M = \text{vect}(1,1)$ et $N = \text{vect}(1,0)$, on trouve $M+N = \mathbb{R}^2$ et donc $L \cap (M+N) = L$, alors que $L \cap M = \{0\} = L \cap N$ et donc $L \cap M + L \cap N = \{0\}$. Pour le reste, on a les trois inclusions. A démontrer…
120. Cours : Application linéaire
121. Cours : le rôle important des projecteurs!

Chapitre 25

Espace vectoriel de dimension finie

Résumé -

Les espaces engendrés par une famille finie de vecteurs sont de dimension finie. On démontre alors que, toutes les familles libres et génératrices de cet ensemble F ont le même cardinal. Cet invariant (appelé dimension) est essentiel dans l'étude des espaces de dimension finie et permet de simplifier l'étude.
Nous concentrons sur les forme linéaire qui sont des applications linéaires des plus simples : les noyaux de ces applications sont des hyperplan (de co-dimension 1, i.e. supplémentaire à un espace de dimension 1). Dans le cas général, les applications linéaires sont des matrices (et réciproquement). Nous trouverons alors un résultat important qui formalise une heuristique sur les systèmes : le théorème du rang. Si on change de base, les applications ne changent pas, seule la matrice de description évolue. Il doit donc y avoir un lien très profond entre les matrices associées à une même application linéaire mais écrite dans des bases différentes. Matriciellement, il s'agit de la relation de similitude entre matrices…

Sommaire

1. Problèmes 490
2. Bases et dimension 491
2.1. Existence et unicité de l'écriture de tout vecteur dans une base 491
2.2. Critère pour être une base 492
2.3. Dimension d'un espace vectoriel 494
2.4. Sous-espaces vectoriels en dimension finie 498
3. Ecriture d'une application linéaire en dimension finie . . 502
3.1. Détermination 502
3.2. Matrice d'une application linéaire 504
3.3. Changements de bases 509
4. Théorème (formule) du rang et conséquences 513
4.1. Théorème du rang 513
4.2. Application du théorème du rang (Critère de bijection) 514
4.3. Itération 515
4.4. Formes linéaires et hyperplans 516
5. Rang (et noyau) d'une matrice 519
5.1. Rappel sur la résolution d'un système linéaire 519
5.2. « Action » des matrices sur $\mathbb{K}^n \equiv \mathcal{M}_{n,1}(\mathbb{K})$ 520
5.3. Image d'une matrice et famille génératrice 521
5.4. Noyau d'une matrice et famille libre 521

5.5. Théorème du rang 522
5.6. Bilan : nouveau critère d'inversibilité (pour une matrice carrée) 522
5.7. Action : $(P,Q)\cdot M \mapsto P\times M\times Q^{-1}$ 523
5.8. Matrices extraites 525
6. Bilan 526

1. Problèmes

? Problème 106 - Combinaison linéaire

Est-ce que $(2,1)$ est une combinaison linéaire de $(1,1)$ et de $(1,2)$?
Assurément ? Faut-il nécessairement connaître les nombres α et β tels que $(2,1)=\alpha(1,1)+\beta(1,2)$ pour répondre à la question ?
Et $(2,1,0)$ est une combinaison linéaire de $(1,1,1)$ et de $(1,2,1)$?

? Problème 107 - Combinaison linéaire (unique)

Et $(2,1,0)$ est une combinaison linéaire de $(1,1,1)$ de $(1,2,1)$, de $(1,2,3)$ et de $(1,-1,0)$.
Il semble que plus on ajoute de vecteurs dans la combinaison linéaire, « plus la réponse à la question précédente est vraie ».
Et y a-t-il unicité dans cette écriture ? Est-ce important ?

? Problème 108 - Coordonnées et projections

Si $\mathscr{B}=(e_1,\dots e_n)$ est une base de E, on sait que la description de chaque vecteur est unique :

$$\forall\, x\in E, \exists!(x_1,\dots x_n) \qquad \text{tel que} x=\sum_{i=1}^{n} x_i e_i$$

Notons $[\cdot]_i^{\mathscr{B}} : x\mapsto x_i$. Alors clairement $[\lambda x+\mu y]_i^{\mathscr{B}}=\lambda[x]_i^{\mathscr{B}}+\mu[y]_i^{\mathscr{B}}$, donc cette application est linéaire. C'est l'application i-ieme coordonnées.
Et si au lieu de découper E en espace de dimension 1, on le découpe en espace plus gros : $E=\oplus_{i=1}^{r} E_i$.
Que peut-on dire de $x\mapsto x_i$ avec $x=\sum_{i=1}^{r} x_i$ où pour tout $i\in\mathbb{N}_r$, $x_i\in E_i$.

? Problème 109 - $f\in\mathscr{L}(E,F)$ avec E et F de dimension finie

On suppose que $\mathscr{B}=(e_1,\dots e_p)$ est une base de E et $\mathscr{C}=(f_1,\dots f_n)$, une base de F.
Alors $f\in\mathscr{L}(E,F)$ est parfaitement connue par l'ensemble des valeurs

$$\forall\, j\in\mathbb{N}_p, \qquad f(e_j)=\sum_{i=1}^{n}\lambda_{i,j} f_i$$

Donc la connaissance de f est équivalente à celle de $(\lambda_{I,j})$, et donc à celle d'une matrice.
On a donc, pour deux bases fixées a priori $\mathscr{B}=(e_1,\dots e_p)$ est une base de E et $\mathscr{C}=(f_1,\dots f_n)$, une bijection :

$$\mathscr{L}(E,F)\longrightarrow\mathscr{M}_{n,p}$$

Les opérations $+, \times \dots$ se correspondent-elles?
Et plus généralement, comment ces deux points de vue s'éclairent-ils mutuellement?

Problème 110 - Changement de bases

On vient de voir que pour deux bases fixées a priori $\mathscr{B} = (e_1, \dots e_p)$ est une base de E et $\mathscr{C} = (f_1, \dots f_n)$, on a une bijection :

$$\mathscr{L}(E,F) \longrightarrow \mathscr{M}_{n,p}$$

Et si on change de base, mais qu'on garde l'application linéaire f, que peut-on dire des matrices qu'on obtient?

2. Bases et dimension

2.1. Existence et unicité de l'écriture de tout vecteur dans une base

Définition - Base d'un espace vectoriel
On dit qu'une famille de vecteurs de E est une base de E si elle est une famille libre et génératrice de E.

Attention - Non unicité
On dit bien UNE base et non LA base de E...

Exemple - Nombreux exemples
- une base de $\mathbb{R}^2$ est
- une base du $\mathbb{R}$-e.v $\mathbb{C}$ est
- une base de $\{y \in \mathscr{F}(\mathbb{R},\mathbb{R}) \mid y'' + y' - 2y = 0\}$ est

Proposition - Bases canoniques de $\mathbb{K}^n$, de $\mathscr{M}_{n,p}(\mathbb{K})$ et de $\mathbb{K}_n[X]$
On définit la famille $(e_i)_{1 \leqslant i \leqslant n}$ de $\mathbb{K}^n$ par

$$e_1 = (1,0,\dots,0); e_2 = (0,1,0,\dots,0); \dots; e_n = (0,\dots,0,1).$$

Alors cette famille est une base du $\mathbb{K}$-e.v $\mathbb{K}^n$ appelée base canonique de $\mathbb{K}^n$.
La base canonique de $\mathscr{M}_{n,p}(\mathbb{K})$ est la famille $(E_{i,j})_{i \in \mathbb{N}_n, j \in \mathbb{N}_p}$.
La base canonique de $\mathbb{K}_n[X]$ est $(1, X, X^2, \dots, X^n) = (X^i)_{0 \leqslant i \leqslant n}$, celle de $\mathbb{K}[X]$ est $(X^i)_{i \in \mathbb{N}}$.

Pour aller plus loin - Pour les impatients...
Existent-ils deux bases de $\mathbb{C}^4$ telles que les seuls vecteurs communs à ces deux bases soient $(,0,1,1)$ et $(1,1,0,0)$?
A quelle condition portant sur le scalaire x, les vecteurs $(1,1,1)$ et $(1,x,x^2)$ forment-ils une base de $\mathbb{R}^3$?
A quelle condition portant sur le scalaire x, les vecteurs $(0,1,x)$, $(x,0,1)$ et $(x,1,1+x)$ forment-ils une base de $\mathbb{R}^3$?

Exercice
Déterminer une base du $\mathbb{R}$-e.v. $\mathbb{C}^n$.

Correction
Une base est par exemple $(e_1, e_2, \dots e_{2n-1}, e_{2n})$ donnée par

$$e_{2k+1} = (\underbrace{0,\dots,0}_{k \text{ termes}}, 1, \underbrace{0\dots0}_{n-1-k \text{ termes}}) \qquad e_{2k+2} = (\underbrace{0,\dots,0}_{k \text{ termes}}, i, \underbrace{0\dots0}_{n-1-k \text{ termes}})$$

Remarque - Démonstration de la base canonique
On ne démontre pas le nom de canonique. Il s'agit en fait d'une trace de l'histoire des mathématiques.
Quant à la démonstration de la base, on voit que c'est celle qu'on utilise depuis toujours...

Théorème - Caractérisation de la base
Une famille $\mathscr{B} = (e_i)_{1 \leqslant i \leqslant n}$ de vecteurs de E est une base de E si et seulement si, pour tout $x \in E$, il existe une unique famille $(\lambda_i)_{1 \leqslant i \leqslant n} \in \mathbb{K}^n$ telle que

$$x = \sum_{i=1}^{n} \lambda_i \cdot e_i$$

$\lambda_1, \dots, \lambda_n$ s'appellent les coordonnées (ou composantes) de x dans la base $\mathscr{B}$.

Heuristique - La fonction Φ
D'après ce théorème, si $\mathscr{B}$ est une base de E, alors

$$\Phi_{\mathscr{B}} : \mathbb{K}^n \longrightarrow E, \qquad (\lambda_1, \lambda_2, \dots \lambda_n) \longmapsto \sum_{i=1}^{n} \lambda_i e_i$$

est une application bijective : $\forall\, x \in E, \exists!(\lambda_i)_i$ tel que $x = \sum_{i=1}^{n} \lambda_i \cdot e_i$.
Les coordonnées de x sont alors les antécédents de x par $\Phi_{\mathscr{B}}$.
Pour la démonstration qui va suivre, on va montrer :
— $\Phi_{\mathscr{B}}$ est injective si et seulement si $\mathscr{B}$ est libre.
— $\Phi_{\mathscr{B}}$ est surjective si et seulement si $\mathscr{B}$ est génératrice de E.

Démonstration
$\Phi_{\mathscr{B}}$ est bien définie.
$\Phi_{\mathscr{B}}$ est surjective ssi $\forall\, x \in E, \exists\, (\lambda_1, \dots \lambda_n) \in \mathbb{K}^n$ tel que $x = \Phi_{\mathscr{B}}((\lambda_i)) = \sum_{i=1}^{n} \lambda_i \cdot e_i$.
Donc $\Phi_{\mathscr{B}}$ est surjective si et seulement si $\mathscr{B}$ est génératrice de E.
$\Phi_{\mathscr{B}}$ est injective ssi $[\forall\, (\lambda_i)_i, (\mu_i)_i \in \mathbb{K}^n, \Phi_{\mathscr{B}}((\lambda_i)) = \Phi_{\mathscr{B}}((\mu_i)) \Longrightarrow (\lambda_i)_i = (\mu_i)_i]$
ssi $[\forall\, (\lambda_i)_i, (\mu_i)_i \in \mathbb{K}^n, \sum_{i=1}^{n} (\lambda_i - \mu_i) e_i = 0 \Longrightarrow \forall\, i \in \mathbb{N}_n, \lambda_i = \mu_i]$
Donc $\Phi_{\mathscr{B}}$ est injective si et seulement si $\mathscr{B}$ est une famille libre. Finalement :
$\mathscr{B}$ est une base de E
si et seulement si $\mathscr{B}$ est libre et génératrice de E
si et seulement si $\Phi_{\mathscr{B}}$ est injective et surjective
si et seulement si $\Phi_{\mathscr{B}}$ est bijective
si et seulement si pour $x \in E$, il existe une unique $(\lambda_i)_{1 \leqslant i \leqslant n} \in \mathbb{K}^n$ telle que $x = \sum_{i=1}^{n} \lambda_i \cdot e_i$ □

Attention - Ne pas oublier
On dit qu'*« une famille est génératrice (ou une base)**DE E** »*, si on oublie l'objet indirect (« de ... ») cela ne veut rien dire.
En revanche, une famille est libre, indépendamment de l'espace vectoriel considéré (mais pas du corps). On peut donc se contenter de *« une famille est libre »*.

Remarque - Base infinie
Pour une base infinie on a un résultat similaire avec une famille presque nulle $(\lambda_i)_{i \in I}$.

Application - Exemples classiques
- les coordonnées de $a + ib$ dans la base $(1, i)$ du $\mathbb{R}$-e.v $\mathbb{C}$ sont
- les coordonnées de $(x_1, \dots, x_n) \in \mathbb{K}^n$ dans la base canonique de $\mathbb{K}^n$ sont

2.2. Critère pour être une base

Proposition - Base
Soit $\mathscr{F} = (e_1, e_2, \dots e_p)$ une famille d'éléments de E.
On a les équivalences :
(i) $\mathscr{F}$ est une base de E.
(ii) $\mathscr{F}$ est une famille libre maximale (dans E).

(iii) $\mathscr{F}$ est une famille génératrice minimale de E.

On commence par démontrer deux lemmes :

Lemme - Complétion libre
Soient $(e_1,\dots,e_p)$ une famille libre de E et $x \in E$.
$x \notin \text{vect}(e_1,\dots,e_p)$ si et seulement si $(e_1,\dots,e_p,x)$ est encore libre.
ou $x \in \text{vect}(e_1,\dots,e_p)$ si et seulement si $(e_1,\dots,e_p,x)$ est lié

Lemme - Réduction liée
Soit $(e_1,\dots,e_p,e_{p+1})$ une famille de E.
$e_{p+1} \in \text{vect}(e_1,\dots,e_p)$ si et seulement si $\text{vect}(e_1,\dots,e_p,e_{p+1}) = \text{vect}(e_1,\dots,e_p)$

Heuristique - Interprétation en terme de famille libre maximale et famille génératrice minimale
Si $(e_1,\dots,e_p)$ une famille libre de E et $x \notin \text{vect}(e_1,\dots,e_p)$, alors $(e_1,\dots e_p)$ n'est pas maximale.
Si $(e_1,\dots,e_p,e_{p+1})$ une famille génératrice de E et $e_{p+1} \in \text{vect}(e_1,\dots,e_p)$, alors $(e_1,\dots e_p,e_{p+1})$ n'est pas minimale.

On commence par démontrer les lemmes puis la proposition.

Démonstration
Lemme de la complétion libre
Si $x \in \text{vect}(e_1,\dots e_p)$, alors x est une c.l. non triviale de $(e_1,\dots e_p)$.
Donc la famille $(e_1,\dots e_p,x)$ ne peut pas être libre.
Réciproquement. Supposons que $x \notin \text{vect}(e_1,\dots e_p)$ (famille libre).
Soient $\lambda_1,\dots\lambda_p,\lambda \in \mathbb{K}$ tels que $\sum_{i=1}^{p} \lambda_i \cdot e_i + \lambda \cdot x = 0$.
Si $\lambda \neq 0$, alors $x = \sum_{i=1}^{p} \frac{-\lambda_i}{\lambda} e_i$, donc $x \in \text{vect}(e_1,\dots e_p)$ ce qui est faux.
Donc $\lambda = 0$, et donc $\sum_{i=1}^{p} \lambda_i \cdot e_i = 0$ et donc $\forall\, i,\ \lambda_i = 0$
Par conséquent, la famille $(e_1,\dots,e_p,x)$ est libre.
Lemme de la réduction liée
Si $\text{vect}(e_1,\dots e_p,e_{p+1}) = \text{vect}(e_1,\dots e_p)$.
Alors e_{p+1} élément du premier ensemble est dans le second.
Donc $e_{p+1} \in \text{vect}(e_1,\dots e_p)$.
Réciproquement. Notons qu'on a évidemment l'inclusion : $\text{vect}(e_1,\dots,e_p) \subset \text{vect}(e_1,\dots,e_p,e_{p+1})$.
Et si $x \in \text{vect}(e_1,\dots,e_p,e_{p+1})$, alors $x = \sum_{i=1}^{p+1} x_i e_i = \sum_{i=1}^{p} x_i e_i + x_{p+1} e_{p+1}$.
Et comme $e_{p+1} = \sum_{i=1}^{p} a_i e_i$, on a donc $x = \sum_{i=1}^{p} (x_i + x_{p+1} a_i) e_i$.
Et ainsi $\text{vect}(e_1,\dots,e_p,e_{p+1}) \subset \text{vect}(e_1,\dots,e_p)$.
Par double inclusion, on a le résultat attendu □

Démonstration
On démontre les résultats par implications successives $(i) \Rightarrow (ii) \Rightarrow (iii)$.
— Si $\mathscr{F} = (e_1,\dots,e_n)$ est une base de E.
C'est donc une famille libre.
Et si $x \in E$, alors x s'écrit comme une combinaison linéaire des éléments de $\mathscr{F}$.
Ainsi $(e_1,e_2,\dots,e_n,x)$ n'est pas libre. Et donc $(e_1,e_2,\dots e_n)$ est libre maximale.

— Si $\mathscr{F} = (e_1,\dots,e_n)$ est libre maximale,
alors pour tout $x \in E$, nécessairement $(e_1,e_2,\dots,e_n,x)$ n'est pas libre et donc $x \in \text{vect}(e_1,\dots e_n)$.
et donc $(e_1,\dots e_n)$ est génératrice de E.
Elle est minimale. En effet, considérons $i \in \mathbb{N}_n$.
alors si $\mathscr{F} \setminus \{e_i\}$ était génératrice de E, alors $e_i \in \text{vect}(e_1,\dots,e_{i-1},e_{i+1},\dots e_n)$
et comme $\mathscr{F} \setminus \{e_i\}$ est toujours libre, on aurait $(e_1,e_2,\dots e_n)$ non libre. Absurde.

— Si $\mathscr{F} = (e_1,\dots e_n)$ est génératrice minimale, alors $\mathscr{F}$ est génératrice.
Si $\mathscr{F}$ est liée, alors il existe $i \in \mathbb{N}_n$ tel que e_i est une combinaison linéaire des autres.
Donc $E = \text{vect}(e_1,\dots e_n) = \text{vect}(e_1,\dots e_{i-1},e_{i+1}\dots,e_n)$, par réduction liée.
et ainsi $\mathscr{F}$ ne serait pas minimal. Absurde. Donc $\mathscr{F}$ est libre.
□

2.3. Dimension d'un espace vectoriel

Existence de bases

Définition - Espace de dimension finie
Un $\mathbb{K}$-espace vectoriel E est dit de dimension finie s'il admet une famille génératrice finie.
Par convention $\{0_E\}$ est un espace de dimension finie.
S'il n'est pas de dimension finie, E est dit de dimension infinie.

On a le théorème suivant très important :

Théorème - Théorème de la base incomplète (lemme de Steinitz)
Soit $E \neq \{0_E\}$ un espace vectoriel de dimension finie.
Soit $\mathscr{E} = (e_1,\dots,e_p)$ une famille libre de E et $\mathscr{F} = (f_1,\dots,f_q)$ une famille génératrice de E, alors : il existe une base de E de la forme $\mathscr{B} = (e_1,\dots,e_p,e_{p+1},\dots,e_n)$ où $\{e_{p+1},\dots,e_n\} \subset \mathscr{F}$ (quitte à être vide).
En d'autres termes on peut compléter une famille libre de E en une base avec des vecteurs pris dans une famille génératrice.

Démonstration
On considère $N = \{\text{card}(\mathscr{E},\mathscr{G})$ tel que $\mathscr{G} \subset \mathscr{F}$ et $(\mathscr{E},\mathscr{G})$ libre$\}$.
— N est non vide. Car $p \in N$, puisqu'avec $\mathscr{G} = \emptyset$, on peut créer un élément de N.
— $N \subset \mathbb{N}$.
— N est majorée par $p+q$.
Donc N admet un plus grand élément, que l'on note n. Nécessairement : $p \leqslant n \leqslant p+q$.
On note alors $\mathscr{G}_0$ la sous-famille de $\mathscr{F}$ tel que $(\mathscr{E},\mathscr{G}_0)$ est libre et $\text{card}(\mathscr{E},\mathscr{G}_0) = n$.
Par construction, $(\mathscr{E},\mathscr{G}_0)$ est libre.
En fait elle est maximale. On peut aussi montrer qu'elle est génératrice de E :
Pour tout $f \in \mathscr{F}$, $f \in \text{vect}(\mathscr{E},\mathscr{G}_0)$ (sinon, on compléterait).
Donc $E = \text{vect}\mathscr{F} \subset \text{vect}(\mathscr{E},\mathscr{G}_0)$.
Ainsi, $\text{vect}(\mathscr{E},\mathscr{G}_0)$ est une base de E.
Le lemme de Steinitz est démontré □

Remarque - Constructivité? Algorithme
La démonstration précédente est efficace et propre. Mais elle souffre du fait qu'elle ne dit pas concrètement comment on s'y prend de manière efficace.
On pire, il s'agit de faire toutes les 2^q réunions $(\mathscr{E},\mathscr{G})$ pour $\mathscr{G} \subset \mathscr{F}$.
On a un algorithme de complétion de famille libre, en une base (si l'espace est de dimension finie) - en q étapes :

Savoir faire - Base incomplète
Pour le théorème de la base incomplète, on exploite un algorithme plus efficace. On suit l'algorithme suivant :

```
B=[e[i] for i in range(1,p)]
E=vect(B)
for i in range(q):
    if f[i] notin E :
        B=B+[f[i]]
        E=vect(B)
return(B)
```

L'algorithme termine car il est paramétré avec une boucle `for`.
L'algorithme renvoie la famille libre maximale, contenant e_i, pour tout

$i \in \mathbb{N}_p$.
Par construction, pour tout $i \in \mathbb{N}_q$, $f_i \in \text{vect}(B)$,
— en effet, ou bien f_i n'appartenait pas à B au moment du test, et alors, on l'a mis dans B,
— ou bien il en faisait partie et toujours à la fin.
D'après le lemme de réduction : $\text{vect}\mathscr{F} = E \subset \text{vect}(B)$.
Donc B est également une famille génératrice de E.
Il faut également montrer que B est une famille libre.
En fait, pour tout i, B_i est libre d'après le lemme de complétion libre.
C'est donc également le cas en fin d'algorithme.

Application - Compléter $\mathscr{E} = ((1,1,1),(1,-1,-1))$ en une base de $\mathbb{R}^3$.
On considère la base de canonique $\mathscr{F} = ((1,0,0),(0,1,0),(0,0,1))$ de $\mathbb{R}^3$.
$(1,0,0) \in \text{vect}((1,1,1),(1,-1,-1))$, car $(1,0,0) = \frac{1}{2}((1,1,1)+(1,-1,-1))$
$(0,1,0) \notin \text{vect}((1,1,1),(1,-1,-1))$: si $(a,b,c) \in \text{vect}((1,1,1),(1,-1,-1))$, alors $b = c$.
On considère alors $\text{vect}((1,1,1),(1,-1,-1),(0,1,0))$.
Enfin, $(0,0,1) \in \text{vect}((1,1,1),(1,-1,-1),(0,1,0))$ car $(0,0,1) = \frac{1}{2}((1,1,1)-(1,-1,-1)-2(0,1,0))$.
Donc une base de $\mathbb{R}^3$ complétée à partir de E est $((1,1,1),(1,-1,-1),(0,1,0))$.
On remarque qu'elle est constituée de 3 *vecteurs.*
A partir d'un ensemble réduit à l'unique élément $\{0\}$,

Corollaire -
Si E, non réduit au vecteur nul, est de dimension finie, alors de toute famille génératrice de E on peut extraire une base.

Corollaire -
Tout espace vectoriel de dimension finie, non réduit au vecteur nul, admet une base.

Cardinal d'une base

En fait, on a mieux, en terme de cardinaux

Proposition - Relation entre cardinaux de familles libres/familles génératrices
Soit $\mathscr{L}$ une famille libre de E et $\mathscr{G}$ une famille génératrice finie de E, alors $\mathscr{L}$ est finie et
$$\text{Card}\mathscr{L} \leqslant \text{Card}\mathscr{G}$$

Heuristique - Amélioration du lemme de Steinitz
Pour la démonstration, on améliore la démonstration du lemme de Steinitz.
En cherchant un invariant : comment transformer un à un les élément de $\mathscr{G}$ en élément de $\mathscr{L}$ tout en gardant la génération de E.
On démontre que pour tout $s \leqslant \text{card}(\mathscr{L}) = p$ ($q = \text{card}(\mathscr{G})$) :
il existe $I_s \subset \mathbb{N}_q$, tel que $\text{card}(I_s) = q - s$ et $E = \text{vect}\left((e_i)_{i\in\mathbb{N}_s}, (f_j)_{j\in I_s}\right)$

Notons que la démonstration qui suit est en fait constructive!

Démonstration
On note donc $p = \text{card}(\mathscr{L})$ et $q = \text{card}(\mathscr{G})$. Par récurrence, on démontre que pour tout $s \in [\![0,p]\!]$,
$\mathscr{P}_s$: « il existe $I_s \subset \mathbb{N}_q$, tel que $\text{card}(I_s) = q - s$ et $E = \text{vect}\left((e_i)_{i\in\mathbb{N}_s}, (f_j)_{j\in I_s}\right)$. »
— $\mathscr{P}_0$ est vraie.

— Démontrons $\mathscr{P}_1$, même si ce n'est pas nécessaire.
$e_1 \in E$, donc il existe $(\lambda_j)_{j\in\mathbb{N}_q} \in \mathbb{K}^q$ tel que $e_1 = \sum_{j=1}^{q} \lambda_j f_j$.
Comme e_1 est non nul (sinon $(e_1,\dots e_p)$ ne serait pas libre), il existe j_0 tel que $\lambda_{j_0} \neq 0$.
Et donc avec $I_1 = \mathbb{N}_q \setminus \{j_0\}$, on trouve $f_{j_0} = \frac{1}{\lambda_{j_0}} e_1 - \sum_{j\neq j_0} \frac{\lambda_j}{\lambda_{j_0}} f_j$.
Par réduction lié : $E = \text{vect}(e_1, f_1 \dots f_q) = \left((e_1, (f_j)_{j\in I_1}\right)$.
— Soit $s \in \mathbb{N}_{p-1}$. On suppose que $\mathscr{P}_s$ est vraie.
$e_{s+1} \in E = \text{vect}\left((e_i)_{i\in\mathbb{N}_s}, (f_j)_{j\in I_s}\right)$, d'après $\mathscr{P}_s$.
Donc il existe $(\mu_i)_{i\in\mathbb{N}_s}, (\lambda_j)_{j\in I_s} \in \mathbb{K}^q$ tel que $e_{s+1} = \sum_{j\in\mathbb{N}_s} \mu e_j + \sum_{j\in I_s} \lambda_j f_j$.
Comme $(e_1,\dots e_s, e_{s+1})$ est libre, nécessairement, il existe j_s tel que $\lambda_{j_s} \neq 0$.
Et donc, au passage, nécessairement l'ensemble I_s est non vide.
Et donc avec $I_{s+1} = I_s \setminus \{j_s\}$, on trouve $f_{j_s} = \frac{1}{\lambda_{j_s}} e_{s+1} - \sum_{i\in\mathbb{N}_s} \frac{\mu_i}{\lambda_{j_s}} - \sum_{j\in I_{s+1}} \frac{\lambda_j}{\lambda_{j_s}} f_j$.
Par réduction lié : $E = \text{vect}\left((e_i)_{i\in\mathbb{N}_s}, (f_j)_{j\in I_s}\right) = \text{vect}\left((e_i)_{i\in\mathbb{N}_{s+1}}, (f_j)_{j\in I_{s+1}}\right) = \text{vect}\left((e_i)_{i\in\mathbb{N}_{s+1}}, (f_j)_{j\in I_{s+1}}\right)$.
Donc $\mathscr{P}_{s+1}$ est vraie.
Le résultat obtenu avec $\mathscr{P}_p$ donne le théorème de la base incomplète et nécessairement $I_p \neq \emptyset$, donc $\text{card}(I_p) = q - p \geqslant 0$, donc $p \leqslant q$. □

Autre interprétation :

Corollaire - Maximalité de liberté
Soit $(e_1,\dots,e_n)$ une famille de vecteurs de E.
Soit $(x_j)_{j\in J}$ une famille de vecteurs de E qui sont combinaisons linéaires de $(e_1,\dots,e_n)$ (i.e. : $\forall\ j \in J,\ x_j \in \text{vect}(e_1, e_2, \dots e_n)$).
Si $\text{Card}J \geqslant n+1$ alors nécessairement la famille $(x_j)_{j\in J}$ est liée.

Si l'espace vectoriel possède une famille libre infinie, alors il est de dimension infinie (au sens : il n'est pas de dimension finie).

Corollaire - Espace vectoriel de dimension infinie
Il existe des espaces vectoriels de dimension infinie. C'est en particulier le cas de $\mathbb{R}^{\mathbb{N}}$ ou de $\mathscr{F}(\mathbb{R},\mathbb{R})$.

Pour aller plus loin - Famille libre maximale/génératrice minimale
On pourrait aussi parle de famille maximale libre (de plus grand cardinal), ou de famille minimale génératrice (de plus petit cardinal).
Le cardinal de toutes ces familles est le même : c'est la dimension de l'espace

Pour aller plus loin - Module (3)
On dit qu'un module est de type fini, s'il est engendré par une famille fini d'éléments.
On peut montrer que M est un A-module de type fini s'il existe une bijection linéaire de M sur A^n (n étant la taille de la famille fini engendrant M). On dit qu'il est libre, s'il possède une base.
Enfin, on s'intéresse souvent pour des raisons de décomposition structurelle aux A-module de torsion M (de type fini), les modules de torsion vérifiant :
$$\forall\ x \in M, \exists\ a \in A \mid ax = 0$$

Démonstration
Par exemple : notons pour tout $m \in \mathbb{N}$: $\delta^m = (\delta_{m,n})_{n\in\mathbb{N}}$, la suite nulle en tout terme sauf le m^e qui vaut 1.
La famille $(\delta^m)_m$ est une famille infinie libre de $\mathbb{R}^{\mathbb{N}}$.
De même : notons pour tout $m \in \mathbb{Z}$, $f_m : x \mapsto \begin{cases} 1 & \text{si} \quad x \in [m, m+1[\\ 0 & \text{sinon} \end{cases}$.
La famille $(f_m)_m$ est une famille infinie libre de $\mathscr{F}(\mathbb{R},\mathbb{R})$.
□

Théorème - Dimension constante
Toutes les bases d'un $\mathbb{K}$-espace vectoriel E de dimension finie, non réduit au vecteur nul, ont même cardinal.

Démonstration
Si E est de dimension finie, il admet une base $\mathscr{B}$, de cardinal fini. Notons $n = \text{Card}\mathscr{B}$.
Soit $\mathscr{B}'$ une autre base de E.
Alors $\mathscr{B}'$ est libre, et $\mathscr{B}$ est génératrice de E, donc $\text{Card}\mathscr{B}' \leqslant \text{Card}\mathscr{B}$.
Alors $\mathscr{B}$ est libre, et $\mathscr{B}'$ est génératrice de E, donc $\text{Card}\mathscr{B} \leqslant \text{Card}\mathscr{B}'$.
Donc pour tout $\mathscr{L}$ de E, $\text{Card}\mathscr{B}' = \text{Card}\mathscr{B} = n$. □

Définition - Dimension
Soit E un $\mathbb{K}$-e.v. de dimension finie, non réduit au vecteur nul.
On appelle dimension de E le cardinal commun de toutes ses bases.
On le note $\dim E$ ou $\dim_{\mathbb{K}} E$.
Par convention $\dim\{0_E\} = 0$.

Exemple - Compléter

- $\dim_{\mathbb{K}} \mathbb{K}^n =$
- $\dim_{\mathbb{R}} \mathbb{C} =$
- $\dim_{\mathbb{R}} \mathbb{C}^n =$
- $\dim_{\mathbb{K}} \mathbb{K}_n[X] =$
- Pour $a \in \mathscr{C}(\mathbb{R},\mathbb{K})$, $\dim_{\mathbb{K}} \{y \in \mathscr{F}(\mathbb{R},\mathbb{K}) \mid y' + a(t)y = 0\} =$
- Pour $(a,b,c) \in \mathbb{K}^3$ fixé, $a \neq 0$, $\dim_{\mathbb{K}} \{y \in \mathscr{F}(\mathbb{R},\mathbb{K}) \mid ay'' + by' + cy = 0\} =$
- Pour $(a,b,c) \in K^3$, $a \neq 0, c \neq 0$, $\dim_{\mathbb{K}} \{(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}} \mid au_{n+2} + bu_{n+1} + cu_n = 0\} =$

Théorème - Conséquence sur les cardinaux

Soit E un $\mathbb{K}$-e.v. de dimension $n \geqslant 1$. Alors :

— Une famille libre de E de cardinal p vérifie $p \leqslant n$ et c'est une base si et seulement si $p = n$.

— Une famille génératrice de E de cardinal p vérifie $p \geqslant n$ et c'est une base si et seulement si $p = n$.

Démonstration

E est de dimension n, on note $\mathscr{B}$ une base de E. On sait que $\text{Card}\mathscr{B} = n$.
Si $\mathscr{L}$ est libre, on a vu que $\text{Card}\mathscr{L} \leqslant n$.
Supposons en outre que $\text{Card}\mathscr{L} = n$.
Si $\mathscr{L}$ n'est pas maximale, alors on peut obtenir une famille libre avec plus de vecteurs qu'une famille génératrice (la base).
Impossible. Donc $\mathscr{L}$ est maximale, c'est donc une base de E La réciproque est assurée.

Si $\mathscr{G}$ est génératrice de E, on a vu que $p \geqslant n$.
Supposons en outre que $\text{Card}\mathscr{G} = n$.
Si $\mathscr{G}$ n'est pas minimale, alors on peut obtenir une famille génératrice de $n-1$ vecteurs, avec un vecteur de moins que la famille libre qui est la base. Impossible.
Donc $\mathscr{G}$ est génératrice minimale de E. Il s'agit donc d'une base de E.
La réciproque est assurée.
□

Savoir faire - Montrer qu'une famille est une base

En général pour montrer qu'une famille d'un $\mathbb{K}$-e.v. de **dimension** n **connue** est une base on montre qu'elle est **libre de cardinal** n.
(Dans de rares cas, on montre que la famille est génératrice et du bon cardinal).

Exemple - Dans $E = \mathbb{R}^n$

La famille $(f_1,\dots,f_n)$ définie par

$$f_1 = (1,0,\dots,0), \quad f_2 = (1,1,0,\dots,0),\dots, f_n = (1,1,\dots,1)$$

est une base de $\mathbb{R}^n$.

Exercice

Montrer que la famille des polynômes $(N_k)_{0\leqslant k\leqslant n}$ est une base de $\mathbb{R}_n[X]$. Avec

$$N_0 = 1 \qquad \forall\, k \geqslant 1 : N_k = \frac{X\times(X-1)\cdots(X-k+1)}{k!}$$

(On appelle cette base, la base de Newton. Elle est en particulier intéressante pour : $\forall\, h \in \mathbb{Z}$, $N(h) \in \mathbb{Z}$)

Correction

Pour tout k, $\deg(N_k) = k$, donc $(N_0, N_1, \dots N_n)$ est une famille de degrés échelonnés, elle est donc libre.
En outre, elle est composée de $n+1 = \dim(\mathbb{R}_n[X])$ éléments. C'est une base de $\mathbb{R}_n[X]$.

Dimension d'un produit

Théorème - Dimension d'un produit cartésien

Soient E, F deux $\mathbb{K}$-e.v. de dimension finie. Alors $E \times F$ est de dimension finie et

$$\dim E \times F = \dim E + \dim F.$$

Démonstration

On note, pour simplifier, $\dim E = n$ et $\dim F = p$.
Notons $\mathscr{B} = (e_1, e_2, \dots e_n)$ une base de E et $\mathscr{B}' = (f_1, f_2, \dots f_p)$ une base de F.

$$\forall\, x = (a,b) \in E\times F \exists\,!(a_1,\dots a_n) \in \mathbb{K}^n, \exists\,!(b_1,\dots b_p) \in \mathbb{K}^p, x = \left(\sum_{i=1}^{n} a_i e_i, \sum_{j=1}^{p} b_j e_j\right) = \sum_{i=1}^{n} a_i(e_i,0) + \sum_{j=1}^{p} b_i(0,f_j)$$

Donc $\mathscr{B}'' = \big((e_1,0),(e_2,0)\dots,(e_n,0),(0,f_1),(0,f_2)\dots(0,f_p)\big)$ est une base de $E\times F$.
Ainsi $\dim(E\times F) = n + p = \dim E + \dim F$. □

Par récurrence :

Corollaire - Dimension d'un produit fini d'espaces vectoriels

Soient $E_1,\dots,E_k$ des $\mathbb{K}$-e.v. de dimensions finies respectivement $n_1,\dots,n_k$.
Alors $E_1 \times \cdots \times E_k$ est de dimension finie égale à $n_1 + \cdots + n_k$.

2.4. Sous-espaces vectoriels en dimension finie

Dimension d'un s.e.v

Théorème - Dimension d'un sous-espace vectoriel

Soit E un $\mathbb{K}$-e.v. de dimension finie. Soit F un s.e.v de E.
Alors F est de dimension finie, avec $\dim F \leqslant \dim E$.
De plus

$$\dim F = \dim E \text{ si et seulement si } E = F.$$

Démonstration

F est un sev de E.
F est dimension $\leqslant k$ est équivalent à : toutes les familles libres de F ont un cardinal $\leqslant k$.
Supposons donc que F n'est pas de dimension finie, ou avec une dimension $> n$.
Alors (contraposée) il existe une famille libre de F d'au moins $n+1$ éléments.
Mais ces éléments sont également dans E (sur le même corps $\mathbb{K}$), donc $\dim E \geqslant n+1$. Ce qui est faux. □

Savoir faire - Montrer que deux espaces vectoriels sont égaux

Pour montrer que deux $\mathbb{K}$-e.v. E et F de **dimension finie** sont égaux, on montre généralement une inclusion et l'égalité des dimensions.

Corollaire - S.e.v. de $\mathbb{R}^2$ et $\mathbb{R}^3$

Les sous-espaces vectoriels de $\mathbb{R}^2$, autres que $\{0_{\mathbb{R}^2}\}$ et $\mathbb{R}^2$, sont les droites vectorielles.
Les sous-espaces vectoriels de $\mathbb{R}^3$, autres que $\{0_{\mathbb{R}^3}\}$ et $\mathbb{R}^3$, sont les droites vectorielles et les plans vectoriels.

Définition - Rang d'une famille de vecteurs

Soit $(x_1,\dots,x_p)$ une famille finie de vecteurs d'un $\mathbb{K}$-espace vectoriel.
On appelle rang de la famille $(x_1,\dots,x_p)$ la dimension du sous-espace vectoriel $\text{vect}(x_1,\dots,x_p)$:

$$\text{rg}\,(x_1,\dots,x_p) = \dim \text{vect}(x_1,\dots,x_p)$$

Comme $(x_1,\dots,x_p)$ est une famille génératrice de $\text{vect}(x_1,\dots,x_p)$, on peut affirmer

Proposition - Majorant et
$\text{rg}\,(x_1,\dots,x_p) \leqslant p$. Et

$$\text{rg}\,(x_1,\dots,x_p) = p \Longrightarrow (x_1,\dots,x_p) \text{ est libre}$$

Sommes et supplémentaires

Théorème - Base et dimension d'une somme directe
Soient E un $\mathbb{K}$-e.v. de dimension finie, E_1 et E_2 deux s.e.v de E
Soient $(e_1,\dots,e_p)$ une base de E_1 et $(f_1,\dots,f_q)$ une base de E_2.
Alors E_1 et E_2 sont en somme directe si et seulement si
$(e_1,\dots,e_p,f_1,\dots,f_q)$ (juxtaposition des bases de E_1 et E_2) est libre.
Dans ce cas c'est une base de $E_1 \oplus E_2$ et on a

$$\dim E_1 \oplus E_2 = \dim E_1 + \dim E_2.$$

Le résultat se généralise à plus de deux s.e.v.

Démonstration
Supposons d'abord que $(e_1,\dots,e_p,f_1,\dots,f_q)$ est libre.
Montrons que $\forall (x_1,x_2) \in E_1 \times E_2, x_1+x_2=0_E \Rightarrow x_1=x_2=0_E$.

$x_1 \in E_1$ s'écrit $x_1 = \sum_{i=1}^{p} \alpha_i.e_i$ et $x_2 \in E_2$ s'écrit $x_2 = \sum_{j=1}^{q} \beta_j.f_j$, d'où

$$\begin{aligned} x_1+x_2=0_E &\Rightarrow \sum_{i=1}^{p} \alpha_i.e_i + \sum_{j=1}^{q} \beta_j.f_j = 0_E \\ &\Rightarrow \forall (i,j), \alpha_i=\beta_j=0 \text{ car } (e_1,\dots,e_p,f_1,\dots,f_q) \text{ libre} \\ &\Rightarrow x_1=x_2=0_E \end{aligned}$$

On a donc

$$(e_1,\dots,e_p,f_1,\dots,f_q) \text{ libre } \Rightarrow E_1+E_2 \text{ directe.}$$

Réciproquement, on suppose E_1+E_2 directe.
Soient $(\alpha_i)_{1\leqslant i\leqslant p}$ et $(\beta_j)_{1\leqslant j\leqslant q}$ des familles d'éléments de $\mathbb{K}$. On a

$$\begin{aligned} \sum_{i=1}^{p} \alpha_i.e_i + \sum_{j=1}^{q} \beta_j.f_j = 0_E &\Rightarrow \sum_{i=1}^{p} \alpha_i.e_i = \sum_{j=1}^{q} \beta_j.f_j = 0_E \text{ car la somme est directe} \\ &\Rightarrow \forall (i,j), \alpha=i=\beta_j=0 \text{ car les deux familles sont libres} \end{aligned}$$

Donc : E_1+E_2 directe $\Rightarrow (e_1,\dots,e_p,f_1,\dots,f_q)$ libre. D'où l'équivalence.
D'autre part $(e_1,\dots,e_p,f_1,\dots,f_q)$ est clairement une famille génératrice de E_1+E_2 (toute CL de $(e_1,\dots,e_p,f_1,\dots,f_q)$ est la somme d'un élément de E_1 et d'un élément de E_2, et réciproquement), donc si elle est libre c'est une base de $E_1 \oplus E_2$. □

Théorème - Caractérisation des couples de s.e.v supplémentaires
Soient E un e.v. de dimension finie n et F,G deux s.e.v de E. Alors

$$E = F \oplus G \Leftrightarrow F \cap G = \{0_E\} \text{ et } \dim F + \dim G = n;$$

$$E = F \oplus G \Leftrightarrow F + G = E \text{ et } \dim F + \dim G = n;$$

$E = F \oplus G$
$\Leftrightarrow$ la juxtaposition d'une base de F et d'une base de G est une base de E.

Exercice
Montrer que dans $\mathbb{R}^4$, $F = \text{vect}((1,2,-1,0),(0,2,0,1))$ et $G = \text{vect}((2,0,0,1),(1,0,0,1))$ sont supplémentaires.

Correction
$\dim F + \dim G = 2+2 = 4 = \dim \mathbb{R}^4$.
De plus si $x(1,2,-1,0)+y(0,2,0,1)+z(2,0,0,1)+t(1,0,0,1)=(0,0,0,0)$, on a

$$\left\{\begin{array}{rcrcrcl} x & & +2z & +t & = & 0 \\ 2x & +2y & & & = & 0 \\ -x & & & & = & 0 \\ & & z & +t & = & 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcrcrcl} x & & & & = & 0 \\ y & & & & = & 0 \\ & & z & +t & = & 0 \\ & & 2z & +t & = & 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} x & = & 0 \\ y & = & 0 \\ z & = & 0 \\ t & = & 0 \end{array}\right.$$

On a donc $F \cap G = \{0\}$.

Démonstration
Si $E = F \oplus G$.
Alors $n = \dim E = \dim(F \oplus G) = \dim F + \dim G$. Et comme la somme est directe, $F \cap G = \{0\}$.
Et de même : $n = \dim F + \dim G$ et $F+G \subset E$, avec même dimension donc $F+G=E$.
Réciproquement, supposons que $F \cap G = \{0\}$ et $n = \dim E = \dim F + \dim G$.
Donc la somme est directe : $F+G = F \oplus G$. Puis par $\dim(F \oplus G) = \dim F + \dim G = \dim E$.
Et comme $F \oplus G \subset E$, par égalité des dimensions : $F \oplus G = E$.
Enfin, supposons que $F+G=E$ et $n = \dim E = \dim F + \dim G$.
Notons $\mathscr{B}_1$, une base de F et $\mathscr{B}_2$, une base de G.
$\text{rg}\,(\mathscr{B}_1,\mathscr{B}_2) = \dim(F+G) = \dim E = \dim F + \dim G = \text{rg}\,(\mathscr{B}_1) + \text{rg}\,(\mathscr{B}_2) = \text{Card}(\mathscr{B}_1) + \text{Card}(\mathscr{B}_2)$.
Donc $(\mathscr{B}_1,\mathscr{B}_2)$ est une famille génératrice de E, de dimension $\text{Card}(\mathscr{B}_1) + \text{Card}(\mathscr{B}_2)$.
Il s'agit donc d'une base de E (bon nombre d'éléments) et donc d'une famille libre.
Par conséquent, la somme est direct : $F+G = F \oplus G$ et donc $E = F \oplus G$. □

Remarque - Famille libre : $F \cap G = \{0\}$ & Famille génératrice : $F+G=E$
Notons $\Phi : F \times G \to E$, $(x,y) \mapsto x+y$.

$$F \cap G = \{0\} \Longleftrightarrow \Phi \text{ injective}$$

$$F + G = E \Longleftrightarrow \Phi \text{ surjective}$$

$$F \oplus G = E \Longleftrightarrow \Phi \text{ bijective}$$

Ce qui est affirmé sur les familles libres (en particulier les savoir-faire) est également vrai pour la caractéristique $F \cap G = \{0\}$ (ou « la somme est directe »).

Théorème - Existence de supplémentaires en dimension finie
Soit E un $\mathbb{K}$-e.v. de dimension finie, F un s.e.v de E. Alors F admet au moins un supplémentaire dans E.

Démonstration
Notons $\mathscr{B}$ une base de E (de dimension finie).
Soit F un s.e.v. de E. On note $\mathscr{L}$ une base de F.
$\mathscr{L}$ est libre dans E, on peut la compléter avec une sous-famille de vecteurs de $\mathscr{B}$, en une nouvelle base de E :
$(\mathscr{L},\mathscr{B}')$ base de E Notons $G = \text{vect}(\mathscr{B}')$, alors $F \oplus G = E$. □

Remarque - Processus algorithmique
La démonstration de ce théorème est tout aussi importante que le résultat puisqu'elle fournit un moyen de recherche d'un supplémentaire en dimension finie.
Tout, ici, est équivalent au théorème de la base incomplète.
Exercice
Donner **un** supplémentaire dans $\mathbb{R}^4$ de $F = \text{vect}((1,1,1,1),(2,0,1,1),(-2,4,1,1))$

Correction
On considère la base canonique $\mathscr{B}$ de $\mathbb{R}^4$.
Il y a un piège ici, la famille $\big((1,1,1,1),(2,0,1,1),(-2,4,1,1)\big)$ n'est pas libre :

$$4\cdot(1,1,1,1) - 3\cdot(2,0,1,1) - 1\cdot(-2,4,1,1) = (0,0,0,0)$$

Une base de F est donc $\big((1,1,1,1),(2,0,1,1)\big)$.
$(1,0,0,0) \notin F$, en effet, si $(1,0,0,0) = a\cdot(1,1,1,1) + b\cdot(2,0,1,1) = (a+2b,a,a+b,a+b)$, donc $a=0$ puis $b=0$.
$(0,1,0,0) \in \text{vect}\big((1,1,1,1),(2,0,1,1),(1,0,0,0)\big)$, en effet : $(0,1,0,0) = (1,1,1,1) - (2,0,1,1) + (1,0,0,0)$.
$(0,0,1,0) \notin \text{vect}\big((1,1,1,1),(2,0,1,1),(1,0,0,0)\big)$.
Donc un supplémentaire de F est $G = \text{vect}\big((1,0,0,0),(0,0,1,0)\big)$.

Théorème - Dimension d'une somme de deux s.e.v., relation de Grassman
Soient E un $\mathbb{K}$-e.v. de dimension finie, F, G deux s.e.v de E. Alors

$$\dim(F+G) = \dim F + \dim G - \dim(F \cap G).$$

Démonstration
$F \cap G \subset F$, donc il existe $F' \subset F$ tel que $F = F' \oplus (F \cap G)$;
on a alors $\dim F = \dim F' + \dim(F \cap G)$.
$F \cap G \subset g$, donc il existe $G' \subset G$ tel que $G = G' \oplus (F \cap G)$;
on a alors $\dim G = \dim G' + \dim(F \cap G)$.
Enfin : $F + G = F' \oplus G' \oplus F \cap G$.
En effet $F \subset F' \oplus F \cap G$, donc $F \subset F' \oplus G' \oplus F \cap G$
Et $G \subset G' \oplus F \cap G$, donc $G \subset F' \oplus G' \oplus F \cap G$
Donc $F + G \subset F' \oplus G' \oplus F \cap G$ (stabilité vectorielle)
Réciproquement : $F' \subset F + G$, $G' \subset F + G$, $F \cap G \subset F + G$.
Donc $F' \oplus G' \oplus F \cap G \subset F + G$ (stabilité vectorielle)
Reste à montrer que la somme est directe.
Soient $x \in F'$, $y \in G'$, $z \in F \cap G$ tels que $x + y + z = 0$.
Alors $x = -y - z \in G$ (car $y \in G' \subset G$, $z \in F \cap G \subset G$), donc $x \in F' \cap (F \cap G) = \{0\}$.
Ainsin $x = 0$, de même $y = 0$, puis $z = 0$.
On a ainsi $F + G = F' \oplus G' \oplus F \cap G$.
En passant au dimension :

$$\dim(F+G) = \dim F' + \dim G' + \dim(F \cap G) = \dim F - \dim(F \cap G) + \dim G - \dim(F \cap G) + \dim(F \cap G)$$
$$\dim(F+G) = \dim F + \dim G - \dim(F \cap G)$$

□

Pour aller plus loin - Autre construction
On cherche G tel que $E = F \oplus G$.
En réfléchissant aux dimensions, on trouve que $\dim E = \dim F + \dim G = \dim E \times G$ (produit cartésien).
Il existe une sorte de division euclidienne : la division en classe d'équivalence.
On note $\mathscr{R}$: $u \mathscr{R} v$ ssi $u - v \in F$.
$\mathscr{R}$ est une relation d'équivalence. L'ensemble des classes d'équivalence $G = \frac{E}{\mathscr{R}} = \frac{E}{F}$ est un « espace vectoriel » et alors $\forall\, x \in E$, $\exists!\, (U, y) \in G \times F$ tel que $x - y \in U (= \overline{u})$ (classe de u et donc $x = y + U$ (mais ce n'est pas l'addition de E…)

Théorème - Dimension et somme d'espaces vectoriels
Si $F_1, \dots, F_p$ sont des s.e.v. de dimension finie de E $\mathbb{K}$-espace vectoriel, alors

$$\dim \sum_{i=1}^{p} F_i \leqslant \sum_{i=1}^{p} \dim F_i$$

avec égalité si et seulement si la somme est directe.

Démonstration
D'après la proposition précédente, pour $k \geqslant 2$:

$$\dim\left(\sum_{i=1}^{k} F_i\right) = \dim(F_k) + \dim\left(\sum_{i=1}^{k-1} F_i\right) - \dim\left(F_k \cap \left(\sum_{i=1}^{k-1} F_i\right)\right)$$

On a donc $\dim\left(\sum_{i=1}^{k} F_i\right) \leqslant \dim\left(\sum_{i=1}^{k-1} F_i\right) + \dim(F_k)$.

Et par téléscpage : $\dim\left(\sum_{i=k}^{p} F_k\right) = \sum_{k=1}^{p} \left(\dim\left(\sum_{i=1}^{k} F_i\right) - \dim\left(\sum_{i=1}^{k-1} F_i\right)\right) \leqslant \sum_{k=1}^{p} \dim(F_k)$

On a alors égalité, si et seulement si : $\forall\, k \in \mathbb{N}_p$, $k \geqslant 2$: $\dim\left(F_k \cap \sum_{i=1}^{k-1} F_i\right) = 0$.

Donc pour tout $k \in \mathbb{N}_p$, $k \geqslant 2$, F_k est en somme directe avec $\sum_{i=1}^{k-1} F_i$.

Ce qui est équivalent à : $\forall\, k \in \mathbb{N}_p$, $k \geqslant 2$, $F_k \oplus \left(\sum_{i=1}^{k-1} F_i\right)$.

Et donc finalement, équivalent à $\sum_{k=1}^{p} F_k = \bigoplus_{k=1}^{p} F_k$ □

Définition - Droite et plan vectoriel
Soit E un $\mathbb{K}$-e.v. de dimension quelconque et soit F un s.e.v de E. On dit que
— F est une droite (vectorielle) si $\dim F = 1$;
— F est un plan (vectoriel) si $\dim F = 2$.
— F est un hyperplan (vectoriel) s'il admet un supplémentaire de dimension 1 (soit si $\dim F = n - 1$).

3. Ecriture d'une application linéaire en dimension finie

3.1. Détermination

Détermination par les bases

Théorème - Image d'une base
Soient E un $\mathbb{K}$-e.v de dimension finie n et F un $\mathbb{K}$-e.v. quelconque.
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E et $(f_1, \dots, f_n)$ une famille de n vecteurs de F.
Alors il existe une unique application linéaire u de E dans F telle que

$$\forall\, i \in [\![1, n]\!],\ u(e_i) = f_i.$$

On dit que u est entièrement déterminée par la donnée des images des vecteurs d'une base.

Démonstration
C'est l'application

$$u \ : \ x \left(= \sum_{i=1}^{n} x_i e_i\right) \longrightarrow \sum_{i=1}^{n} x_i f_i$$

□

Remarque - Dimension infinie
Ce résultat se généralise à la dimension infinie.
Si $(e_i)_{i \in I}$ est une base de E et $(f_i)_{i \in I}$ une famille de F (même ensemble d'indices), alors il existe une unique application linéaire $u \in \mathscr{L}(E, F)$ telle que $u(e_i) = f_i$ pour tout $i \in I$.

Corollaire - Egalité d'applications
Deux applications linéaires qui coïncident sur une base sont égales.

Corollaire - Applications linéaires de $\mathbb{K}^n$ dans $\mathbb{K}^p$
Soit $u \in \text{Ł}_{\mathbb{K}}(\mathbb{K}^n, \mathbb{K}^p)$. Alors u est de la forme

$$u : \begin{array}{ccc} \mathbb{K}^n & \to & \mathbb{K}^p \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pn}x_n \end{pmatrix} \end{array} \text{ où } \begin{cases} \forall\, i \in [\![1, p]\!] \\ \forall\, j \in [\![1, n]\!], \end{cases} a_{ij} \in \mathbb{K}.$$

Réciproquement, toute application de cette forme est linéaire du $\mathbb{K}$-e.v. $\mathbb{K}^n$ dans le $\mathbb{K}$-e.v. $\mathbb{K}^p$.

Proposition - Surjection coordonnée
Tout $\mathbb{K}$-e.v de dimension n est isomorphe à $\mathbb{K}^n$.
Si $\mathscr{B}$ une base de E $\mathbb{K}$-e.v. de dimension finie non nulle n. Alors

$$u : \begin{array}{l} E \to \mathbb{K}^n \\ x \mapsto \text{ coordonnées de } x \text{ dans } \mathscr{B} \end{array}$$

est un isomorphisme de E dans $\mathbb{K}^n$.

Démonstration

— Soient $(x,y)\in E^2, (\lambda,\mu)\in\mathbb{K}^2$.

$$x=\sum_{i=1}^{n}x_i.e_i, y=\sum_{i=1}^{n}y_i.e_i \Rightarrow \lambda.x+\mu.y=\sum_{i=1}^{n}(\lambda x_i+\mu y_i).e_i$$

$(\lambda x_i+\mu y_i)_{1\leqslant i\leqslant n}$ sont les coordonnées de $\lambda.x+\mu.y$ dans $\mathscr{B}$: u est linéaire.

— Tout $(x_1,\dots,x_n)\in\mathbb{K}^n$ admet un unique antécédent par u, c'est $\sum_{i=1}^{n}x_i.e_i$: u est bijective.

□

Corollaire - Sans passer par $\mathbb{K}^n$
Soient E un $\mathbb{K}$-e.v de dimension finie et F un $\mathbb{K}$-e.v. a priori quelconque. Alors E et F sont isomorphes si et seulement si F est de dimension finie avec $\dim F=\dim E$.

Démonstration
Soit $u:E\to\mathbb{K}^n$ un isomorphisme ($\dim E=n$).

— Si E et F sont isomorphes, soit $v:E\to F$ un isomorphisme. Alors $v\circ u^{-1}:\mathbb{K}^n\to F$ est un isomorphisme et transforme une base de $\mathbb{K}^n$ en une base de F : F est de dimension finie n.

— Si F de dimension finie n, alors il existe un isomorphisme $w:F\to\mathbb{K}^n$, et alors $w^{-1}\circ u$ est un isomorphisme de E dans F.

□

Théorème - Dimension de $\mathscr{L}(E,F)$
Soient E et F deux $\mathbb{K}$-e.v. de dimension finie. Alors $\mathscr{L}(E,F)$ est un $\mathbb{K}$-e.v. de dimension finie et

$$\dim\mathscr{L}(E,F)=\dim E\times\dim F.$$

Démonstration
Si $\dim E=n, \dim F=p$ et si $(e_1,\dots,e_n)$ est une base de E, $(f_1,\dots,f_p)$ une base de F, alors une base de $\mathscr{L}(E,F)$ est donnée par la famille $(u_{i,j})_{1\leqslant i\leqslant n,1\leqslant j\leqslant p}$ telle que $u_{i,j}$ soit l'unique application linéaire de E dans F telle que

$$\forall k\in[\![1,n]\!],\ u_{i,j}(e_k)=\delta_{i,k}f_j.$$

(ce résultat se comprendra mieux avec les matrices)

□

Remarque - Espace dual
Avec $F=\mathbb{K}$ on trouve $\dim E^*=\dim E$.

Détermination par la restriction à des supplémentaires

E,F désignent toujours deux $\mathbb{K}$-espaces vectoriels.

Théorème -
Soient E_1 et E_2 deux s.e.v. supplémentaires dans E et $u_1\in\mathscr{L}(E_1,F), u_2\in\mathscr{L}(E_2,F)$. Alors il existe une unique application linéaire $u\in\mathscr{L}(E,F)$ telle que

$$u_{|E_1}=u_1 \text{ et } u_{|E_2}=u_2.$$

Plus généralement :

Théorème - Description unique sur une famille de supplémentaires
Si $E_1,\dots,E_p$ sont des s.e.v. de E (de dimension quelconque) vérifiant $E=\bigoplus_{i=1}^{p}E_i$ et si $\forall i$, $u_i\in\mathscr{L}(E_i,F)$, alors il existe une et une seule application $u\in\mathscr{L}(E,F)$ telle que $\forall i$, $u_{|E_i}=u_i$

Démonstration
Elle existe : c'est

$$u:x=\sum_{i=1}^{p}x_i\longrightarrow\sum_{i=1}^{p}u_i(x_i)$$

(où l'on a décomposé x sur la décomposition $E=\bigoplus_{i=1}^{p}E_i$ Elle est unique : en réfléchissant deux secondes on voit bien qu'il ne peut pas y en avoir une autre. □

3.2. Matrice d'une application linéaire

Matrice d'une famille de vecteurs

Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $\mathscr{B}=(e_1,\dots,e_n)$ une base de E.

Définition - Matrice d'une famille de p vecteurs
La matrice dans la base $\mathscr{B}$ d'une famille $(x_1,\dots,x_p)$ de vecteurs de E est la matrice dont la j-ième colonne, pour $j\in[\![1,p]\!]$, est formée des coordonnées de x_j dans la base $\mathscr{B}$. C'est donc la matrice à n lignes et p colonnes :

$$\mathscr{M}_{\mathscr{B}}(x_1,\dots,x_p)=\begin{pmatrix}a_{11}&\cdots&\cdots&a_{1p}\\a_{21}&\cdots&\cdots&a_{2p}\\\vdots&\vdots&\vdots&\vdots\\a_{n1}&\cdots&\cdots&a_{np}\end{pmatrix}=(a_{i,j})_{1\leqslant i\leqslant n;1\leqslant j\leqslant p}$$

telle que, pour tout j, $x_j=\sum_{i=1}^{n}a_{i,j}e_i$.

Exemple - Dans $\mathbb{R}^2$
On considère $\mathscr{B}=\big((1,1),(1,-1)\big)$ une base de $\mathbb{R}^2$.
Puis $x_1=(1,2)$, $x_2=(0,0)$ et $x_3=(-1,1)$.
Alors $\mathscr{M}_{\mathscr{B}}(x_1,x_2,x_3)=\begin{pmatrix}\frac{3}{2}&0&0\\-\frac{1}{2}&0&-1\end{pmatrix}$

Heuristique - Cas particulier $p=1$: la « matrice du vecteur x dans $\mathscr{B}$ »
Dans le cas particulier d'une famille à un vecteur x, la matrice $\mathscr{M}_{\mathscr{B}}(x)$ est une matrice colonne, c'est la matrice colonne formée des coordonnées de x dans la base $\mathscr{B}$. On parle souvent de la « matrice du vecteur x dans la base $\mathscr{B}$ ».
Soit $\mathscr{B}$ la base canonique de $\mathbb{K}^n$. L'application

$$\begin{array}{ccc}\mathbb{K}^n&\to&\mathscr{M}_{n,1}(\mathbb{K})\\x&\mapsto&\mathscr{M}_{\mathscr{B}}(x)\end{array}$$

est alors un isomorphisme d'espaces vectoriels. On identifie donc usuellement matrices colonnes (à n lignes) et vecteurs de $\mathbb{K}^n$

Matrice d'une application linéaire

Définition - Matrice d'un morphisme u
E et F sont deux espaces vectoriels sur $\mathbb{K}$, de dimension finie (respectivement n et p).
$\mathscr{B}=(e_1,\cdots,e_n)$ et $\mathscr{C}=(f_1,\cdots,f_p)$ désignent respectivement des bases de E et de F.
Soit $u\in\mathscr{L}(E,F)$, alors $\forall j\in[\![1,n]\!], u(e_j)\in F$ et donc on peut écrire $u(e_j)=$

$\sum_{i=1}^{p} a_{ij} f_i$.
On appelle **matrice de** u dans les bases $\mathscr{B}$ et $\mathscr{C}$, la matrice :

$$\mathscr{M}_{\mathscr{B},\mathscr{C}}(u) = \mathscr{M}(u,\mathscr{B},\mathscr{C}) = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ a_{21} & \cdots & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{p1} & \cdots & \cdots & a_{pn} \end{pmatrix} = (a_{ij})_{1\leqslant i\leqslant p; 1\leqslant j\leqslant n}$$

a_{ij} désigne la i-ième coordonnée de $u(e_j)$ dans $\mathscr{C}$.
C'est la matrice dans $\mathscr{C}$ de la famille $(u(e_1),\dots,u(e_n))$.

Attention - Taille de la matrice
Il s'agit d'une matrice à n colonnes (nombre de vecteurs d'une base de l'ensemble de départ) et p lignes (dimension de l'ensemble d'arrivée), soit p lignes et n colonnes.

Exemple - Matrice de $P \mapsto P'$
Soit $E = \mathbb{R}_3[X]$, $F = \mathbb{R}_2[X]$ et $u(P) = P'$
Les bases canoniques respectives $\mathscr{B}$ et $\mathscr{C}$ de E et F sont $\mathscr{B} = (1, X, X^2, X^3)$ et $\mathscr{C} = (1, X, X^2)$.
On décompose $u(X^j)$ pour j variant de 1 à 4 sur $\mathscr{C}$: ($p = 3, n = 4$) 3 lignes et 4 colonnes :

$$\begin{aligned} u(1) &= 0 &&= 0.1 + 0.X + 0.X^2, \\ u(X) &= 1 &&= 1.1 + 0.X + 0.X^2, \\ u(X^2) &= 2X &&= 0.1 + 2.X + 0.X^2, \\ u(X^3) &= 3X^2 &&= 0.1 + 0.X + 3.X^2. \end{aligned}$$

La matrice de u dans les bases canoniques est donc

$$\mathscr{M}_{\mathscr{B},\mathscr{C}}(u) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Théorème - Réciproquement de la matrice au morphisme
Soient E et F deux $\mathbb{K}$-e.v., $\dim E = n$, $\dim F = p$. On suppose fixées $\mathscr{B}$ une base de E et $\mathscr{C}$ une base de F. Alors, pour toute matrice $A \in \mathscr{M}_{p,n}(\mathbb{K})$, il existe une unique application linéaire $u \in \mathscr{L}(E,F)$ telle que $\mathscr{M}_{\mathscr{B},\mathscr{C}}(u) = A$.

Démonstration
Par construction, cette unique application ne peut être que :

$$u : e_j \mapsto \sum_{i=1}^{p} \text{Coef}_{i,j}(A) f_i$$

□

Proposition - Calcul matriciel de l'opération $u(x)$
Soient E et F deux $\mathbb{K}$-e.v., $\dim E = n$, $\dim F = p$. On suppose fixées $\mathscr{B}$ une base de E et $\mathscr{C}$ une base de F.
Soient $u \in \mathscr{L}(E,F)$, $A = \mathscr{M}_{\mathscr{B},\mathscr{C}}(u)$, X la matrice colonne des coordonnées d'un vecteur x de E dans la base $\mathscr{B}$, alors la matrice colonne Y des coordonnées de $y = u(x)$ dans la base $\mathscr{C}$ est donnée par la relation

$$Y = AX.$$

Démonstration
$y = \sum_{i=1}^{p} \text{Coef}_i(Y) = u(x) = u\left(\sum_{j=1}^{n} x_j e_j\right) = \sum_{j=1}^{n} x_j u\left(e_j\right)$
$= \sum_{j=1}^{n} \text{Coef}_j(X)\left(\sum_{i=1}^{p} \text{Coef}_{i,j}(A)\right) = \sum_{i=1}^{p}\left(\sum_{j=1}^{n} \text{Coef}_j(X)\text{Coef}_{i,j}(A)\right)$.
Donc pour tout $i \in \mathbb{N}_p$, $\text{Coef}_i(Y) = \sum_{j=1}^{n}\left(\text{Coef}_{i,j}(A)\text{Coef}_j(X)\right) = \text{Coef}_i(AX)$, donc $Y = AX$. □

Corollaire - Nouveau critère d'égalité matriciel
Soient $A, B \in \mathscr{M}_{p,n}(\mathbb{K})$. Alors :

$$\left(\forall X \in \mathscr{M}_{n,1}(\mathbb{K}),\ AX = BX\right) \Rightarrow A = B$$

Démonstration
Pour tout $x \in E$, $u(x) = v(x)$, donc $u = v$ donc $A = B$ □

Définition - Matrice d'un endomorphisme
Soient E un $\mathbb{K}$-espace vectoriel de dimension n, $\mathscr{B}$ une base de E, $u \in \mathscr{L}(E)$. Alors, pour $u \in \mathscr{L}(E)$, $\mathscr{M}_{\mathscr{B},\mathscr{B}}(u) \in \mathscr{M}_n(\mathbb{K})$ s'appelle la matrice de u dans la base $\mathscr{B}$ et se note simplement $\mathscr{M}_{\mathscr{B}}(u)$ (ou $\mathscr{M}(u,\mathscr{B})$).

Exemple - Dans $\mathbb{R}^2$
On prend $E = F = \mathbb{R}^2$ comme espaces vectoriels (on les interprète comme l'espace vectoriel des vecteurs du plan), on choisit la base $\mathscr{B} = ((1,0),(0,1)) = \mathscr{C}$ ce qui correspond aux vecteurs $\vec{i}$ et $\vec{j}$ sur les axes. On caractérise géométriquement le morphisme

$$u : E \to F \text{ tel que } \mathscr{M}_{\mathscr{B}}(u) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

comme la symétrie orthogonale d'axe Ox.
Exercice
Quelle est la matrice dans la base $\mathscr{B} = \mathscr{C}$ de la symétrie orthogonale par rapport à la première bissectrice ?

Correction
$u : (x,y) \mapsto (y,x)$, donc $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$\mathscr{L}(F,G)$ & $\mathscr{M}_{n,p}(\mathbb{K})$ isomorphes

Théorème - L'application linéaire $u \mapsto \mathscr{M}_{\mathscr{B},\mathscr{C}}(u)$
Soient E, F deux $\mathbb{K}$-espaces vectoriels ($\dim E = n, \dim F = p$) de bases respectives $\mathscr{B}$, $\mathscr{C}$, $u, v \in \mathscr{L}(E,F)$, $\alpha, \beta \in \mathbb{K}$ alors

$$\mathscr{M}_{\mathscr{B},\mathscr{C}}(\alpha u + \beta v) = \alpha \mathscr{M}_{\mathscr{B},\mathscr{C}}(u) + \beta \mathscr{M}_{\mathscr{B},\mathscr{C}}(v).$$

L'application

$$\begin{aligned} \mathscr{L}(E,F) &\to \mathscr{M}_{p,n}(\mathbb{K}) \\ u &\mapsto \mathscr{M}_{\mathscr{B},\mathscr{C}}(u) \end{aligned}$$

est donc un isomorphisme d'espaces vectoriels.

Théorème - Produit matriciel et composition
Soient trois espaces vectoriels E, F, G munis des bases respectives $\mathscr{B}, \mathscr{C}, \mathscr{D}$, et deux applications linéaires $u \in \mathscr{L}(E,F)$, $v \in \mathscr{L}(F,G)$. Alors la matrice de $v \circ u \in \mathscr{L}(E,G)$ est donnée par

$$\mathscr{M}_{\mathscr{B},\mathscr{D}}(v \circ u) = \mathscr{M}_{\mathscr{C},\mathscr{D}}(v) \times \mathscr{M}_{\mathscr{B},\mathscr{C}}(u)$$

Démonstration
Le coefficient de $\alpha u + \beta v(e_j)$ selon f_j est égal
au coefficient de $(\alpha u)(e_j) + (\beta v)(e_j)$ selon f_j
au coefficient de $\alpha u(e_j) + \beta v(e_j)$ selon f_j
au nombre de $\alpha \text{Coef}_{i,j}(\mathscr{M}(u)) + \beta \text{Coef}_{i,j}(\mathscr{M}(v))$ selon f_j.
Donc $\mathscr{M}(\alpha u + \beta v) = \alpha M(u) + \beta M(v)$.
Autre méthode : si $y = u(e_j)$, alors se traduit matriciellement par $Y = \mathscr{M}(u) \times E_j$.
Et donc $z = v \circ u(e_j)$ se traduit matriciellement par $\mathscr{M}(u \circ v)E_j = Z = \mathscr{M}(v) \times (\mathscr{M}(u) \times E_j) = [\mathscr{M}(v) \times \mathscr{M}(u)]E_j$.
Ce résultat est vrai pour tout E_j, donc $\mathscr{M}(v \circ u) = \mathscr{M}(v) \times \mathscr{M}(u)$ □

Remarque - Nouvelle interprétation du produit matriciel
Cela justifie, d'une nouvelle façon, l'utilité de la définition de la multiplication entre les matrices : ceci permet de calculer avec un nombre fini d'opérations une composée de deux applications linéaires.

Corollaire -
Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $\mathscr{B}$ une base de E. L'application $u \mapsto \mathscr{M}_{\mathscr{B}}(u)$ est un isomorphisme d'algèbres de $\mathscr{L}(E)$ sur $\mathscr{M}_n(\mathbb{K})$ (isomorphisme d'espaces vectoriels et morphisme d'anneaux)

Proposition - Bijection de u et inversibilité de $\mathscr{M}$
Soient E et F deux espaces vectoriels de même dimension n (en particulier on peut avoir $E = F$) de bases respectives $\mathscr{B}$ et $\mathscr{C}$,
Soit u une application linéaire de E dans F et $A = \mathscr{M}_{\mathscr{B},\mathscr{C}}(u)$.
Alors u est bijective (donc est un isomorphisme)
si et seulement si A est inversible.
Et alors

$$A^{-1} = \mathscr{M}_{\mathscr{C},\mathscr{B}}(u^{-1})$$

Savoir faire - Exploitation
Ce résultat peut être utilisé de deux façons :
— Pour trouver l'isomorphisme réciproque de u, on calcule l'inverse de la matrice de u (voir plus loin pour les méthodes).
— Pour trouver l'inverse d'une matrice, on peut parfois la reconnaître comme la matrice d'un isomorphisme dont on sait facilement exprimer l'endomorphisme réciproque.

Démonstration
u est bijective ssi $\exists\, v \in \mathscr{L}(F,E)$ tel que $u \circ v = v \circ u = \text{id}$.
u est bijective ssi $\exists\, v \in \mathscr{L}(F,E)$ tel que $\mathscr{M}(v) \times A = A \times M_v = I_n$ u est bijective ssi A est inversible
□

Exercice
Soit $A \in \mathscr{M}_{n+1}(\mathbb{R})$ définie par $a_{ij} = \binom{j-1}{i-1}$ (avec la convention $\binom{j}{i} = 0$ si $j < i$) pour $i, j \in [\![1, n+1]\!]^2$. Justifier l'inversibilté de A et déterminer A^{-1}.

Correction
A est la matrice de $u : P \mapsto P(X+1)$ dans la base canonique de $\mathbb{R}_n[X]$.
En effet, $u(X^p) = (X+1)^p = \sum_{k=0}^{p} \binom{p}{k} X^k$.

L'application réciproque de u est $v : P \mapsto (X-1)$.
Or pour tout p, $v(X^p) = (X-1)^p = \sum_{k=0}^{p} (-1)^k \binom{p}{k} X^k$.
Donc $A^{-1} = \mathscr{M}_{\mathscr{B}}(v) = \left((-1)^{i-1}\binom{j-1}{i-1}\right)$.

Réciproquement, application canoniquement associée à une matrice

Heuristique - Identification
L'application de $\mathbb{K}^n$ dans $\mathscr{M}_{n,1}(\mathbb{K})$ qui à $x = (x_1, \dots, x_n)$ associe la matrice colonne $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ est un isomorphisme naturel ("canonique") entre $\mathbb{K}^n$ et $\mathscr{M}_{n,1}(\mathbb{K})$. Il permet d'identifier un n-uplet x avec la matrice colonne X.
D'autre part, on sait que si $u \in \mathscr{L}_{\mathbb{K}}(\mathbb{K}^n, \mathbb{K}^p)$, alors u est de la forme

$$u : \begin{array}{ccc} \mathbb{K}^n & \to & \mathbb{K}^p \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pn}x_n \end{pmatrix} \end{array} \quad \text{où } \forall i \in [\![1,p]\!], \forall j \in [\![1,n]\!], a_{ij} \in \mathbb{K}.$$

Définition - Application canoniquement associée à A
Soit $A \in \mathscr{M}_{p,n}(\mathbb{K})$, alors il existe une unique application linéaire $u \in \mathscr{L}(\mathbb{K}^n, \mathbb{K}^p)$ telle que la matrice de u dans les bases canoniques respectives de $\mathbb{K}^n$ et $\mathbb{K}^p$ soit A. On dit alors que u est canoniquement associée à A.
u peut alors être identifiée à l'application

$$\begin{array}{ccc} \mathscr{M}_{n,1} & \to & \mathscr{M}_{p,1}(\mathbb{K}) \\ X & \mapsto & AX \end{array}$$

Remarque - Convention d'usage
On écrit aussi $y = Ax$ avec $x \in \mathbb{K}^n, y \in \mathbb{K}^p$.

Proposition - Noyau, image
Soit $A \in \mathscr{M}_{p,n}(\mathbb{K})$ et u l'application linéaire canoniquement associée.
On rappelle que :

$$\text{Ker } A = \{X \in \mathbb{K}^n \equiv \mathscr{M}_{n,1}(\mathbb{K}) \mid AX = 0_{\mathbb{K}^p}\}$$

$$\text{Im } A = \{Y \in \mathbb{K}^p \equiv \mathscr{M}_{p,1}(\mathbb{K}) \mid \exists X \in \mathbb{K}^n \equiv \mathscr{M}_{n,1}(\mathbb{K}), Y = AX\}.$$

Par les identifications précédentes $\text{Ker } A = \text{Ker } u$ et $\text{Im } A = \text{Im } u$.

Réinterprétation du produit par blocs

Proposition - Blocs nuls et stabilité
Soient F et G deux sous-espaces supplémentaires de E $\mathbb{K}$-e.v. ($\dim E = n, \dim F = p$) et $u \in \mathscr{L}(E)$ telle que la matrice de u s'écrive, dans une base adaptée à la décomposition $E = F \oplus G$, par blocs $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ (avec $A \in \mathscr{M}_p(\mathbb{K})$).
Alors :
— F est stable par u si et seulement si $C = O_{n-p,p}$; dans ce cas $A = \mathscr{M}(u_{|F})$
— G est stable par u si et seulement si $B = O_{p,n-p}$; dans ce cas $D = \mathscr{M}(u_{|G})$

Démonstration
On ne démontre que le premier cas.
Notons $(f_1,\dots f_p)$ une base de F et $(g_1,\dots g_{n-p})$ une base de G. F est stable par u si et seulement si pour tout $j\leqslant p$, $u(f_j)$ ne s'écrit qu'en fonction de $(f_1,\dots f_p)$.
$\forall\ j\leqslant p, \forall\ i>p+1$, la i coordonnée de $u(f_j)$ est nul.
$\forall\ j\leqslant p, \forall\ i>p+1, \text{Coef}_{i,j}(M)=0$.
$C=O_{n-p,p}$.
□

Exercice
Montrer que les projecteurs et les symétries ont, dans des bases bien choisies, des matrices par blocs très simples.

Correction
Si $E=F\oplus G$, que $\mathscr{B}$ est une base adaptée à cette décomposition.
Si p est la projection sur F parallèlement à G et s, la symétrie par rapport à F et de direction G, alors

$$\mathscr{M}_{\mathscr{B}}(p)=\begin{pmatrix} I_p & O \\ O & O_{n-p}\end{pmatrix} \qquad \mathscr{M}_{\mathscr{B}}(p)=\begin{pmatrix} I_p & O \\ O & -I_{n-p}\end{pmatrix}$$

on aura noté $p=\dim F$

Remarque - Généralisation
La notation et le calcul par blocs peuvent se généraliser à plus de deux blocs.
La condition : la taille des blocs doit être compatible au produit envisagé.
On peut aussi voir le produit $AX=\sum_{i=1}^{p} x_i C_i$ comme un produit par blocs…

3.3. Changements de bases

Le but de ce paragraphe est de trouver le lien entre les différentes matrices d'une même application linéaire lorsque l'on change de bases dans les ensembles E et F.

Matrice de passage

Définition - Matrice de passage (changement de base vectoriel)
Soient E un $\mathbb{K}$-e.v. de dimension n,
$\mathscr{B}=(e_1,\cdots,e_n)$ (ancienne) et $\mathscr{B}'=(e'_1,\cdots,e'_n)$ (nouvelle), deux bases de E.
On appelle matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$, notée $P_{\mathscr{B}}^{\mathscr{B}'}$ (ou $P_{\mathscr{B},\mathscr{B}'}$), la matrice de la famille $\mathscr{B}'$ dans la base $\mathscr{B}$:

$$P_{\mathscr{B}}^{\mathscr{B}'}=\mathscr{M}_{\mathscr{B}}(e'_1,\cdots,e'_n)=\mathscr{M}_{\mathscr{B}',\mathscr{B}}(\text{id}_{E,E})$$

Attention - Ecrire la bonne matrice
On obtient donc la matrice de passage P de $\mathscr{B}$ à $\mathscr{B}'$ en écrivant en colonnes les coordonnées dans la base $\mathscr{B}$ des vecteurs e'_i (de $\mathscr{B}'$).
(C'est celle que l'on sait écrire sans problème car les vecteur e'_i sont toujours donnés par leurs coordonnées dans $\mathscr{B}$)

Théorème - Inverse d'une matrice de passage
On a $P_{\mathscr{B}}^{\mathscr{B}'}=\mathscr{M}_{\mathscr{B}',\mathscr{B}}(Id_E)$.
Une matrice de passage est donc inversible (car Id_E est bijectif) et $(P_{\mathscr{B}}^{\mathscr{B}'})^{-1}=P_{\mathscr{B}'}^{\mathscr{B}}$.

Pas de démonstration supplémentaire.

Théorème - Calcul matriciel du changement de base
Soient E un $\mathbb{K}$-espace vectoriel, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et P la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$. Si X est la matrice colonne des coordonnées dans $\mathscr{B}$ de $x\in E$ et X' la matrice colonne des coordonnées dans $\mathscr{B}'$ de x, alors $X=PX'$, c'est-à-dire

$$\mathscr{M}_{\mathscr{B}}(x)=P_{\mathscr{B}}^{\mathscr{B}'}\mathscr{M}_{\mathscr{B}'}(x)$$

Savoir faire - Petite aide mnémnotechnique
Se souvenir que la formule donne facilement les coordonnées dans l'ancienne base en fonction des coordonnées dans la nouvelle base, ce qui est rarement ce dont on a besoin! Pour avoir les coordonnées dans la nouvelle base en fonction des anciennes, il faut calculer P^{-1}.

Démonstration
$\mathscr{M}_{\mathscr{B}',\mathscr{B}}(Id_E)\times\mathscr{M}_{\mathscr{B}'}(x)=\mathscr{M}_{\mathscr{B}}(x)$ □

Matrices équivalentes

Théorème - Changement de base d'une application de $\mathscr{L}(E,F)$
Soient E,F deux $\mathbb{K}$-e.v., de bases $\mathscr{B}$ et $\mathscr{B}'$ pour E, $\mathscr{C}$ et $\mathscr{C}'$ pour F. On pose $P=P_{\mathscr{B}}^{\mathscr{B}'}$ et $Q=P_{\mathscr{C}}^{\mathscr{C}'}$.
Alors, si $u\in\mathscr{L}(E,F)$, $A=\mathscr{M}_{\mathscr{B},\mathscr{C}}(u)$, $A'=\mathscr{M}_{\mathscr{B}',\mathscr{C}'}(u)$ on a

$$A'=Q^{-1}AP$$

Démonstration à bien savoir faire, pour retrouver rapidement le résultat. On rappelle que si « tout va bien » (dimension) : $\mathscr{M}_{\mathscr{B},\mathscr{D}}(u\circ v)=\mathscr{M}_{\mathscr{C},\mathscr{D}}(u)\times\mathscr{M}_{\mathscr{B},\mathscr{C}}(v)$ (flèche à l'envers pour les bases)

Démonstration
$A'=\mathscr{M}_{\mathscr{B}',\mathscr{C}'}(u\circ\text{id})=\mathscr{M}_{\mathscr{B}',\mathscr{C}'}(u).\mathscr{M}_{\mathscr{B}',\mathscr{B}}(\text{id})=\mathscr{M}_{\mathscr{B}',\mathscr{C}'}(\text{id}\circ u).\mathscr{M}_{\mathscr{B}',\mathscr{B}}(\text{id})=\mathscr{M}_{\mathscr{C},\mathscr{C}'}(\text{id}).\mathscr{M}_{\mathscr{B},\mathscr{C}}(u).\mathscr{M}_{\mathscr{B}',\mathscr{B}}(\text{id})$
□

Remarque - Rappel
On rappelle que deux matrices A et B sont équivalentes, s'il existe $P,Q\in\mathscr{GL}_n(\mathbb{K})$ tel que $A=P\times B\times Q^{-1}$.
On a également vu que A et B sont équivalentes si et seulement si $\text{rg}(A)=\text{rg}(B)$. Et qu'il existe une famille de représentants des classes d'équivalence : les J_r

Proposition - Nouvelle interprétation de l'équivalence matricielle
$A,B\in\mathscr{M}_{n,p}(\mathbb{K})$ sont équivalentes si et seulement si
elles représentent la même applications linéaire dans des bases différentes (a priori au départ et à l'arrivée)

Démonstration
Cela découle du théorème… □

Matrices semblables

Dans le cas particulier où $E=F$ on peut prendre $\mathscr{B}=\mathscr{C}$ et $\mathscr{B}'=\mathscr{C}'$ d'où $Q=P$ et on a le théorème suivant :

Théorème -
Soient E un $\mathbb{K}$-espace vectoriel, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et P la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$. Alors, si $u\in\mathscr{L}(E)$, $A=Mat_{\mathscr{B}}(u)$, $A'=Mat_{\mathscr{B}'}(u)$ on a

$$A'=P^{-1}AP$$

Exercice

Soit $E=\mathbb{R}^2$. On considère les deux vecteurs $f_1=(1,2)$ et $f_2=(1,3)$.

1. Montrer que $\mathscr{B}'=(f_1,f_2)$ est une base de E.
2. Soit $\mathscr{B}$ la base canonique de E. Ecrire la matrice de passage $P_{\mathscr{B}}^{\mathscr{B}'}$.
3. Soit $x=(4,1)\in E$. Déterminer matriciellement les coordonnées de x dans la base $\mathscr{B}'$.
4. Soit u l'endomorphisme de E défini par $u((x,y))=(2x+y,x-y)$. Ecrire les matrices de u dans les bases $\mathscr{B}$ et $\mathscr{B}'$.

Correction

1. La matrice $\begin{pmatrix}1&1\\2&3\end{pmatrix}$ est inversible (de déterminant 1).
2. $P_{\mathscr{B}}^{\mathscr{B}'}=\begin{pmatrix}1&1\\2&3\end{pmatrix}$
3. Les coordonnées de x dans la base $\mathscr{B}'$ sont données par $P_{\mathscr{B}'}^{\mathscr{B}}X=\left(P_{\mathscr{B}}^{\mathscr{B}'}\right)^{-1}X=\begin{pmatrix}3&-1\\-2&1\end{pmatrix}\begin{pmatrix}4\\1\end{pmatrix}=\begin{pmatrix}11\\-7\end{pmatrix}$ (on peut vérifier)
4. $\mathscr{M}_{\mathscr{B}}(u)=\begin{pmatrix}2&1\\1&-1\end{pmatrix}$ et $\mathscr{M}_{\mathscr{B}'}(u)=P_{\mathscr{B}'}^{\mathscr{B}}.\mathscr{M}_{\mathscr{B}}(u)P_{\mathscr{B}}^{\mathscr{B}'}=\begin{pmatrix}3&-1\\-2&1\end{pmatrix}\begin{pmatrix}2&1\\1&-1\end{pmatrix}\begin{pmatrix}1&1\\2&3\end{pmatrix}=\begin{pmatrix}13&17\\-9&-12\end{pmatrix}$

Définition - Matrices semblables
$A,B\in\mathscr{M}_n(\mathbb{K})$ sont dites semblables s'il existe $P\in GL_n(\mathbb{K})$ telle que $B=P^{-1}AP$.

Remarque - Relation d'équivalence
Il s'agit d'une relation d'équivalence. C'est une relation particulière qui dérive de la relation « être équivalente ».
Etant plus précise, les classes d'équivalence pour la relation de similitude sont plus nombreuse. Le cours de diagonalisation de seconde année consiste à chercher des représentants relativement simples (diagonale, au mieux) de ces classes de similitude.
On a alors, par récurrence,

Proposition - Calcul de puissance
Si A et B son semblables, précisément : $B=P^{-1}AP$.
Alors pour tout $k\in\mathbb{N}$, $B^k=P^{-1}A^kP$ (car $PP^{-1}=I_n$).

Théorème - Ré-interprétation de la similitude
Soient E un $\mathbb{K}$-espace vectoriel de dimension n, $A,B\in\mathscr{M}_n(\mathbb{K})$.
Alors les matrices A et B sont semblables si et seulement si
il existe $\mathscr{B}$ et $\mathscr{B}'$, bases de E, $u\in\mathscr{L}(E)$ tq $A=\mathscr{M}_{\mathscr{B}}(u)$ et $B=\mathscr{M}_{\mathscr{B}'}(u)$.
Autrement dit, A et B sont semblables si elles représentent le même endomorphisme dans deux bases différentes.

Truc & Astuce pour le calcul - Etant donnée A et B, trouver $\mathscr{B}$, $\mathscr{B}'$ et u
Il n'y a pas unicité du triplet $(\mathscr{B},\mathscr{B}',u)$. Il faut donc choisir un représentant.
En revanche, on connait A et B puis donc P.
Classiquement, on considère (dans l'ordre) :

1. $E=\mathscr{M}_{n,1}(\mathbb{K})$ (équivalent à $\mathbb{K}^n$)
2. $\mathscr{B}=(X_1,\dots X_n)$, la base canonique de E
3. $u:X\mapsto A\times X$. Par construction $A=\mathscr{M}_{\mathscr{B}}(u)$.

En fait comme $\mathscr{B}$ est la base canonique, $AX_j=C_j(A)=\sum_{i=1}^{n}[A]_{i,j}X_i$

4. $\mathscr{B}'=P(\mathscr{B})=(Y_1,Y_2,\dots Y_n)=(PX_1,PX_2,\dots PX_n)$, c'est bien une base car P est inversible.
$u(Y_j)=u(PX_j)=APX_j=PBX_j=PC_j(B)$, car $\mathscr{B}$ est la base canonique.
Donc $u(Y_j)=P\sum_{i=1}^{n}[B]_{i,j}X_i=\sum_{i=1}^{n}[B]_{i,j}PX_i=\sum_{i=1}^{n}[B]_{i,j}Y_i$ Ainsi $\mathscr{M}_{\mathscr{B}'}(u)=B$

Exercice

Soit $A=\begin{pmatrix}1&2&3\\3&1&2\\2&3&1\end{pmatrix}$. Montrer que A est semblable à ${}^tA$.

Correction

On considère $P=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}=P^{-1}$. On a $A^T=PAP^{-1}$.

Proposition - Matrices semblables et trace
Deux matrices semblables ont même trace.

Démonstration
Si A et B sont semblables, alors

$$\mathrm{Tr}(B)=\mathrm{Tr}(P^{-1}AP)=\mathrm{Tr}(APP^{-1})=\mathrm{Tr}(A)$$

(On peut permuter circulairement le produit matriciel au coeur de la trace. □

Définition - Trace d'un endomorphisme
Soit E est un $\mathbb{K}$-espace vectoriel de dimension finie. Soit $\mathscr{B}$ une base de E.
Soit $u\in\mathscr{L}(E)$. On appelle trace de u le scalaire

$$\mathrm{Tr}\,u=\mathrm{Tr}\,(u)=\mathrm{Tr}\,M_{\mathscr{B}}(u).$$

Remarque - Une démonstration ?
Ceci a bien un sens d'après la proposition précédente qui assure que les matrices de u dans des bases différentes ont toujours la même trace (invariante selon la base considérée).

Corollaire - Propriétés simples de Tr
L'application trace sur $\mathscr{L}(E)$ est linéaire et

$$\forall u,v\in\mathscr{L}(E),\ \mathrm{Tr}\,(u\circ v)=\mathrm{Tr}\,(v\circ u).$$

Proposition - Rang=trace d'un projecteur
Soit $p\in L(E)$ un projecteur. Alors $\mathrm{Tr}\,(p)=\mathrm{rg}\,(p)$.

Démonstration
On a vu qu'en prenant une base adaptée à $E=\mathrm{Im}\,p\oplus\mathrm{Ker}\,p$, on a

$$P=\mathscr{M}(u)=\begin{pmatrix}I_r&0\\0&O_{n-r}\end{pmatrix}$$

On a alors $\mathrm{Tr}\,(u)=\mathrm{Tr}(P)=r=\dim(\mathrm{Im}\,p)=\mathrm{rg}\,(p)$ □

4. Théorème (formule) du rang et conséquences

4.1. Théorème du rang

Rang(s)

Définition - Rang d'une application linéaire
Soient E, F deux $\mathbb{K}$-espaces vectoriels (de dimensions quelconques) et $u \in \mathscr{L}(E,F)$. On dit que u est de rang fini si $\operatorname{Im} u$ est de dimension finie et on appelle alors rang de u la dimension de $\operatorname{Im} u$:

$$\operatorname{rg} u = \dim \operatorname{Im} u$$

Rappels :

Définition - Rang d'une famille de vecteurs
Soit $(x_1,\dots,x_p)$ une famille finie de vecteurs d'un $\mathbb{K}$-espace vectoriel. On appelle rang de la famille $(x_1,\dots,x_p)$ la dimension du sous-espace vectoriel $\operatorname{vect}(x_1,\dots,x_p)$:

$$\operatorname{rg}(x_1,\dots,x_p) = \dim \operatorname{vect}(x_1,\dots,x_p)$$

Définition - Rang d'une matrice
Soit $A \in \mathscr{M}_{p,n}(\mathbb{K})$ On appelle rang de A (noté $\operatorname{rg} A$) la dimension de $\operatorname{Im} A$.

Remarque - Nouvelle définition
Cette nouvelle définition est conforme à celle vu au premier semestre - en complément.
Le rang de la matrice étaient obtenu comme nombre de pivot après échelonnage de la matrice.

Théorème du rang

Proposition - Isomorphisme canonique (de projection)
Soient E et F deux $\mathbb{K}$-e.v. et $u \in \mathscr{L}(E,F)$. Si S est un supplémentaire de $\operatorname{Ker} u$ dans E alors l'application

$$\begin{aligned} \tilde{u} : \quad & S \to \operatorname{Im} u \\ & x \mapsto u(x) \end{aligned}$$

est un isomorphisme de S sur $\operatorname{Im} u$

Démonstration
C'est en effet une application linéaire.
Et si $x \in \operatorname{Ker} \tilde{u}$,
alors $0 = \tilde{u}(x) = u(x)$, donc $x \in \operatorname{Ker} u$.
Mais par ailleurs, $x \in S$, donc $x \in \operatorname{Ker} u \cap S = \{0\}$.
Donc $\tilde{u}$ est injective.
Par ailleurs, $\tilde{u}$ est également surjective sur $\operatorname{Im} u$.
En effet, si $y \in \operatorname{Im} u$, il existe $x \in E$ tel que $y = u(x)$.
Puis $x = x_1 + x_2$, avec $x_1 \in S$ et $x_2 \in \operatorname{Ker} u$.
Donc $y = u(x) = u(x_1) + u(x_2) = \tilde{u}(x_1)$ et $y \in \operatorname{Im} \tilde{u}$. □

Théorème - Théorème du rang
Soient E un $\mathbb{K}$-e.v. de dimension finie, F un $\mathbb{K}$-e.v. (de dimension quelconque) et $u \in \mathscr{L}(E,F)$. Alors

$$\dim E = \dim \operatorname{Ker} u + \dim \operatorname{Im} u = \dim \operatorname{Ker} u + \operatorname{rg} u$$

Démonstration
Comme S est isomorphe à $\operatorname{Im} u$, on a donc $\dim S = \operatorname{rg} u$.
Et comme $E = S \oplus \operatorname{Ker} u$ est de dimension finie : $\dim E = \dim \operatorname{Ker} u + \dim S = \dim \operatorname{Ker} u + \operatorname{rg} u$ □

4.2. Application du théorème du rang (Critère de bijection)

Proposition - Critère de surjection/injection
Soit $u \in \mathscr{L}(E,F)$.
— Si E est de dimension finie, alors u est de rang fini et $\operatorname{rg} u \leqslant \dim E$ avec égalité si et seulement u est injective.
— Si F est de dimension finie, alors u est de rang fini et $\operatorname{rg} u \leqslant \dim F$ avec égalité si et seulement u est surjective.

Démonstration
Théorème du rang :$\operatorname{rg} u = \dim E - \dim \operatorname{Ker} u$.
Donc $\operatorname{rg} u \leqslant \dim E$ avec égalité si et seulement $\operatorname{Ker} u = \{0\}$ si et seulement u est injective.
$\operatorname{Im} u \subset F$, donc
$\operatorname{rg} u \leqslant \dim F$ avec égalité si et seulement $\operatorname{Im} u = F$ si et seulement si u est surjective. □

Si E et F sont de dimensions finies on a donc $\operatorname{rg} u \leqslant \min(\dim E, \dim F)$

Théorème - Equivalences des caractères de u (cas dimension finie)
E, F deux K-espaces vectoriels de **dimensions finies égales** ($\dim F = \dim E$). Soit $u \in \mathscr{L}(E,F)$. On a équivalence de
(i) $\operatorname{rg} u = \dim E$
(ii) u est injective
(iii) u est surjective
(iv) u est bijective (donc un isomorphisme)

Démonstration

— (i) ⇔ (ii) d'après la propriété précédente (première partie).
— Comme $\dim F = \dim E$, (i) ⇔ (iii) d'après la propriété précédente (seconde partie).
— Donc (i) ⇒ (ii) et (iii) ⇒ (iv).
Réciproquement, si (iv) alors u est un isomorphisme de E sur F, $\operatorname{rg} u = \dim F = \dim E$ (surjection)

□

Remarque - Dans la pratique : u endomorphisme
On exploite souvent ce théorème dans le cas où $u \in \mathscr{L}(E)$ et donc $E = F$. Les deux espaces ont nécessairement la même dimension.
Il n'y a plus d'hypothèses spécifiques à vérifier. Ce qui donne la caractérisation des automorphismes qui suit

Proposition - Conservation du rang
E, F, G trois $\mathbb{K}$-espaces vectoriels de dimensions finies, $u \in \mathscr{L}(E,F)$, $v \in \mathscr{L}(F,G)$.
— si u est un isomorphisme, alors $\operatorname{rg}(v \circ u) = \operatorname{rg} v$
— si v est un isomorphisme, alors $\operatorname{rg}(v \circ u) = \operatorname{rg} u$

Démonstration
On a le graphe :

$$E \xrightarrow{u} F \xrightarrow{v} G$$

Et donc les relations :

$$\operatorname{Im} v\circ u = \operatorname{Im} v_{|\operatorname{Im} u} \qquad \operatorname{Ker} v\circ u = \{x \mid u(x)\in \operatorname{Ker} v\}$$

Si u est un isomorphisme, $\operatorname{Im} u = F$ et donc $\operatorname{rg}(v_{|\operatorname{Im} u} = \operatorname{rg}(v)$.
Si v est un isomorphisme, $u(x)\in\operatorname{Ker} v \Leftrightarrow u(x)=0 \Leftrightarrow x\in\operatorname{Ker} u$.
donc $\dim\operatorname{Ker} v\circ u = \dim\operatorname{Ker} u$, par théorème du rang $\operatorname{rg}(v\circ u)=\operatorname{rg} u$. □

On obtient ainsi la caractérisation des automorphismes en dimension finie :

Théorème - Cas des endomorphismes
E un $\mathbb{K}$-espace vectoriel de **dimension finie** n. Soit $u\in\mathscr{L}(E)$. On a équivalence de
(i) $\operatorname{rg} u = n$
(ii) u est injective
(iii) u est surjective
(iv) u est bijective (donc un automorphisme, soit $u\in GL(E)$)
(v) il existe $v\in\mathscr{L}(E)$ tel que $v\circ u = Id_E$ (u admet un inverse à gauche)
(vi) il existe $w\in\mathscr{L}(E)$ tel que $u\circ w = Id_E$ (u admet un inverse à droite)

4.3. Itération

Proposition - Majoration de rg $(v\circ u)$ en toute généralité
Soient $u\in\mathscr{L}(E,F)$ et $v\in\mathscr{L}(F,G)$, avec E et F de dimensions finies.
Alors $\operatorname{rg}(v\circ u)\leqslant\min(\operatorname{rg} u,\operatorname{rg} v)$.

Démonstration
$\operatorname{Im}(v\circ u)\subset\operatorname{Im} v$. Il suffit de prendre les dimensions pour une première inégalité.
$\operatorname{Ker} u\subset\operatorname{Ker} v\circ u$, ainsi $\dim\operatorname{Ker} u\leqslant\dim\operatorname{Ker} v\circ u$, donc (théorème du rang) :

$$\operatorname{rg} u = \dim E - \dim\operatorname{Ker} u \geqslant \dim E - \dim\operatorname{Ker}(v\circ u) = \operatorname{rg}(v\circ u)$$

□

Savoir faire - Exploiter le rang d'endomorphisme restreint ou composé
Pour les inégalités sur les rang, ou les inclusions Im /Ker, on exploite :
— la composition (cf. démonstration précédente)
— la restriction à A sev de E : $u_{|A}$
On pense : $u_{|A} : A\to F,\ x\mapsto u(x)$, on a $\operatorname{Ker} u_{|A} = \operatorname{Ker} u\cap A$ donc $\operatorname{rg} u_{|A} = \dim A - \dim(\operatorname{Ker} u\cap A)$.

L'exercice suivant est classique (première question). La fin est importante :
Exercice
Soit $u\in\mathscr{L}(E)$, avec E de dimension finie. On note, pour tout $r\in\mathbb{N}$, $I_r = \operatorname{Im} u^r$ et $i_r = \dim(I_r)$ et $K_r = \operatorname{Ker} u^r$ et $k_r = \dim K_r$.

1. Montrer que $K_r\subset K_{r+1}$ et $I_{r+1}\subset I_r$. Qu'en déduire pour les suites (i_r) et (k_r).
2. Montrer que $K_r = K_{r+1}$ si et seulement si $I_{r+1} = I_r$.
3. On note $s = \min\{r \mid K_r = K_{r+1}\}$. Montrer que s existe et que $\forall\, r\geqslant s$, $K_r = K_s$ (et $I_r = I_s$).
Montrer que dans ce cas $E = K_s\oplus I_s$.
4. Montrer que pour tout $r\leqslant s+1$, $k_{r+1}-k_r\leqslant k_r - k_{r-1}$.
On dit que la suite (k_r) est concave. De même ici, on dirait que (i_r) est convexe.
On pourra considérer H tel que $K_{r+1} = H\oplus K_r$ et $u_{|H} : H\to K_r$, bijective...

Correction

1. Si $x\in K_r$, alors $u^{r+1}(x) = u(u^r(x)) = u(0) = 0$ (u linéaire), donc $x\in K_{r+1}$.
Si $y\in I_{r+1}$, alors il existe $a\in E$, tel que $y = u^{r+1}(a) = u^r(u(a))$, donc $y\in I_{r+1}$.
La suite (k_r) est croissante, la suite (i_r) est décroissante.
2. En exploitant les dimensions, (et les inclusions précédentes) on a
$K_r = K_{r+1}\Leftrightarrow k_r = k_{r+1}\Leftrightarrow \dim E - i_r = \dim E - i_{r+1}\Leftrightarrow I_{r+1} = I_r$.
3. (k_r) est une suite d'entiers, décroissante, nécessairement elle stationne, donc $\{r \mid K_r = K_{r+1}\}$ est non vide et admet un plus petit élément. Ainsi s existe. On a alors, par récurrence immédiate : $K_{r+1} = K_r$, pour tout $r\geqslant s$ et donc les suites (d'ensembles ou de nombres concernés ici) sont constantes $\forall\, r\geqslant s$, $K_r = K_s$ (et $I_r = I_s$).
Puis, dans ce cas, si $x\in K_r\cap I_r$, alors $x = u^s(a)$ et $u^{2s}(a) = u^s(x) = 0$, donc $a\in K_{2s} = K_s$, donc $x = u^s(a) = 0$.
Pour des raisons de dimensions : $E = K_s\oplus I_s$.
4. C'est la question difficile.
On sait que $K_r\subset K_{r+1}$, de dimension finie. Donc il existe $H\subset E$ tel que $K_{r+1} = H\oplus K_r$.
Appliquons alors le théorème du rang à $u_{|H}$, on a donc :

$$\dim K_{r+1} - \dim K_r = \dim H = \operatorname{rg} u_{|H} + \dim(\operatorname{Ker} u\cap H)$$

Par ailleurs, si $x\in\operatorname{Ker} u\cap H$, alors $u\in K_1\subset K_r$, donc $x\in K_r\cap H = \{0\}$ donc $x = 0$
Donc $\dim(\operatorname{Ker} u\cap H) = 0$ et $\dim K_{r+1} - \dim K_r = \dim H = \operatorname{rg} u_{|H}$.
Et $\operatorname{Im} u_{|H}\subset K_r$ car si $x\in\operatorname{Im} u_{|H}$, alors $\exists\, a\in H$ tel que $x = u(a)$.
et donc $u^r(x) = u^{r+1}(a) = 0$ car $a\in H\subset K_{r+1}$.
Et en même temps, si $x\in\operatorname{Im} u_{|H}\cap K_{r-1}$, alors $\exists\, a\in H$ tel que $x = u(a)$ et $0 = u^{r-1}(x) = u^r(a)$
donc $a\in H\cap K_r = \{0\}$, donc $a = 0$ et $x = 0$. Ainsi $\operatorname{Im} u_{|H}\cap K_{r-1} = \{0\}$.
Donc $K_{r-1}\oplus\operatorname{Im} u_{|H}\subset K_r$, donc $\operatorname{rg} u_{|H} = \dim\operatorname{Im} u_{|H}\leqslant k_r - k_{r-1}$.
Finalement : $k_{r+1} - k_r\leqslant k_r - k_{r-1}$. Par théorème du rang : $i_r - i_{r+1}\leqslant i_{r-1} - i_r$. On dit que la suite (i_r) est convexe. De même ici, on dirait que (k_r) est concave.

4.4. Formes linéaires et hyperplans

Bases duales

Définition - Forme linéaire coordonnée
Soit $\mathscr{B} = (e_i)_{i\in I}$ une base de l'espace vectoriel E.
On note e_i^* l'unique forme linéaire sur E vérifiant

$$\forall\, j\in I, e_i^*(e_j) = \delta_i^j = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ si } i\neq j \end{cases}.$$

On l'appelle forme linéaire coordonnée d'indice i relative à la base $\mathscr{B}$

Autre nom :

Proposition - Base duale
Soit $\mathscr{B} = (e_i)_{i\in I}$ une base de l'espace vectoriel E.
Alors $\mathscr{B}^* = (e_i^*)_{i\in I}$ est une base de $\mathscr{L}(E,\mathbb{K}) = E^*$, appelée base duale de $\mathscr{B}$

On aurait pu exploiter les dimensions, mais pédagogiquement, on montre plus :

Démonstration
• Supposons que $\sum_{i\in I}\lambda_i e_i^* = 0_{E^*}$.
Donc en e_k : $0_{E^*}(e_k) = 0 = \sum_{i\in I}\lambda_i e_i^*(e_k)\sum_{i\in I}\lambda_i\delta_{i,k} = \lambda_k$ Donc la famille $\mathscr{B}^*$ est libre.
• Soit $f\in E^*$. On note $\alpha_i = f(e_i)$
Pour tout $x = \sum_{k\in I} x_k e_k\in E$,

$$\sum_{i\in I}\alpha_i e_i^*(x) = \sum_{i\in I}\alpha_i\sum_{k\in I}x_k e_i^*(e_k) = \sum_{i\in I}\alpha_i\sum_{k\in I}x_k e_i^*(e_k) = \sum_{i\in I}\lambda_i x_i$$

Et

$$f(x) = f\left(\sum_{k\in I}x_k e_k\right) = \sum_{k\in I}x_k f(e_k) = \sum_{k\in I}x_k\alpha_k$$

Donc $f = \sum_{i\in I}\alpha_i e_i^*$. □

Hyperplan et équation d'un hyperplan

Proposition - Noyau de forme linéaire et hyperplan
Soit H un sous-espace vectoriel de E. On a équivalence des propriétés :

(1) il existe une droite vectorielle D telle que $E = H \oplus D$
(2) il existe une forme linéaire non nulle φ telle que $H = \text{Ker}\,\varphi$

Si ces propriétés sont vérifiées on dit que H est un hyperplan (vectoriel) de E.

Démonstration
Si $E = H \oplus D$, avec D une droite, donc $D = \text{vect}(x)$.
On note p, la projection sur D, parallèlement à H.
Alors $y \in H$ ssi $p(y) = 0$. Mais p n'est pas une forme linéaire.
Pour tout $a \in E$, $p(a) \in D$, donc il existe $\lambda_a \in \mathbb{K}$ tel que $p(a) = \lambda_a x$.
On a alors $H = \text{Ker}\,\varphi$ avec $\varphi : a \mapsto \lambda_a$, forme linéaire.
Réciproquement, si $H = \text{Ker}\,\varphi$ avec φ non nul,
alors il existe $a \in E$ tel que $\varphi(a) \neq 0$.
Notons $D = \text{vect}(a)$.
Soit $x \in E$, $y = x - \frac{\varphi(x)}{\varphi(a)} a$.
Alors, par linéarité, $\varphi(y) = \varphi(x) - \frac{\varphi(x)}{\varphi(a)}\varphi(a) = 0$, donc $y \in H$.
$z = \frac{\varphi(x)}{\varphi(a)} a \in D$ et donc $E = D + H$.
Enfin, si $x \in D \cap H$, alors $x = \lambda a$, avec $0 = \varphi(x) = \lambda\varphi(a)$ et donc $\lambda = 0$ (car $\varphi(a) \neq 0$).
Ainsi $x = 0$ et donc $D \oplus H$. □

D'après la démonstration.

Corollaire - Choix d'un supplémentaire
Si H est un hyperplan de E et si $a \notin H$, alors $E = H \oplus \text{vect}(a)$.

Corollaire - Version forme linéaire
Soit $\varphi \in E^*$. Alors pour tout $x \notin \text{Ker}\,\varphi$, $E = \text{Ker}\,\varphi \oplus \text{vect}(x)$.

Démonstration
Si $x \notin \text{Ker}\,\varphi$, et $\lambda = \varphi(x)$,
alors pour tout $a \in E$, $a = \underbrace{(a - \frac{\varphi(a)}{\lambda} x)}_{\in \text{Ker}\,\varphi} + \underbrace{\frac{\varphi(a)}{\lambda} x}_{\in \text{vect}(x)}$. On montre également l'unicité. □

Proposition - Proportionnalité des formes linéaires
Deux formes linéaires φ et ψ sont proportionnelles si et seulement elles ont le même noyau, c'est-à-dire que pour $\phi, \psi \in \mathscr{L}(E, \mathbb{K})$,

$$\text{Ker}\,\varphi = \text{Ker}\,\psi \Leftrightarrow \exists \lambda \in \mathbb{K}^* \mid \varphi = \lambda\psi$$

Démonstration
Si $\exists \lambda \in \mathbb{K}^* \mid \varphi = \lambda\psi$, alors :

$$x \in \text{Ker}\,\varphi \Leftrightarrow \varphi(x) = 0 \Leftrightarrow \psi(x) = \frac{1}{\lambda}\varphi(x) = 0 \Leftrightarrow x \in \text{Ker}\,\phi$$

Réciproquement, si $H = \text{Ker}\,\varphi = \text{Ker}\,\psi$.
Il existe $D = \text{vect}(a)$ tel que $E = D \oplus \text{Ker}\,\varphi = D \oplus \text{Ker}\,\psi$.
Soit $x \in E$, $\exists\, \lambda \in \mathbb{K}, z \in H$ tels que $x = \lambda a + z$ $\varphi(x) = \lambda\varphi(a)$ et $\psi(x) = \lambda\psi(a)$.
Et donc $\varphi(x) = \frac{\varphi(a)}{\psi(a)}\psi(x)$. Donc $\varphi = A \times \psi$ avec $A = \frac{\varphi(a)}{\psi(a)}$. □

Pour aller plus loin - Produit scalaire
On appelle crochet de dualité, l'application bilinéaire de $E^* \times E$ dans $\mathbb{K}$:

$$< \sum_{i=1}^{n} a_i e_i^* \mid \sum_{j=1}^{n} b_j e_j >= \sum_{k=1}^{n} a_k b_k$$

C'est une forme de produit scalaire. Elle fait le lien algébrique avec les fameux « bra-kets » de la mécanique quantique.

Définition - Equation d'un (hyper)plan
Soient H un hyperplan et $\varphi \in \mathscr{L}(E, \mathbb{K})$ tels que $H = \text{Ker}\,\varphi$. Alors l'equation $\varphi(x) = 0$ s'appelle une équation de H.

Remarque - Infinité d'équations
H admet alors une infinité d'équations, obtenues en écrivant $\lambda\varphi(x) = 0$ avec $\lambda \in \mathbb{K} \setminus \{0\}$.

Proposition - Cas de la dimension finie
Les hyperplans d'un espace vectoriel E de dimension finie n sont exactement les sous-espaces de dimension $n-1$.
Dans une base $(e_1, \ldots, e_n)$ donnée, ce sont les ensembles d'équation

$$a_1 x_1 + \cdots + a_n x_n = 0$$

où $(a_1, \ldots, a_n) \in \mathbb{K}^n \setminus \{0_{\mathbb{K}^n}\}$, $(x_1, \ldots, x_n)$ étant les coordonnées de $x \in E$ dans la base $(e_1, \ldots, e_n)$.

Démonstration
Comme D est une droite vectoriel, $\dim H = \dim E - \dim D = n - 1$.
$H = \text{Ker}\,\varphi$. Or il existe $a_1 (= \varphi(e_1)), a_2, \ldots a_n (= \varphi(e_n)) \in \mathbb{K}$ tel que

$$\varphi : x = \sum_{i=1}^{n} x_i e_1 \longrightarrow \sum_{i=1}^{n} x_i a_i$$

On a donc $H = \{x = \sum_{i=1}^{n} x_i e_i \in E \mid a_1 x_1 + \cdots + a_n x_n = 0\}$ □

Intersection d'hyperplans et dimension

Heuristique - Une équation : un degré perdu
On commence dans un espace vectoriel de dimension n.
A chaque équation, la dimension diminue de une unité.
Les seules exceptions : si une nouvelle équation est une combinaison linéaire des précédentes.
Réciproquement, un sous-espace vectoriel de dimension r dans E de dimension n est le noyau de $n - r$ forme linéaires, ou autrement écrit est obtenu à partir de $n - r$ équations.

Proposition - Réduction des dimensions
Soient $m \in \mathbb{N}^*$ et $H_1, \ldots, H_m$ des hyperplans de E. Alors

$$\dim\left(\bigcap_{i=1}^{m} H_i\right) \geqslant \dim E - m.$$

On commence par un lemme

Lemme -
Soit φ une forme linéaire définie sur E et F, un sev de E de dimension finie égale à p.
Alors $F \cap \text{Ker}\,\varphi$ est de dimension finie et $p - 1 \leqslant \dim(F \cap \text{Ker}\,\varphi) \leqslant p$.
Précisément : $\dim(F \cap \text{Ker}\,\varphi) = p \Leftrightarrow F \subset \text{Ker}\,\varphi \Leftrightarrow \text{rg}\,\varphi_{|F} = 0$. Sinon $\dim(F \cap \text{Ker}\,\varphi) = p - 1$.

Démonstration
Notons que le théorème du rang appliqué à $\varphi_{|F}$ donne :

$$\dim F = \operatorname{rg}\varphi_{|F} + \dim \operatorname{Ker}\varphi \cap F$$

Or φ étant une forme linéaire, $\operatorname{rg}\varphi_{|F} \leqslant \operatorname{rg}\varphi \leqslant 1$.
On a alors les équivalences :

$$\operatorname{rg}\varphi_{|F} = 0 \Leftrightarrow \dim \operatorname{Ker}\varphi \cap F = \dim F \Leftrightarrow \operatorname{Ker}\varphi \cap F = F \Leftrightarrow F \subset \operatorname{Ker}\varphi$$

□

Démonstration
Par récurrence sur m, en exploitant le lemme.
D'abord, le résultat est vrai pour $m = 1$: $\dim H_1 = \dim E - 1 \geqslant \dim E - 1$.
Supposons que le résultat est vrai pour m.
Soient $H_1, \dots H_{m+1}$ $m+1$ hyperplans de E.
Notons $F = H_1 \cap \dots \cap H_m$. Alors d'après l'hypothèse de récurrence, $\dim(F) \geqslant n - m$.
Puis, $\left(\bigcap_{i=1}^{m} H_i\right) = F \cap H_{m+1}$.
Soit φ_{m+1}, une forme linéaire telle que $H_{m+1} = \varphi_{m+1}$.
On applique le résultat du lemme : $\dim\left(\bigcap_{i=1}^{m} H_i\right) = \dim(F \cap H_{m+1}) \geqslant \dim F - 1 = n - (m+1)$
Avec $\mathscr{P}_m$ est vraie. On trouve bien, $n - m - 1 = \dim H - 1 \leqslant \dim(H \cap H_{m+1})$ □

Proposition - Expression exacte
Soient E de dimension n, F un sous-espace vectoriel de E de dimension $n - m$ ($m \in \mathbb{N}^*$). Alors il existe m hyperplans $H_1, H_2, \dots, H_m$ de E tels que $F = \bigcap_{i=1}^{m} H_i$.

Démonstration
Notons $(f_{m+1}, \dots f_n)$ une base de F. On peut la compléter avec $g_1, \dots g_m$ en une base de E.
Soit $D_i = \operatorname{vect}(g_i)$, de dimension 1 et $H_i = \operatorname{vect}(g_1, \dots g_{i-1}, g_{i+1}, \dots g_m, f_{m+1}, \dots f_n)$ un hyperplan supplémentaire à D_i dans E.
Supposons que $x = \sum_{i=1}^{m} \lambda_i g_i + \sum_{j=m}^{n} \mu_j f_j$.
On a alors l'écriture de x selon $E = D_i \oplus H_i$: $x = \lambda_i g_i + (x - \lambda_i g_i)$.

$$x \in \bigcap_{i=1}^{m} H_i \Leftrightarrow \forall\, i \in \mathbb{N}_m\, x \in H_i \Leftrightarrow \forall\, i \in \mathbb{N}_m\, \lambda_i = 0 \Leftrightarrow x \in F$$

□

Corollaire - Interprétation géométrique
Dans $\mathbb{R}^2$:
- les hyperplans vectoriels sont les droites vectorielles
- l'intersection de deux droites est de dimension $\geqslant 0$ (en fait 0 ou 1)
- le s.e.v. $\{0_{\mathbb{R}^2}\}$, de dimension $0 = 2 - 2$, s'écrit comme intersection de deux droites.

Dans $\mathbb{R}^3$:
- les hyperplans vectoriels sont les plans vectoriels
- l'intersection de deux plans est de dimension $\geqslant 1$ (en fait 1 ou 2)
- les droites, de dimension $1 = 3 - 2$, s'écrivent comme intersection de deux plans
- le s.e.v. $\{0_{\mathbb{R}^2}\}$, de dimension $0 = 3 - 3$, s'écrit comme intersection de trois plans.

Dans les deux cas, on retrouve bien les équations usuelles de droites vectorielles dans $\mathbb{R}^2$, de plans vectoriels ou de droites vectorielles dans $\mathbb{R}^3$.

5. Rang (et noyau) d'une matrice

5.1. Rappel sur la résolution d'un système linéaire

Proposition - Résolution (théorique) d'un système linéaire
On doit résoudre le système $(S) : AX = b$ d'inconnue X, avec $A \in \mathscr{M}_{n,p}(\mathbb{K})$.
- Si $b \notin \operatorname{Im} A$, alors $\mathscr{S} = \emptyset$
- Si $b \in \operatorname{Im} A$.
  Alors il existe $X_0 \in \mathscr{M}_{p,1}(\mathbb{K})$ tel que $A \times X_0 = b$.

$$AX = b \Longleftrightarrow A(X - X_0) = 0 \Longleftrightarrow X - X_0 \in \operatorname{Ker} A$$

Alors $\mathscr{S} = X_0 + \operatorname{Ker} A = \{X_0 + Y, Y \in \operatorname{Ker} A\}$ (espace affine).

Savoir faire - Résolution pratique d'un système linéaire
Soit, à résoudre, le système non carrée $AX = b$.

1. On exploite la méthode du pivot de Gauss pour échelonner le système.
   On obtient un système de la forme

$$(E)\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 & +\dots+\dots+\dots+ a_{1,p}x_p &=& b_1 \\ \ddots & \vdots \quad\vdots\quad\vdots & & \\ & a_{r,r+k}x_{r+k}+\dots+a_{r,p}x_p &=& b_r \\ & 0 &=& b_{r+1} \\ & \vdots \quad\vdots\quad\vdots & & \\ & 0 &=& b_n \end{cases} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ équations principales} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} \begin{matrix} n-r \\ \text{équations} \\ \text{auxiliaires} \end{matrix} \end{matrix}$$

   Dans ce cas r est appelé rang du système.
   Et $x_1, x_2 \dots x_r$ sont appelés les inconnues principales et $x_{r+1}, x_{r+2}, \dots x_p$ sont appelés les inconnues auxiliaires ou les variables libres
2. On commente le système échelonné :
   - Combien d'équations principales : c'est le rang de A (voir plus bas)
   - Combien de variables libres?
   - Quel variable libre choisir?
   - Exprimer les variables principales en fonction des variables libres
3. Donner la forme de l'ensemble des solutions du système sous forme de combinaisons linéaires

Exercice

Résoudre $\begin{cases} x + y + z = 2 \\ x + y - z = -1 \\ 2x + 2y = 3 \end{cases}$ et $\begin{cases} x + y + z = 2 \\ x + y - z = -1 \\ 2x + 2y = 1 \end{cases}$

Correction
Le premier n'a pas de solution, $b \notin \operatorname{vect} A$, le second a une variable libre et la solution est $\{(0, \frac{1}{2}, \frac{3}{2}) + y(-1, 1, 0), y \in \mathbb{R}\}$

Heuristique - Synthèse
On a vu qu'il y a une correspondance (calcul de l'inverse) entre la donnée d'une matrice A et la donnée d'un système $\mathscr{S} : AX = 0$. Mais :
- Le rg (A) est défini à partir des colonnes de A : $\operatorname{rg}(A) = \dim(\operatorname{Im} A)$ (voir plus loin)
- Le rg $(\mathscr{S})$ est défini à partir des lignes de $\mathscr{S}$ (donc de A) : nombre pivots non nuls lorsqu'on échelonne $\mathscr{S}$

Est-ce toujours la même valeur? Et si oui, comment le démontrer? Avec le noyau, ou mieux avec la transformation qui va suivre…

5.2. « Action » des matrices sur $\mathbb{K}^n \equiv \mathscr{M}_{n,1}(\mathbb{K})$

D'après le produit par blocs :

Pour aller plus loin - Action d'un groupe sur un ensemble
On dit qu'un groupe G agit sur un ensemble E, s'il existe une opération (loi interne) naturel

$$G \times E \to E, (a, x) \mapsto a \cdot x$$

qui vérifie $e_G \cdot x = x$ pour tout x et $(a \times b) \cdot x =$

Proposition - Multiplication à droite par une colonne : c.l. des colonnes
Soit $A = (C_1|C_2|\cdots|C_p)$, une matrice (association de colonnes de taille n).
Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$, une matrice colonne.
On a alors AX qui est une matrice colonne, plus précisément :
$$AX = x_1C_1 + x_2C_2 + \cdots + x_pC_p,$$
combinaison linéaire des colonnes de A, avec les coefficients-scalaires de X.

Ce résultat justifie le point de vue suivant :

5.3. Image d'une matrice et famille génératrice

Définition - Image et rang d'une matrice
Soit $A = (C_1|C_2|\cdots|C_p) \in \mathcal{M}_{n,p}(\mathbb{K})$.
On appelle image de A, l'ensemble
$$\begin{aligned}\text{Im } A &= \text{vect}(C_1, C_2, \ldots, C_p)\\ &= \{x_1C_1 + x_2C_2 + \cdots + x_pC_p, x_1, x_2, \ldots x_p \in \mathbb{K}\}\\ &= \{A \times X \mid X \in \mathcal{M}_{p,1}(\mathbb{K})\}\end{aligned}.$$
Il s'agit du sous espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{K})$ (des matrices colonnes) engendré par les p colonnes de A.
On appelle rang de A, noté rg (A), la dimension de Im A.

Par définition, Im A (de dimension r) est un s.e.v. de $\mathcal{M}_{n,1}(\mathbb{K})$ (de dimension n).
Ils sont égaux, si et seulement si ils ont la même dimension :

Proposition - Famille génératrice, rang d'une matrice
Soit $A = (C_1|C_2|\cdots|C_p) \in \mathcal{M}_{n,p}(\mathbb{K})$. Supposons que le rang de A est r.
Alors $(C_1, C_2, \ldots, C_p)$ est génératrice de $\mathcal{M}_{n,1}(\mathbb{K})$, i.e. Im $A = \mathcal{M}_{n,1}(\mathbb{K})$ si et seulement si $r = n$

Remarque - Pour les systèmes linéaires
On reprendra ce résultat lors de l'étude complète des systèmes linéaires

5.4. Noyau d'une matrice et famille libre

Analyse - Les colonnes de A forment-elles une famille libre ?
Nous avons vu un critère simple pour voir si les colonnes de $A = (C_1|\cdots|C_p)$ sont génératrices de $\mathcal{M}_{n,1}(\mathbb{K})$.
La question qui se pose ensuite est de savoir s'ils forment dans leur ensemble une famille libre.
Il s'agit donc de montrer que
$$\sum_{i=1}^{p} x_iC_i = 0 \Rightarrow \forall\, i \in \mathbb{N}_p, x_i = 0$$
La proposition de gauche est exactement celle-ci : $AX = 0$, celle de droite est $X = 0$.
Donc $(C_1, C_2, \cdots C_p)$ libre ssi $\{X \in \mathcal{M}_{p,1}(\mathbb{K}) \mid AX = 0\} = \{0_p\}$

Définition - Noyau d'une matrice
Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$.
On appelle noyau de A, l'ensemble
$$\text{Ker } A = \{X \in \mathcal{M}_{p,1}(\mathbb{K}) \mid AX = 0\}.$$

Il s'agit d'un sous espace vectoriel de $\mathcal{M}_{p,1}(\mathbb{K})$.

Exercice
Démontrer qu'il s'agit bien de sous-espaces vectoriels.

Correction
$A \times 0 = 0$, donc Ker A est non vide.
Si $X_1, X_2 \in \text{Ker } A$ et $\lambda_1, \lambda_2 \in \mathbb{K}$, alors $A \times (\lambda_1X_1 + \lambda_2X_2) = \lambda_1AX_1 + \lambda_2AX_2 = 0 + 0 = 0$.
Donc $\lambda_1X_1 + \lambda_2X_2 \in \text{Ker } A$.
D'après l'analyse faite quelques lignes plus haut :

Proposition - Famille libre, noyau d'une matrice
Soit $A = (C_1|C_2|\cdots|C_p) \in \mathcal{M}_{n,p}(\mathbb{K})$.
$(C_1, C_2, \ldots, C_p)$ est une famille libre de $\mathcal{M}_{n,1}(\mathbb{K})$ ssi Ker $A = \{0\}$

5.5. Théorème du rang

Théorème - Théorème du rang
Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors : $\dim(\text{Ker } A) + \text{rg}(A) = p$

Démonstration
Soit $Y_1, Y_2, \ldots Y_m$, une base de Ker A.
Comme Ker $A \subset \mathcal{M}_{n,1}(\mathbb{K})$, on peut la compléter en une base de $\mathcal{M}_{n,1}(\mathbb{K})$.
Notons $Y_1, Y_2, \ldots Y_m, Y_{m+1}, \ldots Y_n$, cette base complétée.
$$\text{Im } A = \{AX, X \in \mathcal{M}_{n,1}(\mathbb{K}) = \{A\sum_{k=1}^{n} a_kY_k, (a_1, \ldots a_n) \in \mathbb{K}^n\} = \{A\sum_{k=m+1}^{n} a_kY_k, (a_{m+1}, \ldots a_n) \in \mathbb{K}^n\}$$
car $AY_1 = AY_2 = \ldots AY_m = 0$.
Finalement
$$\text{Im } A = \text{vect}(AY_{m+1}, \ldots AY_n)$$
Or cette dernière famille est libre :
$$\sum_{k=m+1}^{n} b_kAY_k = 0 \Leftrightarrow \sum_{k=m+1}^{n} b_kY_k \in \text{Ker } A \Leftrightarrow \sum_{k=m+1}^{n} b_kY_k = 0$$
car $\text{vect}(Y_{m+1}, \ldots Y_n) \oplus \text{Ker } A$, donc
$$\sum_{k=m+1}^{n} b_kAY_k = 0 \Leftrightarrow \forall\, k \in [\![m+1, n]\!], b_k = 0$$
car $(Y_{m+1}, \ldots Y_n)$ est une famille libre. Donc rg $(A) = \dim(\text{Im } A) = n - (m+1) + 1 = n - m = n - \dim \text{Ker } A$ □

5.6. Bilan : nouveau critère d'inversibilité (pour une matrice carrée)

Théorème - Noyau de A, image de A et inversibilité
Soit $A \in \mathcal{M}_n(\mathbb{K})$.
Alors, les quatre propositions suivantes sont équivalentes :
i) A est inversible
ii) Ker $A = \{0\}$
iii) Im $A = \mathcal{M}_{n,1}(\mathbb{K})$
iv) le rang de A est égal à n

Attention - Les ensembles du contexte
Il faut bien faire attention qu'ici la matrice carrée de taille $n \times n$ agit sur l'espace des matrices colonnes de taille $n \times 1$.
Ici $p = n$, cela est nécessaire pour espérer que la matrice soit carrée.
On étudie donc alternativement les actions de A sur les deux espaces $\mathcal{M}_{n,n}(\mathbb{K}) = \mathcal{M}_n(\mathbb{K})$ (première partie précédente) et $\mathcal{M}_{n,1}(\mathbb{K})$ (sur cette

, partie)

Démonstration
Notons $A = (C_1|C_2|\cdots|C_n)$.
1. Avec le théorème du rang, on peut affirmer immédiatement que ii) et iii) sont équivalentes. 2. De même nous avons vu que les propositions iii) et iv) sont équivalentes.
3. Enfin montrons que i)⇒ ii) et que iii)=ii)⇒ i).
Si A est inversible.
Soit $X \in \text{Ker } A$, alors $AX = 0$ et donc $A^{-1}AX = X = A^{-1} \times 0 = 0$.
Donc $X = 0$ et donc $\text{Ker } A \subset \{0\}$.
L'inclusion réciproque est vraie donc $\text{Ker } A = \{0\}$.
Si $\text{Im } A = \mathcal{M}_{n,1}(\mathbb{K})$.
Alors $E_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \text{Im } A$, donc il existe X_1 tel que $AX_1 = E_1$.
De même pour tout $i \in \mathbb{N}_n$, où E_i est une colonne de 0 excepté en ligne i où il y a un 1.
Et donc $A \times (X_1|X_2|\cdots|X_n) = (AX_1|AX_2|\cdots AX_n) = (E_1|E_2|\cdots E_n) = I_n$.
Ainsi, A est inversible, et $A^{-1} = (X_1|X_2|\cdots|X_n)$ □

Exercice

Avec $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ -1 & -2 & -3 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 4 & -2 \\ 1 & -2 & 1 \end{pmatrix}$, on voit que $A \times B = 0$.
Pourquoi est-il simple de voir (autrement) que A et B ne sont pas inversibles ?
Quelles sont les dimensions des noyaux et images de A et de B

Correction

On voit que pour B, on a $C_1 = C_3$, donc $C_1 - C_3 = 0$, cela correspond au calcul $B \times \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = 0$.
et donc $\text{Ker } B \neq \{0\}$ et B n'est pas inversible.
On voit que pour A, on a $L_1 = -L_3$
donc pour tout $X \in \mathcal{M}_{3,1}(\mathbb{K})$, le coefficient de $Y = AX$ en ligne 1 est nécessairement opposé à celui en ligne 3,
par conséquent, on a nécessairement (par exemple) $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \notin \text{Im } A$ et donc A ne peut être inversible.
On a $\dim(\text{Ker } A) = 1$, $\text{rg}(A) = 2$,$\dim(\text{Ker } B) = 2$ et $\text{rg}(B) = 1$

5.7. Action : $(P,Q) \cdot M \mapsto P \times M \times Q^{-1}$

Heuristique - Précision sur les classes d'équivalence
Lorsque deux matrices sont équivalentes, on dit qu'elles sont dans une même classe d'équivalence.
La bonne habitude consiste alors à décrire cette classe d'équivalence en choisissant un représentant plus ou moins naturel (le plus simple).
(Comme pour l'angle principal $\theta_0 \in]-\pi,\pi[$ représentant de la classe d'équivalence $\{\theta \mid e^{i\theta} = a, \text{ avec } |a| = 1\} = \{\theta_0 + 2k\pi, k \in \mathbb{Z}\}$).
Pour y arriver, une bonne méthode consiste d'abord à chercher un invariant, c'est-à-dire un objet (mathématique) caractéristique des classes d'équivalence

$$T(A) = T(B) \Longleftrightarrow A \text{ et } B \text{ sont équivalentes}$$

Cet invariant est le rang de A. Et le représentant sera la matrice $J_r(n,p)$

Nous avons vu que toute matrice inversible pouvait s'écrire comme produit de matrices élémentaires (transvection, dilatation, transposition) (il suffit d'appliquer l'algorithme de Gauss à son inverse).

Remarque - Inversibilité comme un cas particulier...
Nous avons vu que les opérations élémentaires conservent le caractère d'inversibilité d'une matrice.
Peut-être conservent-elles quelque chose de plus « large », autrement dit l'inversibilité serait qu'un cas particulier.
En effet, elles conservent le rang. Une matrice A est alors inversible ssi $r = n$.

Analyse - Reprise de l'algorithme de Gauss
Considérons une matrice A,

1. Par produit à gauche avec des matrice de transvection et transposition, on peut rendre A sous la forme d'une matrice échelonnée A_e.
On rappelle qu'on appelle pivot, les éléments non nuls qui bordent inférieurement la matrice alors obtenue.
$$A_e = (E_n E_{n-1} \dots E_1) \times A$$
On note r, le nombre de pivots non nuls ainsi obtenus.
2. Puis par produit à gauche (ou à droite) avec des matrices de dilatations, on peut rendre les pivots de A_e égaux à 1. On obtient alors la matrice A_e^1.
$$A_e^1 = (D_k \dots D_1)(E_n E_{n-1} \dots E_1) \times A$$
3. Puis (fin de la résolution de l'algorithme de Gauss), par produit à gauche (toujours), on annule un à un les termes au dessus de la bordure des pivots égaux à 1 (en commençant par les colonnes de fin). On obtient une matrice échelonnée $A_e^{1,0}$, avec r nombres 1 en bordure, non forcément sur la diagonale.
$$A_e^{1,0} = (E'_p E'_{p-1} \dots E'_1)(D_k \dots D_1)(E_n E_{n-1} \dots E_1) \times A$$
4. Puis par produit à droite (pour la première fois), par des matrices de transposition, on peut transformer A en une matrice toute particulière :
$$J_r(n,p) = \begin{pmatrix} I_r & O_{r,p-r} \\ O_{n-r,r} & O_{n-r,p-r} \end{pmatrix} = \underbrace{\left(\prod_{i=p}^{1} E'_i \prod_{j=k}^{1} D_j \prod_{h=n}^{1} E_h\right)}_{P^{-1}} \times A \times \underbrace{\left(\prod_{\ell=m}^{1} E''_\ell\right)}_{Q}$$

Proposition - Conservation du rang
Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$.
Pour toute matrice $U \in GL_n(\mathbb{K})$ (inversible!), alors $\text{rg}(U \times A) = \text{rg}(A)$.
Pour toute matrice $V \in GL_p(\mathbb{K})$ (inversible!), alors $\text{rg}(A \times V) = \text{rg}(A)$.

Démonstration
On note $A = (C_1|C_2|\cdots|C_p)$.
On a alors :
$$X \in \text{vect}(UC_1, UC_2 \dots, UC_p) \Leftrightarrow X = \sum_{k=1}^{p} a_k UC_k = U \times (\sum_{k=1}^{p} a_k C_k)$$
U établit donc une surjection (on parle d'isomorphisme) de Im A sur Im UA.
Et si $UX = UY$, alors $U(X-Y) = 0$, donc $X - Y = 0$, donc $X = Y$, ainsi U est injective.
En fait, U inversible donc injective, indépendamment des espaces considérés
Donc $\dim(\text{Im}(UA)) = \dim(\text{Im}(A))$.
De même Si $X \in \text{Ker } AV$, alors $VX \in \text{Ker } A$. V établit une bijection de $\text{Ker } AV$ sur $\text{Ker } A$.
Donc $\dim \text{Ker } A = \dim \text{Ker}(AV)$ et par théorème du rang : $\text{rg}(A) = \text{rg}(AV)$. □

Il découle alors de l'algorithme du pivot de Gauss :

Proposition - Rang d'une matrice
Soit A, une matrice de $\mathcal{M}_{n,p}(\mathbb{K})$.
$\text{rg}(A)$ est égal au nombre de pivots (non nul) de toute matrice échelonnée obtenue à partir de l'algorithme de Gauss appliqué à A.
C'est-à-dire, $\text{rg}(A)$ est le nombre de pivots de toute matrice échelonnée équivalente à A

Démonstration
Il faut juste démontrer que le rang d'une matrice échelonnée avec r pivots non nuls est r.
Son noyau est trivialement $n - r$. C'est le nombre de lignes nulles.
Par théorème du rang, son rang vaut $n - (n - r) = r$. □

Définition - Matrice « J_r »
Soient n, p deux entiers et $r \leqslant \min(n,p)$.
On définit $J_r(n,p) = (\alpha_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p} \in \mathcal{M}_{n,p}(\mathbb{K})$ où α_{ij} $\begin{cases} 1 \text{ si } i=j\leqslant r \\ 0 \text{ sinon} \end{cases}$

$$J_r(n,p) = \begin{pmatrix} 1 & 0 & & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \\ 0 & \ddots & 1 & 0 & \cdots & \cdots & 0 \\ 0 & & 0 & 0 & \cdots & \cdots & 0 \\ \vdots & & \vdots & \vdots & & & \\ 0 & & 0 & 0 & \cdots & \cdots & 0 \end{pmatrix} = \begin{pmatrix} I_r & O_{r,p-r} \\ O_{n-r,r} & O_{n-r,p-r} \end{pmatrix}$$

$O_{p,q}$ étant la matrice nulle de $\mathcal{M}_{p,q}(\mathbb{K})$.

En l'absence d'ambiguïté sur la taille de la matrice on la note J_r.

Théorème - Représentant normal
$\text{rg}(A) = r$ si et seulement si il existe $P, Q \in GL_n(\mathbb{K})$, tels que $A = PJ_rQ^{-1}$
si et seulement si A et J_r sont équivalentes.

Par transitivité avec J_r :

Corollaire - Invariant
A et B sont équivalentes ssi $\text{rg}(A) = \text{rg}(B)$

Démonstration
Nous avons vu, par l'étude de l'algorithme que si $\text{rg}(A) = r$, alors A est équivalente à $J_r(n,p)$.
La réciproque est vrai :
$AQ = PJ_r$ est de rang r (P est inversible et J_r de rang r).
$A = (PJ_r)Q$ est de rang r car Q est inversible.
□

Proposition - Rang de la A^T
$\text{rg}(A^T) = \text{rg}(A)$

Démonstration
$A = PJ_rQ^{-1}$, et donc $A^T = (Q^T)^{-1}J_r^TP^T$, donc A^T est équivalente à J_r (et à A!).
On en déduit qu'elles ont le même rang. □

5.8. Matrices extraites

Définition - Matrice extraites
On appelle matrice extraite de A toute matrice obtenue en supprimant une ou plusieurs lignes, une ou plusieurs colonnes de A.

Proposition - Extraction est diminition du rang
Soit B une matrice extraite de A, alors $\text{rg}(B) \leqslant \text{rg}(A)$.

Démonstration
Par suite d'opérations élémentaires, qui ne changent pas la valeurs du rang, il est possible de transformer A en une matrice de la forme $\begin{pmatrix} B & C \\ D & E \end{pmatrix}$ où B est la matrice en question, extraite de A.
Puis par opérations élémentaires, on peut échelonner B et donc A en partie.
Notons $r = \text{rg}(B)$. On trouve alors r pivots non nuls dans A. Donc $\text{rg}(A) \geqslant r$. □

On en déduit une méthode pour connaître le rang d'une matrice :

Proposition - Voir le rang d'une matrice
Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$.
Alors $\text{rg}\ A$ est l'ordre maximum d'une matrice carrée inversible extraite de A.

Démonstration
Pour toutes matrices B extraites de A, $\text{rg}(B) \leqslant \text{rg}(A)$.
Il suffit donc maintenant de trouver une matrice B d'ordre r, inversible extraite de A.
$\text{rg}(A) = r = \text{vect}(C_1, C_2, \dots C_p)$.
Donc il existe une famille libre extraite de $(C_i)_{1\leqslant i\leqslant p}$ de r éléments : $(C'_1, \dots C'_r)$, telle que

$$\text{rg}(A) = r = \text{vect}(C_1, C_2, \dots C_p) = \text{vect}(C'_1, \dots C'_r)$$

La matrice $A_1 = \left(C'_1 | C'_2 | \cdots | C'_r\right) \in \mathcal{M}_{n,r}(\mathbb{K})$ est une matrice extraite de A de rang r.
La matrice $A_1^T = \left((L'_1)^T | (L'_2)^T | \cdots | (L'_n)^T\right) \in \mathcal{M}_{r,n}(\mathbb{K})$ est également de rang r.
On peut lui extraire à elle également, $n-r$ colonnes : $A_2 = \left((L''_1)^T | (L''_2)^T | \cdots | (L''_r)^T\right) \in \mathcal{M}_{r,n}(\mathbb{K})$ est de rang r.
Enfin, $B = A_2^T$ est une matrice extraite de A, elle est de rang égale à r également. □

Corollaire - Majoration du rang
Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$, alors
$$\text{rg}\ A \leqslant \min(n,p).$$

Démonstration
Comme $\text{rg}(A) = \text{vect}(C_1, \dots C_p)$, alors $\text{rg}(A) \leqslant p$.
Et comme $\dim \text{Ker}\, A \geqslant 0$, on a aussi $\text{rg}(A) = n - \dim \text{Ker}\, A \leqslant n$ □

Les propositions suivantes sont déjà connues, mais leurs interprétations sont nouvelles : à partir des applications linéaires…

6. Bilan

Synthèse

⇝ On reprend une remarque précédente : les éléments de E s'écrivent les uns à partir des autres par addition et multiplication par constante. Ces descriptions sont potentiellement multiples : nous préférons la description unique qui élimine les quiproquos.
Deux questions :
— est-il possible que $\forall\, u, \exists!(v,w)$ tel que $u = v + w$? Quel contrainte sur v, w ? La réponse, ils sont pris dans des ensembles supplémentaires (deux conditions : existence et unicité)
— est-il possible que $\forall\, u, \exists!(\lambda_i)_{i\in I} \in \mathbb{K}^I$ tel que $u = \sum_{i\in I} \lambda_i e_i$? Quel contrainte sur $(e_i)_{i\in I}$? La réponse, il s'agit d'une famille génératrice de E et libre (deux conditions : existence et unicité)

⇝ Emerge alors la notion de dimension finie. Si dans un espace, il existe une base finie de cardinal n, alors toutes les bases sont du même cardinal. C'est très pratique (cela réduit alors la double contrainte précédente à une seule contrainte.)

⇝ Lorsque les espaces E et F sont de dimensions finies, l'espace $\mathscr{L}(E,F)$ est alors isomorphe à $\mathscr{M}_{\dim E,\dim F}(\mathbb{K})$. On retrouve l'ensemble des résultats sur les matrices, ils s'interprètent de façon renouvelée et réciproquement $\mathscr{M}_{\dim E,\dim F}(\mathbb{K})$ éclaire l'espace $\mathscr{L}(E,F)$.
Et en particulier, on peut retrouver le théorème du rang.

⇝ Enfin, les formes linéaires nous occupent tout particulièrement, car elles sont comme la dualité de la notion de base. Elle permette de reprendre la notion de dimension, par décroissance.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Base incomplète
— Savoir-faire - Montrer qu'une famille est une base
— Savoir-faire - Montrer que deux espaces vectoriels sont égaux
— Savoir-faire - Exploitation (lien matrice/isomorphisme)
— Savoir-faire - Petite aide mnémnotechnique
— Truc & Astuce pour le calcul. Etant données A et B, trouver $\mathscr{B}$, $\mathscr{B}'$ et u.
— Savoir-faire - Exploiter le rang d'endomorphisme restreint ou composé
— Savoir-faire - Résolution pratique d'un système linéaire

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\text{rg}(x_1,x_2,\dots x_n)$	$\dim(\text{vect}(x_1,x_2,\dots x_n))$		
$\text{rg}\,(u)$	Rang de u	$\text{rg}\,(u)=\dim(\text{Im}\,u)$	$\dim E=\dim(\text{Ker}\,A)+\text{rg}\,(A)$, u inversible ssi $\text{rg}\,(A)=\dim E$.
$\text{Tr}(u)$	Trace de u	$\text{Tr}(u)=\text{Tr}\big(\mathscr{M}_{\mathscr{B}}(u)\big)$ (quelle que soit $\mathscr{B}$).	$\text{Tr}(u\circ v)=\text{Tr}(v\circ u)$, si p projecteur : $\text{Tr}(p)=\text{rg}\,(p)$
$\text{Im}\,(A)$	Image de la matrice A	$\text{Im}\,(A)=\text{vect}(C_k(A))=\{AX;X\in\mathscr{M}_{p,1}(\mathbb{K})\}$	
$\text{Ker}\,(A)$	Noyau de la matrice A	$\text{Ker}\,(A)=\{X\in\mathscr{M}_{p,1}\mid AX=0\}$	A inversible ssi $\text{Ker}\,A=\{0\}$
$\text{rg}\,(A)$	Rang de A	$\text{rg}\,(A)=\dim(\text{Im}\,A)$	$p=\dim(\text{Ker}\,A)+\text{rg}\,(A)$, A inversible ssi $\text{rg}\,(A)=p$, $\text{rg}\,(A)=\text{rg}\,(A^T)$
$J_r(n,p)=\begin{pmatrix} I_r & O_{r,p-r} \\ O_{n-r,r} & O_{n-r,p-r}\end{pmatrix}$	Matrice J_r	$\text{rg}\,(A)=r\iff\exists P,Q\in GL_n(\mathbb{K})\times GL_p(\mathbb{K})$ tel que $A=P\times J_r\times Q$	

Retour sur les problèmes

122. En fait, c'est tout le but de ce cours de montrer qu'll s'agit de terminer LES (unique, car c'est une famille libre) coordonnées de $(2,1)$ avec la famille (génératrice de $\mathbb{R}^2$) : $\big((1,1),(1,2)\big)$.
Ici : $(2,1)=3(1,1)-1(1,2)$.
En revanche, $\big((1,1,1),(1,2,1)\big)$ ne forme pas une base de $\mathbb{R}^3$. L'écriture de $(2,1,0)$ comme c.l. de cette famille n'est pas assurée, mais pas nécessairement impossible non plus a priori. Il faut calculer…
En regardant les deux première valeurs, on a nécessairement $(2,1,\cdot)=3(1,1,1)-1(1,2,1)=(2,1,2)$. Ce n'est donc pas possible.

123. Il n'y a pas unicité, la famille considérée n'est pas libre.
En effet : $(2,1,0)=3(1,1,1)+0(1,2,1)-(1,2,3)+0(1,-1,0)=-3(1,1,1)+3(1,2,1)+0(1,2,3)+2(1,-1,0)$.
Ce n'est important que si l'on veut être sûr de ne pas avoir de quiproquo. Donc c'est souvent très important!

124. Cours

125. Cours : c'est l'isomorphisme de $\mathscr{L}(E,F)\to\mathscr{M}_{p,n}(\mathbb{K})$ étant données une base pour E et une pour F.

126. Elles sont équivalentes, voire semblable si $E=F$ et qu'on considère les mêmes bases.

Chapitre 26

Structures affines

Résumé -

Un espace affine est un espace vectoriel translaté (ou encore avec une origine ailleurs qu'en 0). Une autre façon de penser le lien espace vectoriel/espace affine consiste à faire un faire un parallèle avec le lien base $\mathscr{B} = (\vec{i}, \vec{j}, \vec{k})$ (d'un espace vectoriel) / repère $\mathscr{R} = (O, \vec{i}, \vec{j}, \vec{k})$ (d'un espace affine).

Après avoir vu quelques généralités sur les espaces affines, nous nous concentrons sur les deux exemples typiques de notre programme :

- *L'ensemble des solutions d'un système d'équation linéaire non homogène. (Nous pouvons également penser aux solutions d'une équation différentielles linéaire avec second membre…)*
- *L'espace affine géométrique $\mathbb{R}^2$ ou $\mathbb{R}^3$…*

Sommaire

1. Problèmes 530
2. Introduction 531
3. Translatés d'un sous-espace vectoriel 531
3.1. Translation (linéaire) 531
3.2. (Sous-)Espaces affines 531
3.3. Exemples variées 533
4. Systèmes d'équations linéaires 534
4.1. Contextes 534
4.2. Interprétations 535
4.3. Structure de l'ensemble des solutions 536
5. Equations, intersections et parallélisme 536
5.1. Cas général 536
5.2. Dans un plan (espace de dimension 2) 538
5.3. Dans un espace de dimension 3 538
6. Bilan 540

1. Problèmes

Problème 111 - Droite linéaire vs. droite affine

La géométrie (classique) permet de voir les espaces vectoriels.
Une droite linéaire $\{(x, y) \in \mathbb{R}^2 \mid y = ax\}$ est un sous-espace vectoriel de dimension 1 de $\mathbb{R}^2$.
En géométrie classique, il y a aussi dans l'espace $\mathbb{R}^2$ des sous-ensembles non sev, appelés droites affine : $\{(x, y) \in \mathbb{R}^2 \mid y = ax + b\}$. Elle est "parallèle" à la droite précédente, mais décalée (translatée) de b (ordonnée à l'origine).
Comment peut-on, de la même façon, découper un espace vectoriel en mille-feuille : l'une est vectoriel, les autres affines et parallèles?

Problème 112 - Structure affine de l'ensemble des solutions d'un problème linéaire

A tous les problèmes linéaires nous pouvons associer une structure d'espace vectoriel.
L'ensemble des inconnues est l'espace vectoriel et le problème code une application linéaire.
Lorsqu'il s'agit de trouver les racines du problèmes (solutions lorsque le second membre est nul), on se trouve en présence d'un noyau d'applications linéaires.
Exemple : trouver (u_n) telle que $\forall\, n \in \mathbb{N}$, $u_{n+3} - u_{n+1} + u_n = 0$.
L'espace est $E = \mathbb{K}^{\mathbb{N}}$, l'application linéaire est $\Phi : (u_n) \mapsto (v_n)$ avec $\forall\, n \in \mathbb{N}$, $v_n = u_{n+3} - u_{n+1} + u_n$. Il s'agit de trouver $\mathrm{Ker}\,\Phi$.
Mais si le second membre est non nul, quelle est la structure de l'ensemble des solutions?
Exemple : trouver (u_n) telle que $\forall\, n \in \mathbb{N}$, $u_{n+3} - u_{n+1} + u_n = n + 2$.

Problème 113 - Réciproquement

Si la géométrie permet de mieux voir les espaces et définir les espaces affines, on peut espérer que les structures algébriques permettent réciproquement de mieux comprendre la géométrie.
Que peut-on dire de l'intersection de trois hyperplans affines dans l'espace? Est-il possible de coder ce problème sous forme de système à résoudre? De quelle façon, le rang du système nous informe sur l'ensemble intersecté?

Problème 114 - Espaces quotients et supplémentaires

On note pour F sev de E et $a \in E$, $\mathscr{F}$ l'espace affine $a + F$.
Ainsi $b \in \mathscr{F} \iff \exists\, f \in F$ tel que $b = a + f \iff b - a \in F$.
On définit ainsi une relation d'équivalence : $a \mathscr{R}_F b$.
Que peut-on dire de l'espace affine $\mathscr{F}$ en terme de classe d'équivalence de a pour $\mathscr{R}_F$?
Si H est supplémentaire de F dans E, on a H est un système de représentants de classes pour $\mathscr{R}_F$.

Réciproquement, peut-on exploiter cette relation, pour créer un espace vectoriel $\mathscr{F}$, « supplémentaire » (d'une certaine façon) à F dans E?

2. Introduction

Soit E un $\mathbb{K}$-espace vectoriel ($\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$).

Heuristique - Addition (et soustraction) affine

Si $A,B\in E$, on note $\overrightarrow{AB}=B-A\in\vec{E}$. On a alors

$$\overrightarrow{AB}=\vec{0}\Leftrightarrow A=B$$
$$B=A+\vec{u}\Leftrightarrow\vec{u}=\overrightarrow{AB}$$
$$\overrightarrow{BA}=-\overrightarrow{AB}$$
$$\overrightarrow{AB}+\overrightarrow{BC}=\overrightarrow{AC}$$

Heuristique - Repère affine

On appelle alors *repère affine* de E tout couple $(\Omega,\mathscr{B})$ d'un point Ω de E (l'*origine* du repère) et d'une base $\mathscr{B}$ de $\vec{E}$. Si $\mathscr{B}=(\vec{e_1},\dots,\vec{e_n})$ alors tout point X de E s'écrit de manière unique sous la forme $X=\Omega+\sum_{i=1}^{n}x_i\vec{e_i}$; on dit que les x_i sont les coordonnées du point X dans le repère affine, ce sont également les coordonnées du vecteur $\overrightarrow{\Omega X}$ dans la base $\mathscr{B}$. (Le choix d'une origine permet "d'identifier " E et $\vec{E}$.)

Pour aller plus loin - Principe et notation

On va s'intéresser à la structure affine de E, c'est-à-dire que les éléments de E vont être repérés par rapport à une origine et considérés comme des "points" (on les notera de préférence en majuscule dans ce cas). Les éléments de E "espace vectoriel", seront noté de préférence en minuscule avec une flèche, et on peut, pour faire la différence, noter $\vec{E}$ l'ensemble E quand il est considéré comme espace vectoriel. D'autre fois, E est l'espace vectoriel considéré et $\mathscr{E}$ un espace affine associé…

3. Translatés d'un sous-espace vectoriel

3.1. Translation (linéaire)

Soit $(E,+,\cdot)$ un K-e.v.

Définition - Translation

Soit $a\in E$. On appelle translation de vecteur a l'application

$$t_a:\ \begin{array}{l}E\to E\\ x\mapsto x+a\end{array}$$

Proposition - Le groupe des translations $\mathscr{T}(E)$

On note $\mathscr{T}(E)$ l'ensemble des translations de E. Alors $(\mathscr{T}(E),\circ)$ est un groupe commutatif.
En particulier
- Id_E est la translation de vecteur nul.
- $t_a\circ t_b=t_b\circ t_a=t_{a+b}$.
- t_a est bijective de bijection réciproque t_{-a}

Démonstration

Pour tout $x\in E$,

$$(t_a\circ t_b)(x)=t_a(t_b(x))=t_a(x+b)=(x+b)+a=x+(a+b)=t_{a+b}(x)=(t_b\circ t_a)(x)$$

En fait, on crée ainsi un morphisme bijectif de groupes : $\varphi:(E,+)\to(\mathscr{T}(E),+)\dots$ □

On notera bien, pour ce qui suit, que nous ne définissons jamais (ici) un espace affine, mais seulement des sous-espaces affines (à partir d'un espace vectoriel).

3.2. (Sous-)Espaces affines

Définition - Sous-espace affine (d'un espace vectoriel)

Soit $\mathscr{F}\subset E$, autrement écrit : $\mathscr{F}$ une partie de E.
On dit que $\mathscr{F}$ est un sous-espace affine de E s'il existe $a\in E$ et F sous-espace vectoriel de E tels que

$$\mathscr{F}=t_a(F)=\{a+f\,;\,f\in F\}$$

On note alors $\mathscr{F}=a+F$ et on dit que le s.e.v F est la direction du s.e.a. $\mathscr{F}$.

Remarque - Eléments de $\mathscr{F}$

D'après la définition, les éléments de $\mathscr{F}$ sont des éléments de E donc des vecteurs! Et pourtant la « tradition » veut qu'on appelle ces éléments des points. On les notera souvent avec une lettre majuscule.

Remarque - Autre notation

Si on note un s.e.a. F, on notera sa direction $\vec{F}$.

Remarque - Unicité de $\mathscr{F}$

La définition parle de LA direction F. Faut-il comprendre qu'il est unique?

Démonstration

Supposons $\mathscr{F}=a+F=a'+F'$.
alors comme $0\in F, 0\in F'$, alors a et $a'\in\mathscr{F}$.
Et donc il existe $b\in F$ tel que $a'=a+b$ et donc $a'-a\in F$.
Par symétrie : $a-a'\in F'$, puis, comme ce sont des espaces vectoriels : $a-a'\in F\cap F'$.
Ensuite, pour tout $x\in F$, $a+x\in\mathscr{F}=a'+\underbrace{y}_{\in F'}$, donc $x=a'+y-a\in F'$ et $F\subset F'$.
Par symétrie, on a l'inclusion réciproque : $F'\subset F$.
Donc $F=F'$ □

Définition - Sea particuliers

Soit $\mathscr{F}$ un sous-espace affine de E de direction F. On dit que $\mathscr{F}$ est
- un point (ou un singleton réduit à un point) si $F=\{0_E\}$,
- une droite affine si F est une droite vectorielle,
- un plan affine si F est un plan vectoriel,
- un hyperlan affine si F est un hyperplan vectoriel.

Application - Représentation graphique dans $\mathbb{R}^2$ ou dans $\mathbb{R}^3$

Le plan étant muni d'une origine O, on peut identifier le vecteur nul $\vec{0}$ avec O et un vecteur $\vec{u}=\overrightarrow{OM}$ avec son extrémité M. Une droite vectorielle est alors une droite passant par O et une droite affine (translaté d'une droite vectorielle) une droite quelconque.

Exemple - Cas particuliers

- les s.e.a de $\mathbb{R}^2$ sont

- les s.e.a de $\mathbb{R}^3$ sont

- $\{y\in\mathscr{F}(\mathbb{R},\mathbb{R})\,|\,y''+y'-2y=e^{3x}\}$ est un s.e.a de $\mathscr{F}(\mathbb{R},\mathbb{R})$ de direction

Proposition - Expression d'un s.e.a.

Si $\mathscr{F}$ est un s.e.a de E de direction F,
alors pour tout $a\in\mathscr{F}$ on a $\mathscr{F}=a+F$.

Démonstration

$\mathscr{F}$ a pour direction F. Il existe $u\in E$ tel que $\mathscr{F}=u+F$.
Soit $a\in F$, alors il existe $\vec{a}_0\in F$ tel que $a=u+\vec{a}_0$

$$\forall\, x\in\mathscr{F},\exists\,\vec{x}_0\in F\text{ tel que }x=u+\vec{x}_0$$

$$\forall\, x\in\mathscr{F},\exists\,\vec{x}_0\in F\text{ tel que }x=(a-\vec{a}_0)+\vec{x}_0=a+(\vec{x}_0-\vec{a}_0)$$

Donc, comme $(F,+)$ est un groupe et donc $\vec{x}_0\in F\Leftrightarrow(\vec{x}_0-\vec{a}_0)\in F$, on peut affirmer que $\mathscr{F}=a+F$, pour tout $a\in\mathscr{F}$ □

3.3. Exemples variées

Les résultats suivant sont déjà connus, mais il s'interprète de manière tout à fait naturel dans le langage des espaces affines.

Equation simple

Théorème - Résolution d'une équation linéaire $u(x)=b$
Soient $u\in\mathscr{L}(E,F)$ et $b\in F$. On note $S_{\mathscr{E}}$ l'ensemble des solutions de l'équation $(\mathscr{E}):u(x)=b$.
- Si $b\notin \text{Im } u$ alors $S_{\mathscr{E}}=\emptyset$.
- Si $b\in \text{Im } u$ alors $S_{\mathscr{E}}\neq\emptyset$ et si x_0 est une solution particulière de $(\mathscr{E})$ alors
$$S_{\mathscr{E}}=\{x_0+y;\ y\in \text{Ker } u\}.$$
$S_{\mathscr{E}}$ est un sous-espace affine de E de direction Ker u.

Equations différentielles

Pour l'exercice suivant on donnera une base à l'espace directeur (ce qui donne aussi la valeur de la dimension de l'espace affine des solutions).
Exercice
• Exprimer l'ensemble des solutions de l'équation
$$y'+\cos x\times y=1+\tan^2 x+\sin x$$
• Exprimer l'ensemble des solutions de l'équation
$$-3y''+4y'-y=\sin x$$

Correction
• On cherche l'espace vectoriel des solutions de l'équation homogène :
$$\mathscr{S}=\{t\mapsto A\exp(-\int^t \cos x\mathrm{d}x),A\in\mathbb{R}\}=\{t\mapsto A\exp(-\sin(t)),A\in\mathbb{R}\}$$
Une solution particulière est $x\mapsto\tan x$.
$\mathscr{S}=\{x\mapsto\tan x\}+\text{vect}(x\mapsto\exp(-\sin x))$.
• L'équation caractéristique associée est $3x^2-4x+1=3(x-1)(x-\frac{1}{3})$.
L'espace vectoriel des solutions de l'équations homogène a pour base : $f_1:x\mapsto e^x$ et $f_2:x\mapsto e^{\frac{1}{3}x}$.
Une solution particulière est de la forme :$g:x\mapsto A\sin x+B\cos x$. Alors
$$\sin x=-3g''(x)+4g'(x)-g(x)=(3A-4B-A)\sin x+(3B+4A-B)\cos x$$
Donc $2A-4B=1$ et $2B+4A=0$, donc $A=\frac{1}{10}$ et $B=\frac{-2}{10}$.
$\mathscr{S}=\{x\mapsto\frac{1}{10}(\sin x-2\cos x)\}+\text{vect}(f_1,f_2)$.

Pour aller plus loin - Linéaire+second membre
Tout les problèmes linéaires avec second membre se resolvent de la même façon :
- *on cherche une solution particulière (point de translation)*
- *on cherche l'espace vectoriel des solutions du problème (linéaire) homogène.*

La somme forme l'espace affine des solutions recherchées

Partout...

Exercice
Trouver les suites (u_n) vérifiant :
$$\forall\ n\in\mathbb{N},\qquad u_{n+2}+u_{n+1}-6u_n=2$$

Correction
Si (a_n) est une solution particulière, alors ,
$$(u_n)\text{ est solution de }E\Leftrightarrow(u_n-a_n)\text{ est solution de }E_0$$
On reconnait une addition de deux problèmes : le problème homogène et une solution particulière.
Cherchons UNE solution particulière (a_n) de la forme $\forall\ n\in\mathbb{N},\ a_n=\lambda n+\mu$.
Alors $a_{n+2}+a_{n+1}-6a_n=-4n\lambda+(3\lambda-4\mu)$.
Donc avec $\lambda=0$ et $\mu=-\frac{1}{2}$, on a une solution particulière $(a_n)=(-\frac{1}{2})$.
Puis on étudie $K=\{(u_n)\mid u_{n+2}+u_{n+1}-6u_n=0\}$.

On trouve que $u_n\in K$ ssi $\exists\ A,B\in\mathbb{K}$ tel que $u_n=A2^n+B(-3)^n$.
Donc
$$\{(u_n)\mid\forall\ n\in\mathbb{N},u_{n+2}+u_{n+1}-6u_n=2\}=\{A2^n+B(-3)^n-\frac{1}{2},A,B\in\mathbb{K}\}=\{\frac{1}{2}\}+\text{vect}\big((2^n)_n,((-3)^n)_n\big)$$

Exercice
Trouver l'ensemble des polynômes tels que $P(1)=1$, $P(2)=2$, $P(3)=3$ et $P(4)=5$.
Problème d'interpolation de Lagrange.

Correction
Le problème homogène (ce qui donne l'espace directeur) consiste à trouver T tel $T(1)=T(2)=T(3)=T(4)=0$.
On a donc $T=Q\times(X-1)(X-2)(X-3)(X-4)$.
Pour trouver une solution particulière, on applique le principe de superposition : $P_1(1)=1$, $P_1(2)=P_1(3)=P_1(4)=0$; donc $P_1=\lambda(X-2)(X-3)(X-4)$, avec $\lambda=\frac{-1}{6}$.
$P_2(2)=2$, $P_2(1)=P_1(3)=P_1(4)=0$; donc $P_2=\mu(X-1)(X-3)(X-4)$, avec $\mu=1$.
$P_3(3)=3$, $P_3(1)=P_3(2)=P_3(4)=0$; donc $P_3=\nu(X-1)(X-2)(X-4)$, avec $\nu=\frac{-3}{2}$.
$P_4(4)=5$, $P_4(1)=P_4(2)=P_4(3)=0$; donc $P_4=\theta(X-1)(X-2)(X-3)$, avec $\theta=\frac{5}{6}$.
Pour la solution particulière, on aurait également pu prendre $X+Q$ avec $Q(1)=Q(2)=Q(3)=0$ et $Q(4)=1$.
Donc $\mathscr{S}=\{X+\frac{1}{6}(X-1)(X-2)(X-3)\}+(X-1)(X-2)(X-3)(X-4)\mathbb{K}[X]$.

Exercice
Trouver l'ensemble des nombres N tels que $N\equiv 1[3]$, $N\equiv 2[5]$, $N\equiv 4[7]$ et $N\equiv 1[11]$.
Problème des restes chinois.

Correction
Le problème homogène (ce qui donne l'espace directeur) consiste à trouver M tel $M\equiv 0[3]$, $M\equiv 0[5]$, $M\equiv 0[7]$, $M\equiv 0[11]$ Ces quatre équations sont, ensemble, équivalentes à $M\equiv 0[1155]$ car ces 4 nombres sont premiers.
Pour trouver une solution particulière, on applique le principe de superposition : $N_1\equiv 0[385]$ et $N_1\equiv 1[3]$. Par exemple $N_1=385$.
$N_2\equiv 0[231]$ et $N_2\equiv 2[5]$. Par exemple $N_2=462$.
$N_3\equiv 0[165]$ et $N_3\equiv 4[7]$. Par exemple $N_3=165$.
$N_4\equiv 0[105]$ et $N_4\equiv 1[11]$. Par exemple $N_4=210$.
Donc $\mathscr{S}=\{1222+k1155,k\in\mathbb{Z}\}$.

4. Systèmes d'équations linéaires

4.1. Contextes

Pour aller plus loin - Module affine
Sur ce dernier exercice, il ne s'agit pas a proprement parlé d'espace affine et espace vectoriel mais de module, car l'ensemble est défini (pour la loi externe) sur l'anneau $\mathbb{Z}$ et non un corps $\mathbb{K}$. On parle alors de module

En forme de rappels :

Définition - Vocabulaire
On considère le système de n équations à p inconnues :
$$(S)\begin{cases}a_{11}x_1+a_{12}x_2+\cdots+a_{1p}x_p=b_1\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2p}x_p=b_2\\ \vdots\\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{np}x_p=b_n\end{cases}$$
La matrice $A=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1p}\\ a_{21}&a_{22}&\cdots&a_{2p}\\ \vdots&\vdots&&\vdots\\ a_{n1}&a_{n2}&\cdots&a_{np}\end{pmatrix}\in\mathscr{M}_{n,p}(K)$ s'appelle la matrice du système, $B=\begin{pmatrix}b_1\\ b_2\\ \vdots\\ b_n\end{pmatrix}\in\mathscr{M}_{n,1}(K)$ est la matrice colonne des coordonnées du second membre $b=(b_1,b_2,\dots,b_n)\in K^n$.

On appelle système homogène associé à (S) le système

$$(S_H)\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1p}x_p=0 \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2p}x_p=0 \\ \vdots \\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{np}x_p=0 \end{cases}$$

Définition - Compatibilité du système
Le système est dit compatible si l'ensemble des solutions est non vide.

Remarque - Rang du système
On appelle rang du système (S) le rang de la matrice A.

4.2. Interprétations

Les résultats et propositions qui suivent découlent du cours précédent, ce qui change est leur interprétation (en fait, « le point de vue s'élargit »). Cela ne mérite donc, de manière générale, aucune démonstration.

Proposition - Interprétation linéaire
Soit $u \in \mathscr{L}(\mathbb{K}^p,\mathbb{K}^n)$ définie par

$$u:\ \begin{array}{ccc}\mathbb{K}^p & \to & \mathbb{K}^n \\ \begin{pmatrix}x_1\\ \vdots \\ x_p\end{pmatrix} & \mapsto & \begin{pmatrix}a_{11}x_1+a_{12}x_2+\cdots+a_{1p}x_p \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2p}x_p \\ \vdots \\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{np}x_p\end{pmatrix}\end{array}$$

et $b=(b_1,b_2,\dots,b_n)$. Alors

$$(x_1,\dots,x_p)\in\mathbb{K}^p \text{ est solution de } (S) \Leftrightarrow u(x)=b$$

Le système est compatible si et seulement si $b\in\mathfrak{I}u$.

Proposition - Rang du système
Le rang du système (S) est égal au rang de u : $\operatorname{rg}(S)=\operatorname{rg}(A)=\operatorname{rg}(u)$.

Proposition - Interprétation duale
Considérons les n formes linéaires φ_i sur $\mathbb{K}^p$ définies par

$$\varphi_i:\ \begin{array}{ccc}\mathbb{K}^p & \to & \mathbb{K} \\ (x_1,\dots,x_p) & \mapsto & a_{i1}x_1+a_{i2}x_2+\cdots+a_{ip}x_p\end{array}$$

Alors

$$(x_1,\dots,x_p)\in\mathbb{K}^p \text{ est solution de } (S) \Leftrightarrow \forall i\in\{1,\dots,n\},\ \varphi_i(x)=b_i$$

L'ensemble des solutions du système homogène est alors $\operatorname{Ker}\varphi_1\cap\ldots\cap\operatorname{Ker}\varphi_n$.

4.3. Structure de l'ensemble des solutions

On note $\mathbb{S}_0$ l'ensemble des solutions du système homogène associé et $\mathbb{S}$ l'ensemble des solutions du système (S).

Théorème - Dimension de l'espace vectoriel $\mathbb{S}_0$
$\mathbb{S}_0$ est un $\mathbb{K}$-espace vectoriel de dimension $p-\operatorname{rg}(S)$.

Théorème - Résolution de système. Interprétation affine.
Si (S) est compatible, alors il existe une solution particulière x_0.
Dans ce cas,

$$\mathbb{S}=\{x_0+y;\ y\in\mathbb{S}_0\}$$

et $\mathbb{S}$ est un espace affine de dimension $p-\operatorname{rg}(S)$.
Un tel système a $\operatorname{rg}(S)$ inconnues principales et $p-\operatorname{rg}(S)$ inconnues secondaires.

Exercice
Résoudre le système

$$\begin{cases} 2x_1 & -2x_2 & +x_3 & -5x_4 & +3x_5 & = & 8 \\ & 2x_2 & -4x_3 & -9x_4 & +7x_5 & = & 6 \\ -6x_1 & +7x_2 & -6x_3 & +11x_4 & -7x_5 & = & -23 \\ 2x_1 & -5x_2 & +14x_3 & +5x_4 & +3x_5 & = & 13 \end{cases}$$

Correction
On applique $L_3\leftarrow L_3+3L_1$ et $L_4\leftarrow L_4-L_1$.
On a le système équivalent :

$$\begin{cases} 2x_1 & -2x_2 & +x_3 & -5x_4 & +3x_5 & = & 8 \\ & 2x_2 & -4x_3 & -9x_4 & +7x_5 & = & 6 \\ & x_2 & -3x_3 & -4x_4 & +2x_5 & = & 1 \\ & -3x_2 & +13x_3 & +10x_4 & & = & 5 \end{cases} \Leftrightarrow \begin{cases} 2x_1 & -2x_2 & +x_3 & -5x_4 & +3x_5 & = & 8 \\ & x_2 & -3x_3 & -4x_4 & +2x_5 & = & 1 \\ & 2x_2 & -4x_3 & -9x_4 & +7x_5 & = & 6 \\ & -3x_2 & +13x_3 & +10x_4 & & = & 5 \end{cases}$$

Puis, on fait $L_3\leftarrow L_3-2L_2$ et $L_4\leftarrow L_4+3L_2$
On a le système équivalent :

$$\begin{cases} 2x_1 & -2x_2 & +x_3 & -5x_4 & +3x_5 & = & 8 \\ & x_2 & -3x_3 & -4x_4 & +2x_5 & = & 1 \\ & & 2x_3 & -x_4 & +3x_5 & = & 4 \\ & & 4x_3 & -2x_4 & +6x_5 & = & 8 \end{cases} \Leftrightarrow \begin{cases} 2x_1 & -2x_2 & +x_3 & -5x_4 & +3x_5 & = & 8 \\ & x_2 & -3x_3 & -4x_4 & +2x_5 & = & 1 \\ & & 2x_3 & -x_4 & +3x_5 & = & 4 \end{cases}$$

en faisant $L_4\leftarrow L_4-2L_3$.
Ce qui nous donne le système équivalent :

$$\begin{cases} 2x_1 & -2x_2 & +x_3 & = & 8 & +5x_4 & -3x_5 \\ & x_2 & -3x_3 & = & 1 & +4x_4 & -2x_5 \\ & & 2x_3 & = & 4 & +x_4 & -3x_5 \end{cases} \Leftrightarrow \begin{cases} 2x_1 & -2x_2 & +x_3 & = & 8 & +5x_4 & -3x_5 \\ & x_2 & -3x_3 & = & 1 & +4x_4 & -2x_5 \\ & & x_3 & = & 2 & +\frac{1}{2}x_4 & -\frac{3}{2}x_5 \end{cases}$$

En faisant : $L_1\leftarrow L_1-L_3$ et $L_2\leftarrow L_2+3L_3$, on a le système équivalent

$$\begin{cases} 2x_1 & -2x_2 & = & 6 & +\frac{9}{2}x_4 & -\frac{3}{2}x_5 \\ & x_2 & = & 7 & +\frac{11}{2}x_4 & -\frac{13}{2}x_5 \\ & x_3 & = & 2 & +\frac{1}{2}x_4 & -\frac{3}{2}x_5 \end{cases} \Leftrightarrow \begin{cases} 2x_1 & = & 20 & +\frac{31}{2}x_4 & -\frac{29}{2}x_5 \\ x_2 & = & 7 & +\frac{11}{2}x_4 & -\frac{13}{2}x_5 \\ x_3 & = & 2 & +\frac{1}{2}x_4 & -\frac{3}{2}x_5 \end{cases}$$

Donc $\mathbb{S}=(10,7,2,0,0)+\operatorname{vect}\big((31,22,2,4,0);(-29,-26,-6,0,4)\big)$

5. Equations, intersections et parallélisme

5.1. Cas général

Proposition - Intersection de sous-espaces affines
Soient $\mathscr{F}$ et $\mathscr{G}$ deux sous-espaces affines de directions respectives F et G.
Si $\mathscr{F}\cap\mathscr{G}\neq\emptyset$ alors $\mathscr{F}\cap\mathscr{G}$ est un sea de direction le s.e.v $F\cap G$.

Démonstration
Soit $a \in \mathscr{F} \cap \mathscr{G}$.
On a les équivalences :

$$x \in \mathscr{F} \cap \mathscr{G} \iff \begin{cases} x-a \in F & \text{car } x, a \in \mathscr{F} \\ x-a \in G & \text{car } x, a \in \mathscr{G} \end{cases} \iff x-a \in F \cap G$$

Donc, par équivalence (donc double inclusion) : $\mathscr{F} \cap \mathscr{G}$ est un sous-espace affine de direction le s.e.v $F \cap G$ □

Si $F \cap G = \{0\}$, i.e. $F \oplus G$:

Corollaire - Espaces supplémentaires
Soient $\mathscr{F}$ et $\mathscr{G}$ deux sous-espaces affines de directions respectives F et G vérifiant $F \oplus G = E$. Alors $\mathscr{F} \cap \mathscr{G}$ est un singleton.

Remarque - Hypothèse superflue?
Il faudrait également montrer que $\mathscr{F} \cap \mathscr{G} \neq \emptyset$.
Mais Le fait que la somme $F+G$ donne E implique que $\mathscr{F} \cap \mathscr{G} \neq \emptyset$, d'après un des exercices du chapitre (n°495) …

Définition - Sous-espaces affines parallèles
On dit que le sous-espace affine $\mathscr{F}$ est parallèle au sous-espace affine $\mathscr{G}$ si $F \subset G$.
On dit que que deux sous espaces affines $\mathscr{F}$ et $\mathscr{G}$ sont parallèles si $F = G$.

Attention - Relation d'équivalence. Relation d'ordre
Etre parallèle n'est donc pas une relation d'équivalence (non symétrique).
Mais il s'agit d'une pseudo-relation d'ordre (légère difficulté : on parle des espaces affines, et on a une égalité sur les espaces vectoriels, dans le cas de l'antisymétrie).
Par ailleurs, la relation n'est clairement pas totale

Proposition - Equation d'un hyperplan affine
Soit $\mathscr{R} = (\Omega, e_1, \dots, e_n)$ un repère affine de l'espace E de dimension n. Alors
- Un hyperlpan affine $\mathscr{H}$ de E possède au moins une équation dans $\mathscr{R}$ du type :
$$\sum_{i=1}^{n} a_i x_i = h \text{ avec } (a_1, \dots, a_n) \neq (0, \dots, 0). \quad (*)$$
- Réciproquement la relation $(*)$ est l'équation d'un hyperlpan affine dont la direction admet pour équation cartésienne
$$\sum_{i=1}^{n} a_i x_i = 0.$$
- Deux équations de la forme $(*)$ représentent le même hyperplan affine si et seulement si elles sont proportionnelles.

Démonstration
On exploite le théorème sur les formes linéaires, colinéaires si et seulement si elles ont le même noyau □

5.2. Dans un plan (espace de dimension 2)

On retrouve les résultats du plan usuel, qui sont généralisable à tout espace (affine) de dimension 2 (comme par exemple, l'espace des suites récurrentes linéaires d'ordre 2)

Théorème - Equation de droites
Soit $(\Omega, \vec{e_1}, \vec{e_2})$ un repère du plan. Alors
- Toute droite possède une équation cartésienne de la forme $ax+by+c=0$ où $a, b, c \in \mathbb{R}$, $(a,b) \neq (0,0)$, $\vec{u}(-b,a)$ en est un vecteur directeur.
- Réciproquement, toute équation cartésienne de ce type décrit une droite.
- Deux telles équations représentent la même droite si et seulement si elles sont proportionnelles.

Définition - Equation paramétrique
Soit $(\Omega, \vec{e_1}, \vec{e_2})$ un repère du plan. Alors une droite possède des équations paramétriques (ou une représentation paramétrique) de la forme

$$\begin{cases} x = x_0 + tu_1 \\ y = y_0 + tu_2 \end{cases} \quad t \in \mathbb{R}$$

Il s'agit alors de la droite passant par $M_0(x_0, y_0)$ et de vecteur directeur $\vec{u}(u_1, u_2)$.

Démonstration
Dans ce cas, l'espace affine en question est de la forme $x_0 + \vec{F}$, avec $\vec{F}$, un espace vectoriel de dimension 1.
Donc $\vec{F} = \text{vect}(\vec{u})$ □

Proposition - Droites parallèles
Deux droites affines du plan sont parallèles si elles ont même direction et, si elle ne sont pas parallèles, leur intersection est réduite à un point.

5.3. Dans un espace de dimension 3

Comme précédemment, dans le cas où l'espace vectoriel directeur est de dimension 1 (droite dans l'espace) :

Définition - Représentation paramétrique d'une droite
Soit $(\Omega, \vec{e_1}, \vec{e_2}, \vec{e_3})$ un repère quelconque de l'espace. Alors une droite possède des équations paramétriques (ou une représentation paramétrique) de la forme

$$\begin{cases} x = x_0 + tu_1 \\ y = y_0 + tu_2 \\ z = z_0 + tu_3 \end{cases} \quad t \in \mathbb{R}$$

Il s'agit alors de la droite passant par $M_0(x_0, y_0, z_0)$ et de vecteur directeur $\vec{u}(u_1, u_2, u_3)$.

Comme précédemment, dans le cas où l'espace vectoriel directeur est de dimension 2 (plan dans l'espace) :

Définition - Représentation paramétrique d'un plan
Soit $(\Omega, \vec{e}_1, \vec{e}_2, \vec{e}_3)$ un repère quelconque de l'espace. Alors un plan possède des équations paramétriques (ou une représentation paramétrique) de la forme

$$\begin{cases} x = x_0 + tu_1 + sv_1 \\ y = y_0 + tu_2 + sv_2 \\ z = z_0 + tu_3 + sv_3 \end{cases} \quad (t,s) \in \mathbb{R}^2$$

Il s'agit alors du plan passant par $M_0(x_0, y_0, z_0)$ et de vecteurs directeurs $\vec{u}(u_1, u_2, u_3)$ et $\vec{v}(v_1, v_2, v_3)$ (Attention : $\vec{u}$ et $\vec{v}$ doivent être linéairement indépendants, sinon il s'agit d'une droite).

Théorème - Equation cartésienne d'un plan
Soit $(\Omega, \vec{e}_1, \vec{e}_2, \vec{e}_3)$ un repère de l'espace. Alors
- Tout plan possède une équation cartésienne de la forme $ax + by + cz + d = 0$ où $a, b, c \in \mathbb{R}$, $(a,b,c) \neq (0,0,0)$.
- Réciproquement, toute équation cartésienne de ce type décrit un plan.

Démonstration
L'idée est de noter $ax + by + cz + d = 0$ sous la forme $ax + by + cz = -d$....
On note $\varphi : \vec{E} \to \mathbb{K}$, $(x,y,z) \mapsto ax + by + cz$.
Puis le plan est de la forme $M_0 + \text{Ker}\varphi$, avec M_0 de coordonnées (x_0, y_0, z_0) vérifiant : $ax_0 + by_0 + cz_0 = -d$.
On a alors $\mathscr{P} = \{M(x,y,z) \mid M\vec{M}_0 \in \text{Ker}\varphi\} = \{M(x,y,z) \mid ax + by + cz + d = 0\}$ □

Proposition - Equations cartésiennes d'une droite
Soient deux plans d'équations respectives
$ax + by + cz + d = 0$ et $a'x + b'y + c'z + d' = 0$. Alors
- Si (a,b,c) et (a',b',c') sont proportionnels, alors $\mathscr{P}$ et $\mathscr{P}'$ sont parallèles (i.e. ont le même plan vectoriel comme direction, ou les mêmes vecteurs directeurs).
  De plus si (a,b,c,d) et (a',b',c',d') sont proportionnels alors $\mathscr{P} = \mathscr{P}'$, sinon $\mathscr{P} \cap \mathscr{P}' = \emptyset$.
- Si (a,b,c) et (a',b',c') ne sont pas proportionnels, alors $\Delta = \mathscr{P} \cap \mathscr{P}'$ est une droite.
  $\begin{cases} ax + by + cz + d = 0 \\ a'x + b'y + c'z + d' = 0 \end{cases}$ s'appelle un système d'équations cartésiennes de Δ.

Attention - Parallélisme et intersection
Dans l'espace de dimension 3,
- deux droites sont parallèles si elles ont des vecteurs directeurs colinéaires,
- deux plans sont parallèles s'ils ont le même plan vectoriel pour direction,
- une droite peut être parallèle a un plan si son vecteur directeur appartient à la direction du plan,
- mais il est incorrect de dire qu'un plan est parallèle à une droite,
- l'intersection d'une droite $\mathscr{D}$ non parallèle à un plan $\mathscr{P}$, et du plan $\mathscr{P}$ est un point.

6. Bilan

Synthèse

⇝ Les structures affines sont des milles-feuilles d'espaces vectoriels qui ne contiennent pas nécessairement le vecteur nul. Cela permet d'offrir une liberté aux mathématiciens.

⇝ Cela s'applique dans de nombreux domaines : nous nous concentrons ici uniquement sur les systèmes d'équations linéaires et sur la géométrie de dimension 2 ou 3.

Savoir-faire et Truc & Astuce du chapitre

Notations

Notations	*Définitions*	*Propriétés*	*Remarq*
$\mathscr{F}$	Espace affine, défini par un sous-espace F et a un « point » quelconque de F	$\mathscr{F} = a + F$	

Retour sur les problèmes

127. Cours

128. La suite u définie par $\forall\ n \in \mathbb{N}$, $u_n = An + B$.
$u_{n+3} - u_{n+1} + u_n = A(n+3-n-1+n) + B(1-1+1) = An + (B+2A)$.
Donc avec $A = 1$ et $B = 0$, on a une solution particulière.
On note $a, b, \overline{b}$ les trois racines (complexes) de l'équation caractéristique associée.
L'espace vectoriel des solutions de l'équation homogène est $E = \text{vect}((a^n), (b^n), (\overline{b}^n))$
L'ensemble des solutions du problème est donc l'espace affine : $u + E$.

129. Le rang du système nous donne la codimension de l'espace vectoriel qui dirige l'espace affine en question : 2 ou 1 voir 0. (En fait ce qui compte, c'est la dimension du noyau).
Il faut également trouver un point d'intersection comme origine de l'espace affine solution.

130. $\mathscr{F} = \overline{a}_{\mathscr{R}_F}$.
L'étude sur H, en découle.

Chapitre 27

Espaces vectoriels euclidiens

Résumé -

Dans les situations physiques, les espaces considérés (vectoriels ou affine) sont en règle générale munie d'un produit scalaire. On peut donc faire l'étude de ces espaces que l'on appelle préhilbertien. Mais la motivation mathématique aurait été déjà suffisante : un produit scalaire bien choisi c'est une étude renforcée de la dualité ($E^* = \mathcal{L}(E,\mathbb{K})$), ou encore l'étude des coordonnées sur une base...

Nous commençons par étudier la notion abstraite (théorique) des produits scalaires. Nous enchainons avec la notion importante d'orthogonalité (qui précise d'une certaine façon la question d'espace supplémentaire). Comme pour l'algèbre linéaire, nous nous concentrons ensuite sur le espaces de dimension finies, avant d'étudier une famille d'applications linéaires particulières : les projections orthogonales (et symétries orthogonales). Dans le chapitre suivant, nous élargirons cette étude aux isométries vectorielles et affines.

Sommaire

1. Problèmes 542
2. Définitions et règles de calcul 543
2.1. Produit scalaire 543
2.2. Norme euclidienne 544
2.3. Différentes identités 547
3. Orthogonalité 548
3.1. Vecteurs orthogonaux 548
3.2. Sous-espaces orthogonaux 549
3.3. Familles orthogonales, orthonormales 550
4. Cas de la dimension finie : espaces euclidiens 553
4.1. Définition 553
4.2. Bases orthonormales 554
5. Projections orthogonales 556
5.1. Supplémentaire orthogonal 556
5.2. Projections orthogonales 557
5.3. Distance à un sous-ensemble d'une espace préhilbertien 558
5.4. Symétries orthogonales 559
6. Hyperplans vectoriels et affines d'un espace euclidien . . 560
6.1. Lemme de RIESZ 560
6.2. Espace affine euclidien (élargissement vers l'affine) 561
6.3. Transposition 562
6.4. Crochet de dualité 563
7. Bilan 564

1. Problèmes

Problème 115 - Expérience physique

Les espaces (vectoriels) dont on parle en mathématiques sont des idéalisations des espaces géométriques des espaces à 1,2 ou 3 dimensions de la physique.
Or dans ces espaces physiques (ou géométriques), il y a aussi naturellement un produit entre les vecteurs : le produit scalaire si souvent utilisé en Physique.
Si on essaye alors d'idéaliser également les produit scalaire dans les espaces vectoriels, quelles sont les propriétés algébriques et abstraites que doivent vérifier cette opération entre deux vecteurs ? Quels sont l'origine et le but de cette opération ? Est-elle (bi)linéaire ? Et que penser du fait que $\vec{u}\cdot\vec{u}$ est un nombre strictement positif ssi $\vec{u}\neq 0$?

Problème 116 - Projection selon un vecteur

Continuons. En physique, on exploite souvent le produit scalaire pour projeter un vecteur sur un autre.
Dans le cours sur les espaces vectoriels, les projecteurs sont parfois problématiques : ils existent dès qu'on dispose de deux espaces supplémentaires dans E, mais l'expression $x \mapsto p(x)$ est rarement explicite.
Est-il possible d'exploiter les produits scalaires pour pouvoir exprimer explicitement $p_{\vec{u}}(\vec{x})$, la projection de $\vec{x}$ sur $\vec{u}$?
Et plus largement, sur un sous-espace vectoriel ?

Problème 117 - Espace orthogonaux

Nous savons qu'un sous-espace vectoriel admet une INFINITE de sous-espace supplémentaire dans E.
Si F est connue, ainsi que p_F, alors cela ne définit-il pas aussi l'espace G tel que $E = F \oplus G$ et p_F est la projection sur F de direction G ?
Il existe donc un UNIQUE espace supplémentaire à F qui est privilégié dans l'espace (euclidien) E. Qui est-il ?

Problème 118 - Décomposition sur une base

Comme pour les projecteurs, étant donné une base $\mathcal{B} = (e_1, e_2, \dots e_n)$ de E, l'application

$$\Phi : E \longrightarrow \mathbb{K}^n, x \longmapsto (a_1, \dots a_n) \text{ tel que } x = \sum_{i=1}^{n} a_i e_i$$

n'est pas, en générale, pas explicite. Si il est possible d'expliciter les projecteurs, sûrement est-il également le cas pour cette application ou pour les $\Phi_k : x \mapsto a_k$.
En fait, on verra que cela est naturel quand la base est orthonormée (pour un produit scalaire définie sur E) ? Qu'est-ce que cela signifie ?

? Problème 119 - Bases orthonormées

Est-ce que tous les espaces euclidiens (vectoriels, finis, avec un produit scalaire) admettent au moins une base orthonormée? Peut-on prolonger également les autres théorèmes sur les bases : bases incomplètes…

? Problème 120 - Dualité et problème réciproque

Soit E euclidien, $\mathscr{B} = (e_1, \dots e_n)$ une base. On notera alors que $\Phi_k : E \to \mathbb{K}, x \mapsto a_k$ (tel que $x = \sum_{k=0}^{n} \Phi_k(x) e_k$) est une fome linéaire.

Réciproquement, est-ce qu'une forme linéaire s'associe nécessairement à un vecteur?

Une famille de formes linéaires indépendantes à une base orthogonale?

Cela dépend sûrement du produit scalaire…

Dans ce chapitre les espaces vectoriels sont des $\mathbb{R}$-espaces vectoriels exclusivement.

2. Définitions et règles de calcul

2.1. Produit scalaire

Définition - Produit scalaire

Soit E un $\mathbb{R}$-espace vectoriel. On dit que ϕ est un produit scalaire sur E si ϕ est une forme bilinéaire symétrique définie positive, c'est-à-dire si ϕ est une application de $E \times E$ dans $\mathbb{R}$ vérifiant :

1. (bilinéaire)
$$\forall (x, x', y) \in E^3, \forall (\lambda, \lambda') \in \mathbb{R}^2, \phi(\lambda x + \lambda x', y) = \lambda \phi(x, y) + \lambda' \phi(x', y)$$
$$\forall (x, y, y') \in E^3, \forall (\lambda, \lambda') \in \mathbb{R}^2, \phi(x, \lambda y + \lambda' y') = \lambda \phi(x, y) + \lambda' \phi(x, y')$$
2. (symétrique)
$$\forall (x, y) \in E^2, \phi(x, y) = \phi(y, x)$$
3. (positive)
$$\forall x \in E, \phi(x, x) \geqslant 0$$
4. (définie)
$$\forall x \in E, \phi(x, x) = 0 \Rightarrow x = 0_E$$

Remarque - Linéarité+symétrie

ϕ bilinéaire signifie que, à x_0 fixé, $y \mapsto \phi(x_0, y)$ est une forme linéaire sur E et que, à y_0 fixé, $x \mapsto \phi(x, y_0)$ est aussi une forme linéaire.
Si ϕ est symétrique et "linéaire par rapport à la première variable", alors ϕ est nécessairement bilinéaire.

Définition - Notations

Les notations les plus usuelles sont :
$$\phi(x, y) = (x, y) = \langle x, y \rangle = \langle x | y \rangle = x \cdot y$$

Définition - Espace préhilbertien réel

On appelle espace préhilbertien réel un $\mathbb{R}$-espace vectoriel muni d'un produit scalaire.

Pour aller plus loin - Espace hermitien (1)

Il existe une théorie des produits scalaires complexes. On parle d'espace hermitien, en hommage à Charles Hermite, mathématicien français de la fin du XIX siècle.



Pour aller plus loin - Forme sesquilinéaire, hermitienne

On dit que $f \in E^*$ (forme linéaire), avec E, $\mathbb{C}$-ev est sesquilinéaire si
$\forall \lambda, \mu \in \mathbb{C}, x, y \in E$,
$f(\lambda x + \mu y) = \overline{\lambda} f(x) + \overline{\mu} f(x)$.
On dit que f (forme linéaire sur $(E^*)^2$) est hermitienne si
$\forall x, y \in E$, $f(x, y) = \overline{f(y, x)}$.

On appelle produit scalaire complexe, toute forme linéaire à gauche, sesquilinéaire à droite (ou l'inverse) hermitienne, définie et positive.

Savoir faire - Montrer qu'on a un produit scalaire

On vérifie chacune des hypothèses…
A commencer par le fait qu'il s'agisse d'une forme linéaire!
On démontre la symétrie avant la linéarité à gauche. Comme cela, on obtient la linéarité à droite.
On démontre la forme positive avant le fait que cela soit une forme définie.

Proposition - La bilinéarité en action

Soient $(X_i)_{1 \leqslant i \leqslant r}$ et $(Y_j)_{1 \leqslant j \leqslant s}$ deux familles de vecteurs de E et $(\lambda_i)_{1 \leqslant i \leqslant r}$ et $(\mu_j)_{1 \leqslant j \leqslant s}$ deux familles de réels. Alors
$$\langle \sum_{i=1}^{r} \lambda_i X_i \,|\, \sum_{j=1}^{s} \mu_j Y_j \rangle = \sum_{i=1}^{r} \sum_{j=1}^{s} \lambda_i \mu_j \langle X_i \,|\, Y_j \rangle.$$

Démonstration

Il suffit d'écrire la formule (d'abord linéarité à gauche, puis à droite) :
$$\langle \sum_{i=1}^{r} \lambda_i X_i \,|\, \sum_{j=1}^{s} \mu_j Y_j \rangle = \sum_{i=1}^{r} \lambda_i \langle X_i \,|\, , \rangle \sum_{j=1}^{s} \mu_j Y_j = \sum_{i=1}^{r} \sum_{j=1}^{s} \lambda_i \mu_j \langle X_i \,|\, Y_j \rangle$$
□

Théorème - Inégalité de Cauchy-Schwarz

Soient $x, y \in E$,
$$\langle x \,|\, y \rangle^2 \leqslant \langle x \,|\, x \rangle \langle y \,|\, y \rangle$$
avec égalité si et seulement si (x, y) est une famille liée.

Démonstration classique (parmi les 10 à connaître sur l'année).

Pour aller plus loin - Pour les produit scalaire complexe

L'inégalité de Cauchy-Schwarz reste vraie, on voit apparaître des modules.
Ils sont nécessaires et expliquent la définition donnée à de telles produits

Démonstration

Soient $t \in \mathbb{R}$ et $P(t) = \langle x + ty \,|\, x + ty \rangle$.
Comme le produit scalaire est une forme définie positive, $P(t) \geqslant 0$ avec $P(t) = 0$ ssi $x + ty = 0$.
Or lorsqu'on développe P, par bilinéarité et symétrie, on constate que P est une fonction polynomiale :
$$P(t) = \langle x \,|\, x \rangle + 2t \langle x \,|\, y \rangle + t^2 \langle y \,|\, y \rangle$$
— de degré 2 si $\langle y \,|\, y \rangle \neq 0$ i.e. $y \neq 0$
— de degré 1 si $y = 0$, mais ce cas est sans intérêt… De même on suppose que $x \neq 0$.
Nécessairement son discriminant est négatif
$$\Delta = 4 \langle x \,|\, y \rangle - 4 \langle x \,|\, x \rangle^2 \langle y \,|\, y \rangle^2 \leqslant 0 \Longrightarrow \langle x \,|\, y \rangle^2 \leqslant \langle x \,|\, x \rangle \langle y \,|\, y \rangle$$
Il y a une égalité, si et seulement si $\Delta = 0$, donc que P admet une racine,
Donc si et seulement il existe $t_0 \in \mathbb{R}$ tel que $x + t_0 y = 0$,
et donc, si et seulement si, (x, y) est une famille liée. □

2.2. Norme euclidienne

Définition - Norme

On appelle norme sur un $\mathbb{R}$-espace vectoriel E toute application N de E dans $\mathbb{R}$ telle que

$\forall x \in E, N(x) = 0 \Rightarrow x = 0_E$
$\forall \lambda \in \mathbb{R}, \forall x \in E, N(\lambda x) = |\lambda| N(x)$
$\forall (x, y) \in E^2, N(x + y) \leqslant N(x) + N(y)$ (inégalité triangulaire)

Corollaire - Propriétés directes
Plus précisément :
- $N(x) = 0 \Leftrightarrow x = 0_E$
- $N(-x) = N(x)$
- $N(x) \geqslant 0$

Démonstration
Si $x = 0$, alors $N(x) = N(0 \cdot u) = |0|N(u) = 0$.
On a bien également l'implication $x = 0 \Rightarrow N(x) = 0$.
$N(-x) = N(-1 \cdot x) = |-1|N(x) = N(x)$.
$N(x) = \frac{1}{2}N(x) + \frac{1}{2}N(x) = \frac{1}{2}N(x) + \frac{1}{2}N(-x) \geqslant \frac{1}{2}N(x - x) = \frac{1}{2}N(0) = 0$ □

Proposition - Inégalité triangulaire revisitée
Soit N une norme sur E, alors

$$\forall (x, y) \in E^2, \left|N(x) - N(y)\right| \leqslant N(x + y) \leqslant N(x) + N(y).$$

Démonstration
La partie de droite est connue par l'inégalité triangulaire.
Par ailleurs,

$$N(x + y) + N(y) = N(x + y) + N(-y) \geqslant N(x + y - y) = N(x) \quad \Rightarrow \quad N(x + y) \geqslant N(x) - N(y)$$

De même $N(x + y) = N(y + x) \geqslant N(y) - N(x)$.
Donc $N(x + y) \geqslant \max\big(N(x) - N(y), N(y) - N(x)\big) = |N(x) - N(y)|$ □

Définition - Vecteur unitaire
Soit N une norme sur E. Un vecteur x de E est dit unitaire (ou normé) si $N(x) = 1$.

Définition - Distance associée (et proposition)
Si N est une norme sur E, l'application

$$\begin{array}{rl} d : E^2 & \to \mathbb{R}_+ \\ (A, B) & \mapsto N(B - A) \end{array}$$

est appelée distance associée à la norme N et vérifie
- $\forall (A, B) \in E^2, d(A, B) = 0 \Leftrightarrow A = B$
- $\forall (A, B) \in E^2, d(A, B) = d(B, A)$
- $\forall (A, B, C) \in E^3, d(A, C) \leqslant d(A, B) + d(B, C)$

Démonstration

$$d(A, B) = 0 \Longleftrightarrow N(B - A) = 0 \Longleftrightarrow B - A = 0 \Longleftrightarrow B = A$$
$$d(A, B) = N(B - A) = N(-(B - A)) = N(A - B) = d(B, A)$$

Par inégalité triangulaire :

$$d(A, C) = N(C - A) \leqslant N(C - B) + N(B - A) = d(C, B) + d(B, C)$$

□

Proposition - Norme euclidienne
Si E est muni d'un produit scalaire $\langle . | . \rangle$ alors l'application

$$\begin{array}{rl} E & \to \mathbb{R} \\ x & \mapsto \|x\| = \sqrt{\langle x | x \rangle} \end{array}$$

est une norme sur E. On l'appelle norme euclidienne associée au produit scalaire $\langle . | . \rangle$, la distance associée est appelée distance euclidienne.

Pour aller plus loin - Espace métrique
On appelle espace normé, un espace vectoriel muni d'une norme.
On appelle espace métrique, un espace vectoriel muni d'une distance.
D'après notre définition-proposition : toute espace normé est un cas particulier d'espace métrique.
D'une certaine façon, la topologie est l'étude des espaces métriques.
Les espaces préhilbertiens forment une classe très particulières des espaces métriques…

Histoire - Hermann Minkowski



Hermann Minkowski, né à Alexotas en Russie (aujourd'hui en Lituanie) le 22 juin 1864 et mort à Göttingen le 12 janvier 1909, est un mathématicien et un physicien théoricien allemand.
Il est également connu pour sa contribution non négligeable auprès d'Einstein pour la mise en place de la théorie de la relativité générale.

Remarque - Inégalité de Minkowski
L'inégalité triangulaire d'une norme, qui dérive d'un produit scalaire (norme euclidienne) s'appelle en règle générale l'inégalité de Minkowski. Elle a un sens géométrique certain (et pas uniquement algébrique)

Démonstration
Il faut vérifier point par point, pour N ainsi défini, les axiomes des distances :
- comme le produit scalaire est défini :
$$\|x\| = 0 \Longrightarrow \|x\|^2 = 0 \Longrightarrow \langle x | x \rangle \Longrightarrow x = 0$$
- par bilinéarité puis en prenant la racine :
$$\|\lambda \cdot x\|^2 = \langle \lambda \cdot x | \lambda \cdot x \rangle = \lambda^2 \|x\|^2 \Longrightarrow \|\lambda \cdot x\| = |\lambda| \|x\|$$
- on commence par développer (on exploite la symétrie) et on utilise l'inégalité de Cauchy-Schwarz :
$$\|x + y\|^2 = \langle x + y | x + y \rangle = \|x\|^2 + 2\langle x | y \rangle + \|y\|^2 \leqslant \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$$
En prenant la racine, on trouve le résultat attendu (inégalité de Minkowski).

□

Exercice
Soit E un espace préhilbertien. Dans quel cas a-t-on $\|x + y\| = \|x\| + \|y\|$ (l'égalité triangulaire) ?

Correction
Si on reprend la démonstration, on se rend compte qu'il faut et il suffit que l'on ait l'égalité dans l'inégalité de Cauchy-Schwarz.
Donc il faut et il suffit que x et y soient colinéaire, positivement (puisqu'on prend la racine).
Pour la distance associée cela signifie qu'il faut que les points A, B et C soient alignés. Le plus court chemin entre deux points (A et C) est la ligne droite (passant par B, dans l'alignement entre A et C (et non à l'extérieur)).

Corollaire - Inégalités (Cauchy-Schwarz, Minkowski) avec des normes
Soit E, un espace préhilbertien.

$$\forall (x, y) \in E^2, |\langle x | y \rangle| \leqslant \|x\| \, \|y\|$$

avec égalité si et seulement si (x, y) est une famille liée.

$$\forall (x, y) \in E^2, \|x + y\| \leqslant \|x\| + \|y\|$$

avec égalité si et seulement si (x, y) est positivement liée.

Savoir faire - Montrer qu'on a une norme
On vérifie chacune des hypothèses…
Ou bien; on démontre que la norme dérive d'un produit scalaire bien connue (ou démontré)

Proposition - Produits scalaires usuels et normes associées
On définit des produits scalaires sur $\mathbb{R}^n$, et sur $\mathscr{C}([a, b], \mathbb{R})$, en posant :
- sur $\mathbb{R}^n$, avec $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$,
$$\langle x | y \rangle = \sum_{i=1}^{n} x_i y_i, \quad \|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}$$
- sur $\mathscr{C}([a, b], \mathbb{R})$,
$$\langle f | g \rangle = \int_a^b f(t) g(t) \, dt \quad \|f\| = \sqrt{\int_a^b f(t)^2 \, dt}$$

Démonstration
Le premier produit est bien un produit scalaire :
- Il s'agit bien d'une forme : à valeurs dans $\mathbb{R}$.
- Il est bilinéaire et symétrique.
- Il est positif : $\langle x\,|\,x\rangle = \sum_{i=1}^{n} x_i^2 \geqslant 0$
- Il est défini : $\langle x\,|\,x\rangle = 0 \Rightarrow \sum_{i=1}^{n} x_i^2 = 0 \Rightarrow \forall\, i \in \mathbb{N}_n,\ x_i = 0 \Rightarrow x = 0$

Le second produit est bien un produit scalaire :
- Il s'agit bien d'une forme : à valeurs dans $\mathbb{R}$.
- Il est linéaire à gauche (comme l'intégrale) : $\int_a^b (\lambda_1 f_1 + \lambda_2 f_2)g = \lambda_1 \int_a^b fg + \lambda_2 \int_a^b fg$ et symétrique : $\int_a^b fg = \int_a^b gf$, donc bilinéaire.
- Il est positif : $\langle f\,|\,f\rangle = \int_a^b f^2 \geqslant 0$
- Il est défini : $\langle f\,|\,f\rangle = 0 \Rightarrow \int_a^b f^2 \geqslant 0 \Rightarrow \forall\, x \in [a,b],\ f^2(x) = 0$ car $f^2 \geqslant 0$ et f^2 est continue. Donc $\Rightarrow f = 0_{|[a,b]}$

□

Exemple - Application de ces inégalités

1. dans $\mathbb{R}^n$,
$$\left|\sum_{i=1}^{n} x_i y_i\right| \leqslant \sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2}.$$
2. dans $\mathscr{C}([a,b],\mathbb{R})$,
$$\left|\int_a^b f(t)g(t)\,dt\right| \leqslant \sqrt{\int_a^b f(t)^2\,dt}\sqrt{\int_a^b g(t)^2\,dt}.$$

2.3. Différentes identités

Théorème - Identités
Soit E un e.v. muni d'un produit scalaire $\langle .\,|\,.\rangle$ et $\|.\|$ la norme associée. Pour $(x,y) \in E^2$ on a
$$\|x+y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x\,|\,y\rangle$$
$$\|x-y\|^2 = \|x\|^2 + \|y\|^2 - 2\langle x\,|\,y\rangle$$
$$\langle x\,|\,y\rangle = \frac{1}{4}(\|x+y\|^2 - \|x-y\|^2)$$
$$\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$$
Les trois premières égalités sont appelées « identités de polarisation » (elles permettent de récupérer le produit scalaire à partir de la norme) et la quatrième « égalité du parallélogramme »

Démonstration
Soient $x, y \in E$, par bilinéarité et symétrie :
$$\|x+y\|^2 = \langle x+y\,|\,x+y\rangle = \langle x\,|\,x\rangle + 2\langle x\,|\,y\rangle + \langle y\,|\,y\rangle = \|x\|^2 + \|y\|^2 + 2\langle x\,|\,y\rangle$$
$$\|x-y\|^2 = \langle x-y\,|\,x-y\rangle = \langle x\,|\,x\rangle - 2\langle x\,|\,y\rangle + \langle y\,|\,y\rangle = \|x\|^2 + \|y\|^2 - 2\langle x\,|\,y\rangle$$
On soustrait et on additionne :
$$\|x+y\|^2 - \|x-y\|^2 = 4\langle x\,|\,y\rangle$$
$$\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$$
□

Remarque - Identité de polarisation
Non seulement, elles permettent de récupérer le produit scalaire à partir de la norme, mais surtout, elles permettent de savoir si une norme donné dérive d'un produit scalaire.
Ou encore, de manière identique, elles permettent de savoir si un espace normé est en fait un espace euclidien. Dans ce cas, il aurait une structure beaucoup plus riche (comme on le voit par la suite avec les notions d'orthogonalité ou d'angles…)

Savoir faire - Montrer qu'on a une norme est euclidienne
La polarisation donne une expression d'une forme bilinéaire qui nécessairement est à l'origine de la norme, si celle-ci est bien euclidienne. Il s'agit donc de vérifier chacun des points pour cette forme : $(x,y) := \frac{1}{2}(N(x+y) - N(x) - N(y)$ (ou $\frac{1}{4}(N(x+y) - N(x-y)$). C'est sur la linéarité qu'on peut avoir des difficultés…

Pour l'exercice suivant, on fera attention à ne pas confondre vecteur x, y et coordonnées x, y…
Exercice
Pour $(x,y) \in \mathbb{R}^2$ on pose $Q(x,y) = 2x^2 + 5y^2 - 2xy$. Montrer que Q est le carré d'une norme euclidienne sur $\mathbb{R}^2$.

Correction
Prenons $u = (x,y)$ et $u' = (x',y') \in E = \mathbb{R}^2$.
Notons $\langle u\,|\,u'\rangle = \frac{1}{2}\left(Q(u+u') - Q(u) - Q(u')\right)$
$$= \frac{1}{2}\left(2(x+x')^2 + 5(y+y')^2 - 2(x+x')(y+y') - 2x^2 + 5y^2 - 2xy - 2x'^2 + 5y'^2 - 2x'y'\right)$$
Cela donne $\langle (x,y)\,|\,(x',y')\rangle = 2xx' + 5yy' - 2xy' - 2x'y$.
Ainsi $\langle \cdot\,|\,\cdot\rangle$ est symétrique, bilinéaire.
Il est également positif car $\langle (x,y)\,|\,(x,y)\rangle = Q(x,y) = 2(x-y)^2 + 7y^2 \geqslant 0$.
Et il est défini car $\langle (x,y)\,|\,(x,y)\rangle = Q(x,y)0 \Rightarrow 2(x-y)^2 + 7y^2 = 0 \Rightarrow y = 0$ et $x - y = 0 \Rightarrow x = y = 0$

Exercice
Pour $(x,y) \in \mathbb{R}^2$ on pose $\|(x,y)\|_\infty = \max(|x|,|y|)$. Montrer que $\|.\|_\infty$ est une norme sur $\mathbb{R}^2$, non euclidienne.

Correction
Il s'agit bien d'une norme :
- $\|(x,y)\| \geqslant 0$
- $\|\lambda(x,y)\| = \max(|\lambda x|,|\lambda y|) = |\lambda|\max(|x|,|y|) = |\lambda|\|(x,y)\|$
- $\|(x,y) + (x',y')\| = \max(|x+x'|,|y+y'|)$. Or
$$|x+x'| \underbrace{\leqslant}_{\text{inégalité triangulaire de } |\cdot|_{\mathbb{R}}} |x| + |x'| \underbrace{\leqslant}_{\text{propriété de max}} \|(x,y)\| + \|(x',y')\|$$
De même $|y+y'| \leqslant \|(x,y)\| + \|(x',y')\|$.
Donc en prenant le maximum des deux : $\|(x,y) + (x',y')\| \leqslant \|(x,y)\| + \|(x',y')\|$

Cette norme ne dérive pas d'un produit scalaire, sinon $(x,y)\cdot(x',y') \mapsto \frac{1}{4}\left(\|(x,y) + (x',y')\|^2 - \|(x,y) - (x',y')\|^2\right)$ serait un produit scalaire.
Ce qui ne peut pas fonctionner, c'est la linéarité.
$$(x,y)\cdot(x',y') = \frac{1}{4}\left(\|(x,y) + (x',y')\|^2 - \|(x,y) - (x',y')\|^2\right) = \frac{1}{4}(\max(|x+x'|^2,|y+y'|^2) - \max(|x-x'|^2 + |y-y'|^2)$$
$$(1,2)\cdot(1,1) = \frac{1}{4}(9-1) = 2 \qquad (1,-1)\cdot(1,1) = \frac{1}{4}(4-4) = 0$$
$$[(1,2) + 2(1,-1)]\cdot(1,1) = (3,0)\cdot(1,1) = \frac{1}{4}(16-4) = 3 \neq 2 + 2\times 0 = 2$$

3. Orthogonalité

E désigne un espace préhilbertien réel.

3.1. Vecteurs orthogonaux

Définition - Vecteurs orthogonaux
Soient x et y deux vecteurs de E. x et y sont dits orthogonaux si $\langle x \mid y\rangle = 0$.
On note alors $x \perp y$.

Théorème - Pythagore
$$x \perp y \Leftrightarrow \|x+y\|^2 = \|x\|^2 + \|y\|^2.$$

Démonstration
On exploite la première identité de polarisation □

Exercice
Montrer que dans $\mathscr{C}([0,\pi],\mathbb{R})$ muni de son produit scalaire usuel, $\sin \perp \cos$.

Correction
$\langle \sin \mid \cos\rangle = \int_0^\pi \sin t \cos t \,\mathrm{d}t = \frac{1}{2}\int_0^\pi \sin(2t)\mathrm{d}t = \frac{1}{4}\left[-\cos(2t)\right]_0^\pi = 0$

3.2. Sous-espaces orthogonaux

Définition - Espace orthogonaux
Soient F et G deux s.e.v de E. F et G sont dits orthogonaux si
$$\forall x \in F, \forall y \in G,\ x \perp y.$$
On note alors $F \perp G$.

Proposition - Résultats directs
Soient F et G deux s.e.v de E.
— Si $F \perp G$ alors $F \cap G = \{0_E\}$.
— Si $F = \mathrm{vect}(f_1,\dots,f_n)$ et $G = \mathrm{vect}(g_1,\dots,g_p)$ alors
$$(F \perp G) \Leftrightarrow (\forall (i,j) \in [\![1,n]\!] \times [\![1,p]\!],\ f_i \perp g_j).$$

Démonstration
Si $x \in F \cap G$, alors $\langle x \mid x\rangle = 0$ et donc $x = 0$. Donc $F \cap G = \{0\}$.
Supposons que $F \perp G$.
Alors comme $f_i \in F$ et $g_j \in G$, nécessairement $f_i \perp g_j$.
Réciproquement, supposons que $\forall (i,j) \in [\![1,n]\!] \times [\![1,p]\!]$, $f_i \perp g_j$.
Alors pour $x \in F$, $x = \sum_{i=1}^n x_i f_i$ car $F = \mathrm{vect}(f_1,\dots,f_n)$.
Et pour $y \in F$, $y = \sum_{j=1}^p y_j g_j$ car $G = \mathrm{vect}(g_1,\dots,g_p)$.
Donc, par bilinéarité : $\langle x \mid y\rangle = \sum_{i,j} x_i y_j \langle f_i \mid g_j\rangle = 0$.
Donc $F \perp G$ □

Définition - « Le » espace orthogonal
Soit F un s.e.v de E. On appelle orthogonal de F, et on note $F^\perp$, l'ensemble des vecteurs de E orthogonaux à ceux de F :
$$F^\perp = \{x \in E \mid \forall y \in F, x \perp y\}.$$
$F^\perp$ est un s.e.v. de E. Plus précisément, il s'agit du plus grand espace vectoriel pour la relation d'ordre de l'inclusion :
$$G \perp F \Rightarrow G \subset F^\perp$$

Démonstration
$0 \in F^\perp$, donc $F^\perp$ est non vide.
Si $x_1, x_2 \in F^\perp$ et $\lambda_1, \lambda_2 \in \mathbb{R}$, alors (par linéarité à gauche) :
$$\forall\ y \in F, \qquad \langle \lambda_1 x_1 + \lambda_2 x_2 \mid y\rangle = \lambda_1 \langle x_1 \mid y\rangle + \lambda_2 \langle x_2 \mid y\rangle = 0 + 0 = 0$$
Donc $F^\perp$ est bien un sev de E.
Puis supposons que $G \perp F$. Soit $x \in G$
Alors pour tout $y \in F$, $x \perp y = 0$, donc $x \in F^\perp$. □

Proposition - Propriétés de l'orthogonal
Soient F, G deux s.e.v de E. Alors
$F \subset (F^\perp)^\perp$;
$F \subset G \Rightarrow G^\perp \subset F^\perp$.

Démonstration
Soit $x \in F$.
$$\forall\ z \in F^\perp, \qquad \langle x \mid z\rangle = 0$$
donc $x \in (F^\perp)^\perp$.
Supposons que $F \subset G$.
Soit $x \in G^\perp$.
Alors pour tout $z \in F$, $z \in G$, donc $\langle x \mid z\rangle = 0$, donc $x \perp z$.
Ainsi $x \in F^\perp$.
On a alors montré que $G^\perp \subset F^\perp$. □

Remarque - A-t-on égalité $F = (F^\perp)^\perp$?
Dans le cas des espaces de dimensions finis, nous verrons avec un raisonnement sur la dimension qu'on a nécessairement l'égalité ($\dim F = \dim E - \dim F^\perp = \dim (F^\perp)^\perp$).
Dans le cas infini, il peut n'y avoir qu'une inclusion : Par exemple, en prenant $E = \mathbb{C}^0(I)$ et F, l'espace des fonctions polynomiales.
Alors, par argument de densité : $F^\perp = \{0\}$ et donc $(F^\perp)^\perp = E \neq F$

3.3. Familles orthogonales, orthonormales

Heuristique - Intérêt des bases orthonormales
Lorsqu'on connait une base $\mathscr{B} = (e_1, e_2, \dots e_n)$ d'un espace vectoriel E, on écrit régulièrement :
« *si $x \in E$, alors x s'écrit $x = \sum_{i=1}^n x_i e_i \dots$* ».
Ce qui serait bien ce serait de pouvoir faire « un truc » qui nous permette d'avoir accès à x_i à partir de x et de la base $\mathscr{B}$.
Ce truc, ou opération devrait pouvoir affirmer :
coordonnée du vecteur e_i dans la base (e_k) : 1 si $k = i$ et 0 si $k \neq i$.
C'est exactement ce que propose un produit scalaire, pour une base orthonormale

Pour aller plus loin - Forme linéaire duale
Plus précisément ce qu'on cherche : $\Phi_i : E \to \mathbb{R}$, $x \mapsto x_i$.
On a en fait $\Phi_i : x \mapsto \langle x \mid e_i\rangle$ si la famille $(e_1, e_2, \dots e_n)$ est une base orthonormée de E

Définition - Famille orthogonale - orthonormale
Soit $\mathscr{F} = (u_i)_{i\in I}$ une famille de vecteurs de E.
On dit que $\mathscr{F}$ est orthogonale si $\forall (i,j) \in I^2$, $i \neq j \Rightarrow u_i \perp u_j$, et que $\mathscr{F}$ est orthonormale (orthonormée) si elle est orthogonale et $\forall i \in I$, $\|u_i\| = 1$.

Exercice
Montrer que pour la produit scalaire : $\langle P \mid Q\rangle = \sum_{k=0}^n P^{(k)}(a) Q^{(k)}(a)$ définie sur $\mathbb{R}_n[X]$, la base $((X-a)^k)_k$ est une base orthogonale.
Retrouver la formule de Taylor

Correction
Si $h \leqslant k$, (par récurrence) $\left((X-a)^k\right)^{(h)} = \frac{k!}{(k-h)!}(X-a)^{k-h}$.
Donc « en a », $\left((X-a)^k\right)^{(h)}(a) = 0$ si $h < k$ et $\left((X-a)^k\right)^{(k)}(a) = k!$.

Pour aller plus loin - Polynôme de Lagrange
On peut faire un exercice équivalent en choisissant bien le produit scalaire et pour lequel la base est formée de la famille des polynômes d'interpolation de Lagrange

Par ailleurs comme $\left((X-a)^k\right)^{(k)} = k!$ est une constante, pour tout. $h > k$, $\left((X-a)^k\right)^{(h)} = 0$.

Donc si on note $T_k = (X-a)^k$:

$$\langle T_k \mid T_r\rangle = \sum_{h=0}^{n} T_k^{(h)}(a) T_r^{(h)}(a) = \begin{cases} 0 & \text{si } k \neq r \\ (k!)^2 & \text{si } k = r \end{cases}$$

On a donc une famille orthogonale. Elle est echelonnée donc forme une base.

Si $P = \sum_{i=0}^{n} \lambda_i T_i$, alors, par linéarité :

$$\langle P, T_k \mid =\rangle \sum_{i=0}^{n} \lambda_i \langle T_i \mid T_k\rangle = \lambda_k (k!)^2 = \sum_{i=0}^{n} P^{(i)}(a) T_k^{(i)}(a) = P^{(k)}(a) k!$$

Donc $\lambda_k = \dfrac{P^{(k)}(a)}{k!}$ et ainsi : $P = \sum_{i=0}^{n} \dfrac{P^{(i)}(a)}{i!}(X-a)^i$.

Proposition - Famille libre
Toute famille orthogonale de vecteurs non nuls est libre.
Toute famille orthonormale est libre.

Démonstration
Soit $\mathscr{F} = (u_i)_{i\in I}$ une famille de vecteurs de E.
Soient $(\lambda_i)_{i\in I}$ une famille de réels telle que $\sum_{i\in I} \lambda_i u_i = 0$.

Alors par linéarité :

$$\forall\ j \in I \qquad 0 = \langle 0 \mid u_j\rangle = \sum_{i\in I} \lambda_i \langle u_i \mid u_j\rangle = \lambda_j \|u_j\|^2$$

Donc si $u_j \neq 0$, $\lambda_j = 0$. Ceci est vrai pour tout j donc la famille $\mathscr{F}$ est libre.
Une famille orthonormale est orthogonale avec des vecteurs non nuls car de norme égale à 1. □

Proposition - Pythagore (généralisé)
Soit $(u_1,\dots,u_p)$ une famille orthogonale de vecteurs de E. On a

$$\left\| \sum_{i=1}^{p} u_i \right\|^2 = \sum_{i=1}^{p} \|u_i\|^2.$$

Démonstration
Par bilinéarité :

$$\left\| \sum_{i=1}^{p} u_i \right\|^2 = \langle \sum_{i=1}^{p} u_i \mid \sum_{i=1}^{p} u_i\rangle = \sum_{i=1}^{p}\sum_{j=1}^{p} \langle u_i \mid u_j\rangle$$
$$= \sum_{i=1}^{p}\sum_{j=i} \langle u_i \mid u_j\rangle = \sum_{i=1}^{p} \langle u_i \mid u_i\rangle = \sum_{i=1}^{p} \|u_i\|^2$$

□

Théorème - Algorithme d'orthonormalisation de Schmidt
Soit E un $\mathbb{R}$-e.v. muni d'un produit scalaire et $\mathscr{E} = (e_1,\dots,e_p)$ une famille libre de vecteurs de E.
On définit la famille $\mathscr{F} = (f_1,\dots,f_p)$ par

$$f_1 = \frac{1}{\|e_1\|} e_1$$

$$\forall i \in [\![2,p]\!],\ f_i = \frac{1}{\|e_i'\|} e_i' \text{ où } e_i' = e_i - \sum_{j=1}^{i-1} \langle e_i \mid f_j\rangle f_j$$

Alors $\mathscr{F}$ est une famille orthonormale de E telle que

$$\forall k \in [\![1,p]\!],\ \text{vect}(f_1,\dots,f_k) = \text{vect}(e_1,\dots,e_k).$$

On dit que $\mathscr{F}$ est déduite de $\mathscr{E}$ par le procédé d'orthonormalisation de Schmidt.

Histoire - Schmidt



Erhard Schmidt (13 janvier 1876 - 6 décembre 1959) est un mathématicien allemand né à Dorpat, dans l'Empire russe (aujourd'hui Tartu, en Estonie). Le procédé d'othonormalisation est souvent associé également à Jorgen Petersen Gram.

Démonstration
Notons d'abord que l'algorithme termine bien, a priori on sait déjà le nombre d'étape (boucle `for`) : p.
Pour démontrer la justesse de l'algorithme d'orthonormalisation de Schmidt, nous allons procéder par récurrence sur p.

— Si $p = 1$.
f_1 est normalisé, f_1 est colinéaire à e_1, donc vect(f_1) = vect(e_1).

— Soit $p \in \mathbb{N}$ et supposons que le procédé marche pour $p-1$.
Soient $(e_1,\dots e_p)$ une famille libre de vecteurs de E.
Alors $(e_1,\dots e_{p-1})$ est une famille libre de vecteurs de E, on peut lui appliquer le procédé de Schmidt, on construit ainsi (de manière déterministe donc unique) une famillle $(f_i)_{i\leqslant p-1}$ orthonormalisée et telle que $\forall\ k \leqslant p-1$, vect$(f_1,\dots,f_k)$ = vect$(e_1,\dots,e_k)$. Soit $f_p = \dfrac{1}{\|e_p'\|} e_p'$ où $e_p' = e_p - \sum_{j=1}^{p-1} \langle e_p \mid f_j\rangle f_j$.
Alors pour $i < p$,

$$\langle f_p \mid f_i\rangle = \frac{1}{\|e_p'\|}\left(\langle e_p \mid e_i\rangle - \sum_{j=1}^{p-1} \langle e_p \mid f_j\rangle \overline{f_j f_i}_{=\delta_{i,j}}\right) = \frac{1}{\|e_p'\|}\left(\langle e_p \mid e_i\rangle - \langle e_p \mid f_i\rangle\right) = 0$$

Et $\|f_p\| = \dfrac{1}{\|e_p\|}\|e_p\| = 1$.
Donc la famille $(f_1, f_2, \dots f_p)$ est orthonormée.
Enfin Par construction de f_p, $f_p \in$ vect$(e_1, e_2, \dots e_p)$. De même $f_i \in$ vect$(e_1,\dots e_i) \subset$ vect$(e_1, e_2 \dots e_p)$.
Donc vect$(f_1, f_2, \dots, f_p) \subset$ vect$(e_1, e_2, \dots e_p)$.
Mais ces deux familles sont libres (la première est orthonormales - la seconde, par définition),
donc ces deux espaces engendrés dont de même dimension p. Ils sont égaux

□

Remarque - Cette famille orthonormalisée est-elle unique?
La famille obtenue ne dépend que de la famille initiale. Est-elle unique? D'une certaine façon, non. On aurait pu choisir $-f_i$, on aurait alors obtenue une nouvelle famille orthonormale à partir de la même famille $(e_1,\dots e_n)$.
A cette différence de signe près, il n'y a pas d'autres solutions à partir de la famille $(e_1,\dots e_n)$. Notons que lorsqu'on calcule e_i', les signes se compensent.

Savoir faire - Orthonormaliser une base
Pour obtenir une base orthonormalisée, on considère une base de E.
On commence par l'orthogonaliser, puis la normaliser à chaque étape.
Au final, e_i' est la soustraction de e_i, du projeté orthogonal de e_i sur vect$(e_j)_{j<i}$.

Exercice
Vérifier que l'on munit $\mathbb{R}_2[X]$ d'un produit scalaire en posant $\langle P \mid Q\rangle = \int_0^1 P(t)Q(t)\,dt$. Déterminer une b.o.n. de $\mathbb{R}_2[X]$ pour ce produit scalaire.

Correction
La nouveauté de la première question est que l'espace change (il ne s'agit pas des fonctions continues et définies uniquement sur $[0,1]$).
La différence repose donc sur le fait que $\langle P \mid P\rangle = 0 \Rightarrow \forall\ t \in [0,1], P(t) = 0 \Rightarrow P$ a une infinité de racines donc $P = 0$.
On applique le procédé d'orthonormalisation de Schmidt à la base canonique $(1, X, X^2)$ de $\mathbb{R}_2[X]$.

1. $f_1 = \dfrac{1}{\langle 1 \mid 1\rangle} = 1$
2. On commence par calculer $\langle e_2 \mid f_1\rangle = \int_0^1 t\,dt = \frac{1}{2}$.
   Donc $e_2' = X - \frac{1}{2}1$ et $\|e_2'\|^2 = \int_0^1 (t-\frac{1}{2})^2 dt = \frac{1}{3} - \frac{1}{2} + \frac{1}{4} = \frac{1}{12}$.
   Donc $f_2 = \sqrt{12}(X - \frac{1}{2})$
3. On commence par calculer $\langle e_3 \mid f_1\rangle = \int_0^1 t^2 dt = \frac{1}{3}$ et $\langle e_3 \mid f_2\rangle = \int_0^1 \sqrt{12}t^2(t-\frac{1}{2})dt = \sqrt{12}(\frac{1}{4} - \frac{1}{6}) = \frac{\sqrt{12}}{12} = \frac{1}{2\sqrt{3}}$.
   Donc $e_3' = X^2 - X + \frac{1}{6}$ et $\|e_3'\|^2 = \int_0^1 (t^4 - 2t^3 + \frac{4}{3}t^2 - \frac{1}{3}t + \frac{1}{36})dt = \frac{1}{5} - \frac{1}{2} + \frac{4}{9} - \frac{1}{6} + \frac{1}{36} =$

$\frac{36-90+80-30+5}{180} = \frac{1}{180}$.
Donc $f_3 = 6\sqrt{5}(X^2 - X + \frac{1}{6})$
La base orthonormée obtenue est $(1, \sqrt{12}(X - \frac{1}{2}), 6\sqrt{5}(X^2 - X + \frac{1}{6}))$

4. Cas de la dimension finie : espaces euclidiens

4.1. Définition

Définition - Espace euclidien
Un espace euclidien est un $\mathbb{R}$-e.v. de dimension finie, muni d'un produit scalaire (c'est-à-dire un espace préhilbertien réel de dimension finie).

Exemple - Retour sur les deux produits canoniques
$\mathbb{R}^n$ est un espace euclidien, mais pas $\mathscr{C}([a,b],\mathbb{R})$.
Il y a de nombreux exemples sur $\mathbb{R}_n[X]$

Proposition - Ecriture matricielle
Soit E est un espace euclidien (produit scalaire noté $\langle . | . \rangle$), muni d'une base $\mathscr{B} = (e_1, \dots, e_n)$.
On note A la matrice

$$A = \left(\langle e_i \,|\, e_j \rangle\right)_{1 \leqslant i,j \leqslant n} = \begin{pmatrix} \|e_1\|^2 & \dots & \langle e_1 \,|\, e_n \rangle \\ \vdots & & \vdots \\ \langle e_n \,|\, e_1 \rangle & \dots & \|e_n\|^2 \end{pmatrix}$$

appelée matrice du produit scalaire dans la base $\mathscr{B}$.
Soient X et Y les matrices colonnes de $x \in E$ respectivement de $y \in E$ dans $\mathscr{B}$.
Alors, en identifiant une matrice d'ordre 1 à son unique coefficient, on a

$$\langle x \,|\, y \rangle = {}^t X A Y$$

Exercice
Que dire de $\mathscr{B}$ si $A = I_n$?

Correction
$\mathscr{B}$ est une base orthonormée de E pour le produit scalaire considéré

Démonstration

$${}^t X A Y = \sum_{h,k=1}^{n} {}_1[X^T]^h \, {}_h[A]^k \, {}_k[Y]^1 = \sum_{h,k=1}^{n} {}_h[X]^1 \, {}_h[A]^k \, {}_k[Y]^1 = \sum_{h,k=1}^{n} x_h y_k \langle e_h \,|\, e_k \rangle = \langle x \,|\, y \rangle$$

par bilinéarité □

Proposition - Propriétés de la matrice d'un produit scalaire
Soit A la matrice d'un produit scalaire dans une base quelconque. Alors
- A est une matrice symétrique : ${}^t A = A$;
- A est une matrice *positive* : $\forall X \in \mathscr{M}_{n,1}(\mathbb{R}),\ {}^t X A X \geqslant 0$;
- A est une matrice *définie* : $\forall X \in \mathscr{M}_{n,1}(\mathbb{R}),\ {}^t X A X = 0 \Rightarrow X = O_{n,1}$;
- A est inversible : $A \in GL_n(\mathbb{R})$.

Démonstration
On note $\mathscr{B} = (e_1, e_2, \dots e_n)$ la base de E considérée.
Soient $i, j \in \mathbb{N}_n$, ${}_i[A]^j = \langle e_i \,|\, e_j \rangle = \langle e_j \,|\, e_i \rangle = {}_j[A]^i = {}_i[A^T]^j$, par symétrie du produit scalaire.
Pour tout $X \in \mathscr{M}_{n,1}(\mathbb{R})$, en notant $x = \sum_{i=1}^{n} {}_i[X]^1 e_i$.

$${}^t X A X = \langle x \,|\, x \rangle \geqslant 0$$

Puis, si ${}^t X A X = 0$, alors $\langle x \,|\, x \rangle = 0$ et donc $x = 0$ ainsi $X = O$. Le dernier point est un classique à savoir faire (passer du bilinéaire au linéaire).
Soit $X \in \operatorname{Ker} A$, alors ${}^t X A X = {}^t X O = 0$, donc $X = 0$. Ainsi $\operatorname{Ker} A = \{0\}$. Donc A inversible. □

Pour aller plus loin - Polynômes de Bernoulli
On remarquera que le produit scalaire de l'exercice amène aux polynômes de Bernoulli comme base orthogonale (mais non normalisée).

Pour aller plus loin - Espace hermitien
Un espace préhilbertien complexe de dimension finie a été baptisé par David Hilbert, espace hermitien

Pour aller plus loin - Algèbre bilinéaire
Il s'agit maintenant d'algèbre bilinéaire.
Un même objet -une matrice- peut donc avoir deux sens différents.
En algèbre linéaire : $f(x) \circlearrowleft A \times X$
En algèbre bilinéaire : $\Phi(x,y) \circlearrowleft X^T A \times Y$

Pour aller plus loin - Valeur propre
$\lambda \in \mathbb{R}$ est valeur propre de A s'il existe $X \in \mathscr{M}_{n,1}(\mathbb{R})$, $X \neq O_{n,1}$ tel que $AX = \lambda X$

Remarque - Toutes les propriétés essentielles du produit scalaire
se répercutent directement comme propriétés essentielles de la matrice A.
- La bilinéaire donne l'existence de la matrice
- La forme se transforme en produit qui donne un nombre en bout de course
- Le fait d'être positif
- Le fait d'être défini

Exercice
Montrer que les valeurs propres d'une matrice symétrique définie positive sont des réels strictement positifs.

Correction
Soit λ une valeur propre de A et X le vecteur propre associé.

$${}^t X A X = {}^t X (\lambda X) = \lambda {}^t X X = \lambda \left(\sum_{i=1}^{n} x_i^2 \right) \geqslant 0$$

Donc en divisant pas $\left(\sum_{i=1}^{n} x_i^2 \right) > 0$ car $X \neq 0$, on a $\lambda \geqslant 0$.
Enfin, $\lambda \neq 0$, nécessairement, sinon $AX = 0$, et donc A non inversible

4.2. Bases orthonormales

Définition - Base orthonormale
$\mathscr{B}$ est une base orthonormale de E euclidien si $\mathscr{B}$ est une base de E et une famille orthonormale.

Exemple - Base canonique
La base canonique de $\mathbb{R}^n$ est une base orthonormale de $\mathbb{R}^n$ pour le produit scalaire usuel.

Théorème - Existence de bases orthonormales
- Tout espace vectoriel euclidien possède une base orthonormale.
- Toute famille orthonormale de E peut être complétée en une base orthonormale de E.

Démonstration
Il suffit d'appliquer le procédé d'othonormalisation de Gram-Schmidt □

Exercice
Réciproquement, étant donné une base $\mathscr{B}$ de E, $\mathbb{R}$-ev.
Existe-t-il un produit scalaire de E telle que la base $\mathscr{B}$ soit orthonormales ?

Correction
Oui, trivialement ou canoniquement (en notant $\mathscr{B} = (e_1, e_2, \dots e_n)$:

$$\langle \underbrace{x}_{=\sum x_i e_i} \,|\, \underbrace{y}_{=\sum y_j e_j} \rangle = \sum_{i,j} x_i y_j$$

Tout espace vectoriel de dimension finie est un espace euclidien

Savoir faire - Montrer qu'une famille est une base orthonormée
De même que pour savoir si une famille est une base, on exploite la matrice de cette famille ; pour montrer qu'une famille est une base orthonormale, on peut commencer par écrire sa matrice de corrélation : $A = (\langle e_i, e_j \rangle)_{i,j}$.
Cette matrice est symétrique. Elle est inversible ssi (e_i) est une base.
Cette matrice est diagonale ssi (e_i) est une famille orthogonale.
$A = I_n$ ssi (e_i) est orthonormée.

Proposition - Calculs en b.o.n
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base orthonormale de E euclidien (pour le produit scalaire $\langle . | . \rangle$).
Soient $x = \sum_{i=1}^{n} x_i e_i$ et $y = \sum_{i=1}^{n} y_i e_i$ deux vecteurs de E, X et Y les matrices colonnes associées. Alors :

$$\langle x \,|\, y \rangle = \sum_{i=1}^{n} x_i y_i = {}^t XY$$

$$\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}$$

$$\forall\, i \in [\![1, n]\!],\ x_i = \langle x \,|\, e_i \rangle$$

Proposition - Opération matricielle de changement de base orthonormale
Soient $\mathscr{B}$ une base orthonormale de E euclidien de dimension n, $\mathscr{B}'$ une famille de n vecteurs de E, et P la matrice de $\mathscr{B}'$ dans $\mathscr{B}$. Alors $\mathscr{B}'$ est une base orthonormale de E si et seulement si ${}^t PP = I_n$.
Dans ce cas on a donc $P^{-1} = {}^t P$ (on dit que P est une matrice orthogonale).

Remarque - Matrice de passage
On rappelle que la matrice P de $\mathscr{B}'$ dans $\mathscr{B}$ est, comme son nom l'indique, la matrice des coordonnées des vecteurs de la base $\mathscr{B}'$ écrite dans la base $\mathscr{B}$.
Elle vérifie pour X et X' matrice de x écrites dans les bases $\mathscr{B}$ et $\mathscr{B}'$ respectivement :

$$X = PX'$$

Démonstration
Par définition des matrices de passages,

$$\forall\ j \in \mathbb{N}_n, \qquad e'_j = \sum_{k=1}^{n} {}_k[P]^j e_k$$

Dans ce cas, par bilinéarité (et avec la notation de Kronecker)

$$\langle e'_i \,|\, e'_j \rangle = \sum_{h=1}^{n} \sum_{k=1}^{n} {}_h[P]^i {}_j[P]^k \langle e_h \,|\, e_k \rangle = \sum_{k=1}^{n} {}_i[P^T]^k {}_k[P]^j = \mathrm{Coef}_{i,j}({}^t PP)$$

Ainsi, on obtient l'équivalence de la proposition. □

Savoir faire - Changement de base pour une forme bilinéaire
Soit E un espace euclidien et deux bases $\mathscr{B}$ et $\mathscr{B}'$.
Si x a pour coordonnées X dans $\mathscr{B}$ et X' dans $\mathscr{B}'$.
Si y a pour coordonnées Y dans $\mathscr{B}$ et Y' dans $\mathscr{B}'$.
On note A et A' la matrices du produit scalaire dans chacune des deux bases.
Enfin, on note P la matrice de $\mathscr{B}'$ dans $\mathscr{B}$.
On a alors $X = PX'$, $Y = PY'$.

$$\langle x \,|\, y \rangle = {}^t XAY = {}^t X'A'Y' = {}^t X' {}^t PAPY'$$

Ceci étant vrai pour tout x, y, on a donc nécessairement $A' = {}^t PAP$ Ce résultat reste vraie que les bases sont orthonormales ou non

Exercice
$E = \mathbb{R}^3$, $\mathscr{B}$ base canonique. On pose $\mathscr{B}' = (f_1, f_2, f_3)$ où

$$f_1 = \frac{1}{\sqrt{2}}(e_1 - e_3),\ f_2 = \frac{1}{\sqrt{3}}(e_1 + e_2 + e_3),\ f_3 = \frac{1}{\sqrt{6}}(e_1 - 2e_2 + e_3).$$

Montrer que $\mathscr{B}'$ est une base orthonormale de E (pour le produit scalaire canonique).
Soit $f \in \mathscr{L}(E)$ défini par $f(x, y, z) = (x + y, x + z, y + z)$. Donner la matrice de f dans cette base.

Correction
Pour le produit scalaire canonique, la base canonique est orthonormée.
Donc $\mathscr{B}'$ est orthonormale ssi ${}^t P \times P = I_3$.
Or $P = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{3} & \sqrt{2} & 1 \\ 0 & \sqrt{2} & -2 \\ -\sqrt{3} & \sqrt{2} & 1 \end{pmatrix}$ et on vérifie bien que ${}^t P \times P = I_3$ (en fait ce sont exactement les mêmes calculs).
Les coefficients de la matrice A de f vérifient $\mathrm{Coef}_{i,j}(A) = \langle f(f_i) \,|\, f_j \rangle$ Or $f(f_1) = \frac{1}{\sqrt{2}}(1, 0, -1) = f_1$, $f(f_2) = \frac{2}{\sqrt{3}}(1, 1, 1) = 2f_2$ et $f(f_3) = \frac{1}{\sqrt{6}}(-1, 2, 1) = -f_3$.
Donc $A = \mathrm{diag}(1, 2, -1)$

Exercice
Montrer que la matrice $P = \begin{pmatrix} 0 & -1 & 0 \\ \cos\theta & 0 & -\sin\theta \\ \sin\theta & 0 & \cos\theta \end{pmatrix}$ est inversible et calculer son inverse.

Correction
Pour celui qui a l'oeil, on dirait une matrice de rotation.
Les vecteurs $(0, \cos\theta, \sin\theta)$, $(-1, 0, 0)$ et $(0, -\sin\theta, \cos\theta)$ forment une famille orthonormales.
Donc $P^{-1} = P^T = \begin{pmatrix} 0 & \cos\theta & \sin\theta \\ -1 & 0 & 0 \\ 0 & -\sin\theta & \cos\theta \end{pmatrix}$.

5. Projections orthogonales

5.1. Supplémentaire orthogonal

Théorème - L'orthogonal est un supplémentaire (C.S. : F dimension finie)
Soit E un espace préhilbertien réel (pas nécessairement de dimension finie) et F un s.e.v de dimension finie de E. Alors

$$E = F \oplus F^{\perp}.$$

Démonstration
Nous savons que F et $F^{\perp}$ sont orthogonaux donc $F \oplus F^{\perp}$.
Soit $x \in E$. On note $(e_1, \dots e_p)$ une base orthonormée de F.
Puis $y = \sum_{i=1}^{p} \langle x \,|\, e_i \rangle e_i$. Alors nécessairement $y \in F$.
Par ailleurs, pour tout $i \in \mathbb{N}_p$,

$$\langle x - y \,|\, e_i \rangle = \langle x \,|\, e_i \rangle - \langle y \,|\, e_i \rangle = \langle x \,|\, e_i \rangle - \sum_{j=1}^{p} \langle x \,|\, e_j \rangle \langle e_j \,|\, e_i \rangle = 0$$

Donc $x - y \in F^{\perp}$, et donc $E = F + F^{\perp}$. □

Heuristique - LE supplémentaire
Un des problèmes de la notion de supplémentaire est la non-unicité de ceux-ci (E et F étant donné, il existe généralement une infinité G_i tels que $E = F \oplus G_i$).
Parmi ceux-ci (les G_i) un a une propriété qui le rend unique et intéressant (dans le cas d'un espace préhilbertien).

Définition - Supplémentaire orthogonal
Soit E un espace préhilbertien réel (pas nécessairement de dimension finie) et F un s.e.v de dimension finie de E.
$F^\perp$ est appelé LE supplémentaire orthogonal de F.

Proposition - Deux propriétés
Soit E un espace euclidien et F un s.e.v de E. Alors

$$\dim F^\perp = \dim E - \dim F$$
$$(F^\perp)^\perp = F$$

Démonstration
Nous savons que si $E = F \oplus G$, et E de dimension finie,
alors $\dim E = \dim F + \dim G$.
Il reste à appliquer cette relation à $G = F^\perp$.
Nous savons aussi que $F \subset (F^\perp)^\perp$.
$\dim (F^\perp)^\perp = \dim E - \dim F^\perp = \dim E$.
Et donc, pour des raisons de dimension : $F = (F^\perp)^\perp$ □

5.2. Projections orthogonales

Définition - Projection orthogonale
Soit F un s.e.v de dimension finie de E préhilbertien réel.
On appelle projecteur orthogonal (projection orthogonale) sur F le projecteur sur F de direction $F^\perp$.

Remarque - Exprimer explicitement la projection
La proposition qui suit est très importante, elle permet de dépasser une limite de la notion de projecteur pour les espaces vectoriels quelconques. Il était, alors, généralement impossible d'exprimer ce projecteur explicitement, théoriquement. Dans le cas du projecteur orthogonal, cette impossibilité n'existe plus.

Proposition - Expression du projecteur
Soit p_F le projecteur orthogonal sur F.
Si $\mathscr{B} = (e_1, \dots, e_p)$ b.o.n de F alors

$$\forall x \in E,\ p_F(x) = \sum_{i=1}^{p} \langle x | e_i \rangle e_i \qquad \text{et } y = p_F(x) \Leftrightarrow \begin{cases} y \in F \\ x - y \in F^\perp \end{cases}$$

Remarque - Déjà vu?
• Dans le procédé d'orthonormalisation de Schmidt $e_i' = e_i - \sum_{j=1}^{i-1} \langle e_i | f_j \rangle f_j$ désigne le vecteur obtenu en soustrayant à e_i son projeté orthogonal sur le sous-espace engendré par les précédents vecteurs de la famille.
• Dans la démonstration de la supplémentarité de F et $F^\perp$, nous avons exploité cette fonction p_F (noté $y = p_F(x)$ à l'époque)

Démonstration
Pour démontrer que $E = F \oplus F^\perp$, on a décrit $x \mapsto y (= p_F(x))$.
Il s'agit bien de $p_F(x) = \sum_{i=1}^{p} \langle x | e_i \rangle e_i$, dès que $(e_1, e_2, \dots e_p)$ est une base orthonormée de F.
La caractéristique donnée est la mise à jour de la caractéristique : Si p est la projection de E sur F de direction G,
alors $p(x) = y \Leftrightarrow y \in F$ et $x - y \in G$ □

Corollaire - Cas particuliers
Soit E, un espace préhilbertien réel

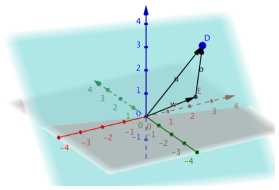
1. Si $F = \text{vect}(e)$ est une droite, alors $p_F(x) = \left\langle x | \frac{e}{\|e\|} \right\rangle \frac{e}{\|e\|} = \frac{\langle x | e \rangle}{\|e\|^2} e$.
2. Si F est un hyperplan de E de dimension finie, alors $F^\perp = \text{vect}(e)$ est une droite et $p_F(x) = x - \left\langle x | \frac{e}{\|e\|} \right\rangle \frac{e}{\|e\|}$.

Démonstration
Le premier résultat est une application direct du résultat précédent avec $\mathscr{B} = (\frac{e}{\|e\|})$, base orthonormée de F.
Pour le second résultat on considère $p_{F^\perp} : x \mapsto \left\langle x | \frac{e}{\|e\|} \right\rangle \frac{e}{\|e\|}$ et donc $p_F = \text{id} - p_{F^\perp}$, on obtient le résultat annoncé. □

Exercice
Déterminer la matrice dans la base canonique de $\mathbb{R}^3$ de la projection orthogonale sur le plan F d'équation $x + y - 2z = 0$.

Correction
$F = \{(x,y,z) \mid x + y - 2z = 0\} = \{(x,y,z) \mid \langle (x,y,z) | 1,1,-2 \rangle = 0\}$, ainsi $F^\perp = \text{vect}(1,1,-2)$.
Ainsi comme $\|(1,1,-2)\|^2 = 6$, on a $p_{F^\perp}(x,y,z) = \frac{x+y-2z}{6}(1,1,-2)$.
Et donc $P = \frac{1}{6}\begin{pmatrix} 5 & -1 & 2 \\ -1 & 5 & 2 \\ 2 & 2 & 2 \end{pmatrix}$

Représentation - Visualisation



On a $d(u, \mathscr{P}) = \|b\|$

5.3. Distance à un sous-ensemble d'une espace préhilbertien

Définition - distance à un sous-ensemble
Soient $x \in E$ et A une partie de E, préhilbertien réel.
L'ensemble $\{d(x,z); z \in A\}$ est une partie non vide de $\mathbb{R}$, minorée par 0, qui admet donc une borne inférieure, appelée distance de x à A :

$$d(x,A) = \inf_{z \in A} \|x - z\|.$$

Théorème - Meilleure approximation
Soient E un espace préhilbertien réel, F un s.e.v de dimension finie de E et p_F la projection orthogonale sur F. Soit $x \in E$, alors

$$y = p_F(x) \Leftrightarrow \begin{cases} y \in F \\ \forall z \in F, \|x - y\| \leqslant \|x - z\| \end{cases} \Leftrightarrow \begin{cases} y \in F \\ \|x - y\| = d(x,F) \end{cases}$$

Remarque - Interprétation
La distance de x à un sous-espace vectoriel F est la distance de x à $p_F(x)$, $p_F(x)$ étant l'unique vecteur de F réalisant cette distance : $p_F(x)$ est le vecteur de F « le plus proche » de x en ce sens.
On dit que $p_F(x)$ est la meilleure approximation de x dans F.

Démonstration
Si $y = p_F(x)$,
alors $y \in F$ et pour tout $z \in F$, d'après Pythagore :

$$\|x - z\|^2 = \|(x - y) + (y - z)\|^2 = \|x - y\|^2 + \|y - z\|^2$$

car $x - y \in F^\perp$ et $y - z \in F$.
Donc $\|x - z\|^2 \geqslant \|x - y\|^2$ et donc $\|x - z\| \geqslant \|x - y\|$.
Ce qui implique, par suite, $\|x - y\| = \inf_{z \in F} \|x - z\|$.
Enfin supposons que $y \in F$ et $\|x - y\| = \inf_{z \in F} \|x - z\|$.
En considérant $y' = p_F(x)$ alors on trouve $\|x - y\| \leqslant \|x - y'\|$.
Or avec Pythagore à nouveau : $\|x - y\|^2 = \|x - y'\|^2 + \|y' - y\|^2$
et donc nécessairement $\|x - y\| = \|x - y'\|$ et surtout $\|y - y'\|^2 = 0$.
Ainsi $y = y' = p_F(x)$ □

Savoir faire - Minimiser une forme quadratique

De manière générale, dans ce contexte, on ne cherche pas le minimum d'une norme, mais bien d'une norme au carré (forme quadratique) qui dérive du produit scalaire canonique.
L'enjeu : reconnaître le produit scalaire et les espaces E et surtout F. Puis, on exploite une projection orthogonale sur F, elle est explicite si l'on connait une base orthonormale de F.
On remarque qu'une base orthogonale de F suffit.

Exercice

Soit $f(x,y) = (x+y-2)^2 + (x-y-2)^2 + (2x+y)^2$.
Montrer que f admet un minimum sur $\mathbb{R}^2$ que l'on déterminera (avec les valeurs de x et y correspondantes).

Correction

On croit voir la norme canonique :

$$f(x,y) = \|(x+y-2, x-y-2, 2x+y)\|^2 = \|(x+y, x-y, 2x+y) - (2,2,0)\|^2$$

Notons alors $F = \text{vect}\big((1,1,2),(1,-1,1)\big)$ et $a = (2,2,0)$.
On cherche $d(a,F)^2$. Celui-ci vaut $\|a - p_F(a)\|^2 = \|a\|^2 - \|p_F(a)\|^2$ (Pythagore) Une base orthonormée de F est donnée par

$$e_1 = \frac{1}{\sqrt{6}}(1,1,2) \qquad e_2 = \frac{1}{\sqrt{21}}(2,-4,1)$$

Donc $p_F(a) = \frac{4}{6}(1,1,2) + \frac{-4}{21}(2,-4,1)$.
Ainsi $\inf f = d(a,F)^2 = 8 - \frac{16}{6} - \frac{16}{21} = \frac{96}{21} = \frac{32}{7}$.

L'exercice qui suit donne une idée de la stratégie de la minimisation par la méthode des moindres carrés. Il s'agit de prendre le problème de manière duale

Exercice

On se donne quatre points $A(1,0)$, $B(0,1)$, $C(3,4)$, $D(-1,-1)$.
Déterminer la droite $\mathscr{D}$ d'équation $y = ax + b$ telle que si A', B', C', D' sont les projetés de A, B, C, D sur $\mathscr{D}$ parallèlement à l'axe Oy, alors $S_{a,b} = AA'^2 + BB'^2 + CC'^2 + DD'^2$ soit minimale.
Comment généraliser cette méthode ?, indépendamment de coordonnés concrètes pour A, B... et d'une projection aussi simple...

Correction

Dans la projection parallèle à $Oy = \text{vect}(\vec{j})$, laisse invariant l'abscisse. Donc, par exemple : $A' = p_D(A) = (x_A, a)$.
On a alors $AA'^2 = (a - y_A)^2$. Quant à a, il vérifie $a = ax_A + b$. De même pour les autres points...
Ainsi

$$S_{a,b} = (a+b-0)^2 + (b-1)^2 + (3a+b-4)^2 + (-a+b+1)^2 = d(u,F)^2$$

avec $u = (0,1,4,-1)$ et $F = \text{vect}\big((1,1,1,1),(1,0,3,-1),\big)$.
Une base orthonormée de F est (e_1, e_2) avec

$$e_1 = \frac{1}{2}(1,1,1,1) \qquad \text{et } e_2 = \frac{1}{\sqrt{140}}(1,-3,9,-7)$$

Donc $p_F(u) = (1,1,1,1) + \frac{40}{140}(1,-3,9,-7)$ Ainsi $\inf f^2 = \|u\|^2 - \|p_F(u)\|^2 = 18 - 4 - \frac{80}{7} = \frac{18}{7}$

Pour aller plus loin - Optimisation de f : $\mathbb{R}^2 \to \mathbb{R}$

Ce problème peut aussi se rencontrer en cours d'optimisation d'une fonction de plusieurs variables.
On remarque ici que

$$f(x,y) = 6x^2 + 3y^2 + 4xy - 8x + 8$$
$$= \frac{1}{3}\big(3y+2x\big)^2 + \frac{14}{3}\Big(x - \frac{6}{7}\Big)^2 + \frac{32}{7}$$

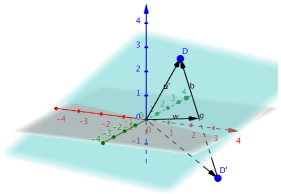
Elle est minimale pour $x = \frac{6}{7}$ et $y = \frac{-4}{7}$ et vaut alors $\frac{32}{7}$.

5.4. Symétries orthogonales

Définition - Symétrie orthogonale

Soient E un espace préhilbertien réel, F un s.e.v de dimension finie de E.
On appelle symétrie orthogonale par rapport à F la symétrie par rapport à F de direction $F^\perp$.
On a $s_F = 2p_F - Id_E$ où p_F est la projection orthogonale sur F.

Représentation - Réflexion dans l'espace



Proposition - CNS de symétrie orthogonale

$s \in \mathscr{L}(E)$ est une symétrie orthogonale si et seulement si

$$s \circ s = Id_E$$
$$\text{Ker}(s - Id_E) \perp \text{Ker}(s + Id_E)$$

Démonstration

Les espaces qui définissent toute symétrie vectorielle sont $\text{Ker}(s - id_E)$ et $\text{Ker}(s + id_E)$.
La symétrie est orthogonale ssi ces espaces sont orthogonaux.
□

Définition - Réflexion

On appelle réflexion toute symétrie orthogonale par rapport à un hyperplan de E.

6. Hyperplans vectoriels et affines d'un espace euclidien

6.1. Lemme de RIESZ

Proposition - Caractérisation des formes linéaires

Soient E un espace euclidien et $\phi \in E^* = \mathscr{L}(E, \mathbb{R})$.
Alors il existe un unique $a \in E$ tel que

$$\forall x \in E, \phi(x) = \langle a \,|\, x \rangle.$$

Démonstration

Si $\phi \in E^*$, alors $\text{Ker}\,\phi$ est un hyperplan.
Donc $(\text{Ker}\phi)^\perp$ est de dimension 1. Notons a, un vecteur directeur de $(\text{Ker}\phi)^\perp$ On a donc $E = \text{Ker}\,\phi \oplus \text{vect}a$ avec $a \neq 0$.

$$\forall\, x \in E, \exists\, (y, \lambda_x) \in \text{Ker}\,\phi \times \mathbb{K} \mid x = y + \lambda_x a$$

Dans ce cas :

$$\phi(x) = \phi(y) + \lambda_x \phi(a) = \lambda_x \phi(a) \qquad \text{et} \qquad \langle a \,|\, x \rangle = \langle a \,|\, y \rangle + \lambda_x \|a\|^2 = \lambda_x \|a\|^2$$

Ainsi, $\phi(x) = \frac{\phi(a)}{\|a\|^2}\langle a \,|\, x \rangle$ En prenant $A = \frac{\phi(a)}{\|a\|^2} a$, on obtient $\phi(x) = \langle A \,|\, x \rangle$, pour tout $x \in E$. □

Heuristique - Principe de construction

Ici on a :

0. Un espace ambiant, euclidien donc muni d'un produit scalaire de référence.
1. Une forme linéaire $f \in E^*$
2. Alors il existe $a \in E$ tel que $f : x \mapsto \langle a \,|\, x \rangle$

Corollaire - Equation de H et vecteur normal

Soient $\mathscr{B}$ une b.o.n de E euclidien et H un hyperplan de E.
Alors il existe $(a_1, \ldots, a_n) \in \mathbb{R}^n$ tel que $\sum_{i=1}^{n} a_i x_i = 0$ soit l'équation de H dans $\mathscr{B}$ et dans ce cas $a \in E$ de coordonnées $(a_1, \ldots, a_n)$ dans $\mathscr{B}$ est un vecteur normal à H, $H = \text{vect}(a)^\perp$.

Exemple - Gradient
Si $f:\mathbb{R}^p\to\mathbb{R}$, différentiable, on a

$$\mathrm{d}f:\mathbb{R}^p\to(\mathbb{R}^p)^*,\qquad x\mapsto\big(a\mapsto=f(x+a)-f(x)+o(\|a\|)\big)$$

Alors, il existe un vecteur $\overrightarrow{grad}(f)(x)$ tel que $\mathrm{d}f(x)(a)=\langle\overrightarrow{grad}(f)(x)\,|\,a\rangle$.
C'est le vecteur dont les coordonnées sont $\dfrac{\partial f}{\partial x_i}(x)$.

6.2. Espace affine euclidien (élargissement vers l'affine)

Vecteur normal

Proposition - Vecteur normal à un hyperplan affine
Soit $\mathscr{R}=(\Omega,e_1,\dots,e_n)$ un repère affine orthonormal de l'espace E de dimension n (c'est-à-dire que $\mathscr{B}=(e_1,\dots,e_n)$ est une b.o.n de E).
Soit $\mathscr{H}$ un hyperlpan affine de E.
On appelle vecteur normal à $\mathscr{H}$, tout vecteur normal à la direction H de $\mathscr{H}$, c'est-à-dire $a\in E$ tel que $H=\mathrm{vect}(a)^\perp$.
Si a a pour coordonnées $(a_1,\dots,a_n)$ dans $\mathscr{B}$, alors $\mathscr{H}$ possède une équation dans $\mathscr{R}$ du type $\sum_{i=1}^n a_i x_i=h$.
Réciproquement

$$\sum_{i=1}^n a_i x_i=h \text{ avec } (a_1,\dots,a_n)\neq(0,\dots,0)$$

est l'équation d'un hyperlpan affine de vecteur normal a de coordonnées $(a_1,\dots,a_n)$ dans $\mathscr{B}$.

Démonstration
Il suffit d'écrire ce que cela signifie □

Exemple - Dans $\mathbb{R}^2$ et $\mathbb{R}^3$
On retrouve ainsi les exemples classiques dans $\mathbb{R}^2$ et $\mathbb{R}^3$:
- Dans le plan euclidien $\mathbb{R}^2$, $ax+by+c=0$, avec $(a,b)\neq(0,0)$, est l'équation dans un repère orthonormal d'une droite de vecteur normal de coordonnées (a,b).
- Dans l'espace euclidien $\mathbb{R}^3$, $ax+by+cz+d=0$, avec $(a,b,c)\neq(0,0,0)$, est l'équation dans un repère orthonormal d'un plan de vecteur normal de coordonnées (a,b,c).

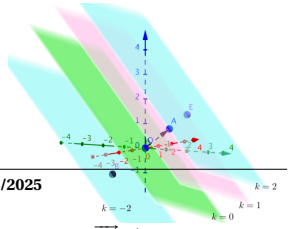
Corollaire - Ligne de niveau : hyperplan
Dans E euclidien, les lignes de niveau de l'application $M\mapsto\overrightarrow{AM}\cdot\vec{n}$ (c'est-à-dire les ensembles $E_k=\{M\in E\,|\,\overrightarrow{AM}\cdot\vec{n}=k\}$) sont des hyperplans affines de vecteur normal $\vec{n}$.

Démonstration
Soit $M_0\in E_k$. Alors

$$M\in E_k\iff\overrightarrow{AM}\cdot\vec{n}=\overrightarrow{AM_0}\cdot\vec{n}\iff(\overrightarrow{AM}-\overrightarrow{AM_0})\cdot\vec{n}=0\iff\overrightarrow{M_0M}\cdot\vec{n}=0$$

Ainsi E_k est l'hyperplan affine normal à $\vec{n}$ et passant par M_0. Est-ce que M_0 existe bien? oui
Prenons $M_0=A+\frac{k}{\|n\|}\vec{n}$, alors $\overrightarrow{AM_0}\cdot\vec{n}=\frac{k}{\|n\|}\vec{n}\cdot\vec{n}=k$. □

Représentation - Les lignes de niveaux - hyperplan



$E_k=\{M\in E\,|\,\overrightarrow{AM}\cdot\vec{n}=k\}$

Distance

Proposition - Distance à un hyperplan affine
Soit $\mathscr{H}$ un hyperplan affine de E euclidien, défini par un point A et un vecteur normal unitaire $\vec{n}$. Alors, pour M point de E, on a

$$d(M,\mathscr{H})=|\overrightarrow{AM}\cdot\vec{n}|.$$

Démonstration
On revient à un hyperplan vectoriel en translatant la relation par $\overrightarrow{OA}$.
Autrement écrit, l'hyperplan vectoriel directeur de $\mathscr{H}$ et $H=\mathrm{vect}(\vec{n})^\perp$. On a alors

$$d(M,\mathscr{H})=d(\overrightarrow{AM},H)=\|\overrightarrow{AM}-p_H(\overrightarrow{AM})\|$$

Comme $\vec{n}$ est normal et unitaire à H, $p_H(\overrightarrow{AM})=\overrightarrow{AM}-\frac{1}{\|\vec{n}\|^2}(\overrightarrow{AM}\cdot\vec{n})\vec{n}$.
On trouve donc

$$d(M,\mathscr{H})=\frac{|\overrightarrow{AM}\cdot\vec{n}|}{\|\vec{n}\|^2}\|\vec{n}\|$$

Et si $\vec{n}$ est unitaire :

$$d(M,\mathscr{H})=|\overrightarrow{AM}\cdot\vec{n}|$$

□

Corollaire - Distance à une droite du plan
Soit $\mathscr{D}$ d'équation $ax+by+c=0$ dans un r.o.n du plan euclidien $\mathbb{R}^2$ et $M(x_M,y_M)$ un point. Alors

$$d(M,\mathscr{D})=\frac{|ax_M+by_M+c|}{\sqrt{a^2+b^2}}.$$

Corollaire - Distance à un plan de l'espace
Soit $\mathscr{P}$ d'équation $ax+by+cz+d=0$ dans un repère orthonormé de l'espace euclidien $\mathbb{R}^3$ et $M(x_M,y_M,z_M)$ un point. Alors

$$d(M,\mathscr{P})=\frac{|ax_M+by_M+cz_M+d|}{\sqrt{a^2+b^2+c^2}}.$$

Démonstration
Dans le premier cas, un vecteur normal à $\mathscr{D}$ est $\frac{1}{\sqrt{a^2+b^2}}(a,b)$
et considérons $A(x_0,y_0)$ un point de $\mathscr{D}$ (donc $ax_0+by_0+c=0$). Alors

$$d(M,\mathscr{D})=|\overrightarrow{AM}\cdot\vec{n}|=\frac{1}{\sqrt{a^2+b^2}}|(x_M-x_0,y_M-y_0)\cdot(a,b)|=\frac{|ax_M+by_M+c|}{\sqrt{a^2+b^2}}$$

Dans le second cas, un vecteur normal à $\mathscr{P}$ est $\frac{1}{\sqrt{a^2+b^2+c^2}}(a,b,c)$
et considérons $A(x_0,y_0,z_0)$ un point de $\mathscr{P}$ (donc $ax_0+by_0+cz_0+d=0$). Alors

$$d(M,\mathscr{D})=|\overrightarrow{AM}\cdot\vec{n}|=\frac{1}{\sqrt{a^2+b^2+c^2}}|(x_M-x_0,y_M-y_0,z_M-z_0)\cdot(a,b,c)|=\frac{|ax_M+by_M+cz_M+d|}{\sqrt{a^2+b^2+c^2}}$$

□

Exercice
Reprendre l'exercice du calcul de distance de $a=(2,2,0)$ à $F=\mathrm{vect}\big((1,1,2),(1,-1,1)\big)$.

Correction
On alors $w=(1,1,2)\wedge(1,-1,1)=(3,1,-2)$, normal à F, qui a pour équation : $3x+y-2z=0$.
Donc $d(a,F)=\dfrac{|3\times2+2-2\times0|}{\sqrt{9+1+4}}=\dfrac{8}{\sqrt{14}}=\dfrac{4\sqrt{14}}{7}$.
On vérifie que $d(a,F)^2=\dfrac{64}{14}=\dfrac{32}{7}$

6.3. Transposition

Un question posée il y a quelques temps : on sait passer de $M=\mathscr{M}_{\mathscr{B}}(u)$ à ${}^tM$. Mais à quel endomorphisme associer alors ${}^tM$?

Définition - Adjoint de $u \in \mathscr{L}(E)$
Soit E un espace euclidien.
Soit $u \in \mathscr{L}(E)$.
Il existe une unique application, noté ${}^t u \in \mathscr{L}(E)$ (parfois u^*) tel que

$$\forall\ x, y \in E, \qquad \langle u(x) \,|\, y\rangle = \langle x \,|\, {}^t u(y)\rangle$$

On appelle cet application u^*, l'adjoint de u.

Démonstration
${}^t u : y \mapsto a$ tel que $\forall\ x \in E, \varphi(x) = \langle u(x) \,|\, y\rangle = \langle a \,|\, x\rangle$. □

Analyse - Interprétation matricielle
Si $\mathscr{B}$ est une base orthonormée de E.
X, Y et U les matrices de x, y et u dans $\mathscr{B}$, respectivement.
Alors

$$\langle u(x) \,|\, y\rangle = (UX)^T \times Y = X^T (U^T Y) = \langle x \,|\, {}^t u(y)\rangle$$

Donc U^T est la matrice de ${}^t u$ dans la base $\mathscr{B}$ orthonormée.
Remarque - S'il n'y a pas de base orthonormée
On en construit une ! cf. partie suivante

6.4. Crochet de dualité

On commence par élargir la notion de produit scalaire.

Définition - Forme bilinéaire non dégénérée
Soit E, F deux espaces vectoriels.
On dit que la forme bilinéaire $B : E \times F \to \mathbb{R}$ est non dégénérée si

$$\begin{aligned}(\forall\ x \in E, B(x,y) = 0) &\Rightarrow y = 0\\ (\forall\ y \in E, B(x,y) = 0) &\Rightarrow x = 0\end{aligned}$$

Exercice
Montrer que tout produit scalaire définie sur E une forme bilinéaire non dégénérée

Correction
On a :

$$\forall\ y \in E \langle x \,|\, y\rangle = 0 \Rightarrow \langle x \,|\, x\rangle = 0 \Rightarrow x = 0$$

Définition - Crochet de dualité
Soit E un $\mathbb{R}$ espace vectoriel. On suppose que E est de dimension finie
On appelle crochet de dualité de E la forme bilinéaire non dégénérée :

$$B : E^* \times E \to \mathbb{R}, \qquad (\varphi, x) \mapsto \varphi(x)$$

Pour aller plus loin - Cas E non de dimension finie
On peut généraliser au cas E de dimension non finie.
On généralise aussi parfois aux espaces topologiques

Exercice
Montrer qu'il s'agit bien d'une forme bilinéaire non dégénérée.

Correction

$$B(\lambda\varphi + \mu\psi, x) = \lambda\varphi(x) + \mu\psi(x) = \lambda B(\varphi, x) + \mu B(\psi, x)$$
$$B(\varphi(\lambda x + \mu y) = \varphi(\lambda x + \mu y) = \lambda\varphi(x) + \mu\varphi(y) = \lambda B(\varphi, x) + \mu B(\varphi, y)$$

Puis :

$$\forall\ x \in E, B(\varphi, x) = 0 \Rightarrow \forall\ x \in E, \varphi(x) = 0 \Rightarrow \varphi = 0$$
$$\forall\ \varphi \in E, B(\varphi, x) = 0 \Rightarrow x = 0$$

En prenant $\varphi : z = \lambda$, si $z = \lambda x + y$, avec $y \in G$ tel que $E = \text{vect}(x) \oplus G$.

Heuristique - Principe de construction/d'application
On a :
0. Un espace vectoriel (ambiant - de dimension finie)
1. Un isomorphisme de E^* sur E, note Φ.
2. On définit alors B, crochet de dualité : $B(f, x) = f(x)$
En fait : $B(f, x) = \langle \Phi(f) \,|\, x\rangle$

On définit alors comme précédemment

Définition - Orthogonal dual
Soit A un sev de E. On note $A^0 = \{\varphi \in E^* \mid \forall\ x \in A, B(\varphi, x) = \varphi(x) = 0\}$.
Soit C un sev de E^*. On note $C^0 = \{x \in E \mid \forall\ \varphi \in C, B(\varphi, x) = \varphi(x) = 0\}$

Application - Mécanique quantique
En mécanique quantique, on définit les `bra-ket` de cette façcon.
Un `bra` noté $<\varphi|$ est une forme linéaire, on considère ensuite ensuite une observable A et un `ket`, noté $|x>$ est un vecteur de l'espace de Hilbert ambiant : $<\varphi|A|x>$.
Exercice
On suppose que E est de dimension finie n. Si $(e_1, \cdots, e_p)$ base de A, complétée en $(e_1, \cdots, e_n)$ base de E.
Donner une caractéristique avec les applications e_i^* de A^0. En déduire $\dim(A^0)$.

Correction

$$\varphi \in A^0 \Longrightarrow \forall\ i \in \mathbb{N}_p \varphi(e_i) = 0 \Longrightarrow \varphi \in \text{vect}(e_{p+1}^*, \ldots e_n^*)$$

Donc $\dim(A^0) = n - p = \dim E - \dim A$

7. Bilan

Synthèse

- ⇝ Avec un produit scalaire, il est simple d'obtenir (=voir numériquement) les dépendances entre vecteurs, d'après l'inégalité de Cauchy-Schwarz.
  Cela donne aussi un moyen explicite de projeter (orthogonalement) sur des sous-espaces vectoriels.
- ⇝ Il est donc bon de savoir reconnaitre les produits scalaires abstraits (et les normes associés), puis les bases orthonormées associées (ou bien les créer directement par l'algorithme de Gram-Schmidt).
- ⇝ La projection orthogonale et donc le calcul de distance deviennent explicite (i.e. calculatoire). Cette méthode nous inspire pour créer une dualité entre espace vectoriel E de dimension finie et son espace dual E^*, par $(\varphi(\in E^*), x) := \varphi(x)$. Au passage on donne également un sens à l'endomorphisme dont la matrice est la transposée de celle de u.

Savoir-faire et Truc & Astuce du chapitre

- — Savoir-faire - Montrer qu'on a un produit scalaire
- — Savoir-faire - Montrer qu'on a une norme
- — Savoir-faire - Montrer qu'on une norme est euclidienne
- — Savoir-faire - Orthonormaliser une base
- — Savoir-faire - Montrer qu'une famille est une base orthonormée
- — Savoir-faire - Changement de base pour une forme bilinéaire
- — Savoir-faire - Minimiser une forme quadratique

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\langle\cdot\vert\cdot\rangle$	Produit scalaire sur E	Forme bilinéaire définie positive	Autre notation classique : $(\cdot,\cdot)$ …
$\Vert\cdot\Vert$	Norme sur E	A valeurs dans $\mathbb{R}_+$, pseudo-linéaire, vérifiant l'inégalité triangulaire $x \mapsto \sqrt{\langle x\vert x\rangle}$ est une norme associée, dite euclidienne Propriété de C-S : $\langle x\vert y\rangle \leqslant \Vert x\Vert \times \Vert y$	Autre notation : $N(\cdot)$.
$x \perp y$	x et y sont orthogonaux	Equivalente à $\langle x\vert y\rangle = 0$	Relation symétrique
$F \perp G$	F et G sont orthogonaux	Equivalente à $\forall\ x \in F, y \in G, \langle x\vert y\rangle = 0$	Relation symétrique
$F^\perp$	L'orthogonal de F	$F^\perp = \{y \in E \mid \forall\ x \in F \langle x\vert y\rangle = \}0$	Si E est de dimension finie, $E = F^\perp \oplus F$
$A = (\langle e_i\vert e_j\rangle)_{i,j}$	Matrice euclidienne de la famille (e_i)	$(e_i)_i$ base orthonormée de E ssi A, positive, définie. A est alors inversible	A est nécessairement symétrique
		$\langle x\vert y\rangle = X^T \times A \times Y$ (avec $x = \sum_{i=1}^{n} X_i e_i$)	Comme la matrice de variance-covariance…
$d(x,A) = \inf_{z\in A} \Vert x - z\Vert$	Distance de x à l'ensemble A	Si $\Vert\cdot\Vert$ est euclidienne, $d(x,A) = \Vert x - p_A(x)\Vert$ (projection orthogonale sur A)	A savoir démontrer!
${}^t u$	Adjoint de u (existe nécessairement si E de dimension finie)	$\forall\ x, y \in E, \langle u(x)\vert y\rangle = \langle x\vert {}^t u(y)\rangle$	Parfois noté u^*
		$\mathcal{M}_{\mathcal{B}on}({}^t u) = \left(\mathcal{M}_{\mathcal{B}on}(u)\right)^T$	
$A^0 = \{\varphi \in E^* \mid \forall\ x \in A, \varphi(x) = 0\}$	Dual de A (pour $A \subset E$)		A^0 est isomorphe à un supplémentaire de A dans E
$C^0 = \{x \in E \mid \forall\ \varphi \in C, \varphi(x) = 0\}$	Dual de C (pour $C \subset E^*$)		C^0 est isomorphe à un supplémentaire de C dans E^*

Retour sur les problèmes

131. Cours
132. Cours : $p_F(u) = \sum_{i=1}^{p} \langle u, e_i\rangle e_i$ si $(e_1, e_2, \ldots, e_n)$ base orthonormale de F.
133. C'est tout simplement $G = F^\perp$.
134. $a_k = \langle u, e_k\rangle$ si $(e_1, \ldots e_n)$ base orthogonale de E et e_k normé.
135. Il suffit d'orthonormaliser une base quelconque par le procédé de Gram-Schmidt.
136. Question plus subtile. On exploite les espaces othogonaux définies à partir d'une forme linéaire. C'est ce qu'on appelle la dualité.

Sixième partie

Combinatoire et groupe fini

Chapitre 28

Dénombrement (combinatoire)

Résumé -

L'expérience montre que ce chapitre peut parfois rester opaque. Or il y a une première clé : pour réussir un bon dénombrement, il faut toujours commencer par une bonne description des choses. Dans un premier temps, nous allons réfléchir à ce que cela signifie. Nous verrons ensuite la seconde clé : il y a trois méthode classique de dénombrement : la bijection entre ensembles, la réunion d'ensembles, le produit cartésien d'ensembles.
Puis nous appliquerons ces méthode pour résoudre quelques cas pratiques. Dans ce chapitre, nous ferrons beaucoup d'exercices pour bien stabiliser les notions introduites et les méthodes présentées

Sommaire

1. Problèmes : expérience, modélisation et ensembles . . . 570
1.1. Questionnement . . . 570
1.2. Expériences réelles et modélisation . . . 571
2. Ensembles finis . . . 572
2.1. Cardinal d'un ensemble . . . 572
2.2. Dénombrement par applications . . . 574
2.3. Dénombrement par calcul du cardinal d'une réunion. Addition. . . . 575
2.4. Dénombrement par calcul du cardinal d'un produit cartésien. Multiplication. . . . 576
3. Listes et combinaisons . . . 577
3.1. Définitions des différents types d'ensemble . . . 577
3.2. Dénombrement d'un ensemble de listes avec répétition . . . 578
3.3. Dénombrement de permutation d'un ensemble E . 579
3.4. Dénombrement d'un ensemble de p-listes sans répétition . . . 580
3.5. Dénombrement d'un ensemble de sous-ensemble à p éléments (combinaison) . . . 581
3.6. Propriétés du coefficient binomial (rappels) . . . 582
4. Exercices d'applications . . . 583
4.1. Tableau des dénombrements classiques . . . 583
4.2. Coefficient multinomial . . . 584
4.3. Séries génératrices . . . 585
5. Bilan . . . 589

Histoire - Actualité de la combinatoire
La combinatoire (ou dénombrement) est une des plus vieille branche des mathématiques. Il s'agit toujours de compter le nombre d'éléments d'un ensemble fini vérifiant une certaine (famille de) propriété(s).
Et pourtant, il s'agit d'un domaine de recherche toujours très actif. On y trouve régulièrement des nouvelles méthodes! Et surtout, beaucoup de résultat de combinatoire s'applique facilement en géométrie. Parfois présentée comme ludique, la combinatoire est une partie des mathématiques les plus exposée à l'application.
Ici nous nous contenterons des premières règles (de jeune Padawan)

1. Problèmes : expérience, modélisation et ensembles

1.1. Questionnement

Exercice
1. Combien de mots de cinq lettres (compréhensibles ou non) existe-t-il en utilisant l'alphabet usuel ?
2. Xavier part en vacances aux États-Unis. Avant de rentrer, il décide d'écrire une carte à chacun de ses meilleurs amis : Arthur, Brigitte, Claude, Dominique et Emeric. Il se précipite chez le vendeurs de cartes postales, qui possèdent 26 modèles de cartes différents. Xavier se demande combien de possibilités il a pour envoyer des cartes postales à ses amis .

Correction
1. Si l'on considère un mot de 5 lettres, on a 26 possibilité pour le choix de la première lettre, 26 pour le choix de la seconde... et 26 encore pour le choix de la dernière.
Le nombre de mots possible est $26\times26\times26\times26\times26=26^5(=11881376)$
2. Pour choisir la carte d'Arthur, Xavier à 26 possibilité et ce choix n'a aucune influence sur le choix de celle de Brigitte (ni de celle de Claude, de Dominique et Emeric). A chaque fois, les possibilités sont identiques : 26.
Là encore, au final, Xavier a donc un nombre de possibilité égal à 26^5.

Analyse - Pourquoi trouve-t-on le même résultat ?
Tout simplement parce qu'il s'agit du même problème. En effet, on peut considérer l'application suivante

$$\begin{array}{ccc}\{\text{Ensemble des lettres de l'alphabet}\} & \xrightarrow{\Phi} & \{\text{Ensemble des cartes postales}\}\\ a & \longmapsto & \text{La première carte postale}\\ \vdots & & \vdots\\ z & \longmapsto & \text{La dernière carte postale}\end{array}$$

Φ *est bijective* (même cardinal) et envoie le premier problème sur le second. En effet, tout mot de 5 lettres (dont les positions sont précises) a pour image par Φ une association de 5 cartes postales possibles (avec des positions précises).
Existe-t-il un **représentant** de l'ensemble de tous ces problèmes identiques?
Oui, c'est le problème de la création d'un ensemble de 5 éléments, ordonnés, à partir d'un ensemble de 26 éléments ; ces éléments pouvant être répétés.

Analyse - Quelles sont les informations importantes dans ces problèmes?
Quelques questions sont nécessaires
1. Combien existe-t-il d'éléments dans l'ensemble des objets que l'on peut prendre?
2. Combien d'objets doit-on retirer?
3. Est-il possible de prendre ces éléments plusieurs fois ou non?
4. Lorsque l'on décrit l'ensemble des solutions possibles, faut-il considérer que les solutions sont différentes si on permute les objets?

Pour ces quatre questions les réponses sont les mêmes dans les deux exercices précédents :
1. 26
2. 5
3. oui (on peut prendre plusieurs fois des objets)
4. oui (les solutions sont différentes si l'on permute les objets), dans ce cas on dit que les solutions sont ordonnées.

Pouvez-vous faire quatre exercice où les réponses aux deux premières questions sont les mêmes (26 et 5 respectivement) et où celles aux deux secondes sont différentes?
Exercice 1 (non, oui)
C'est le cas où le magasin de cartes postales ne possède qu'un exemplaire de chacune des cartes postales, ou si Xavier ne souhaite pas envoyer la même carte à deux personnes au cas où ils les comparent.

Exercice 2(oui, non)
Xavier envoie cinq cartes à une même personne (à plusieurs jours d'intervalle), mais pour des raison de grève de la poste, la personne reçoit les cinq carte en même temps sans savoir l'ordre d'envoi des cartes. *Pour cette personne* (qui reçoit les cartes) les possibilités sont moindres (combien ?)

Exercice 3(non, non)
C'est le cas où le magasin de cartes postales ne possède qu'un exemplaire de chacune des cartes postales, Xavier envoie cinq cartes à une même personne (à plusieurs jours d'intervalle), mais pour des raison de grève de la poste, la personne reçoit les cinq carte en même temps sans savoir l'ordre d'envoi des cartes. *Pour cette personne* (qui reçoit les cartes) les possibilités sont moindres (combien ?)

Exercice 4(non, oui)
C'est celui de l'énoncé.

1.2. Expériences réelles et modélisation

Là encore des exercices vont nous aider à comprendre la méthode générale employée pour dénombrer des ensembles (ou avec le langage probabiliste : événements possibles).
Il est nécessaire là de bien faire la différence entre les ensembles et les listes!

Exercice
Boules tirées dans une urne
On considère une urne composée de 15 boules, numérotées de 1 à 15.
On en tire 3 avec remise, puis 5 sans remise et enfin une poignée de 4 boules.
Pouvez-vous décrire un exemple donné par une expérience ?
Quelle est la forme de la l'ensemble des résultats possibles ?

Correction
Un exemple : on tire dans l'ordre 2, 4, 2 puis 1, 3, 4, 7, 2 puis l'ensemble $\{10,14,15,5\}$.
L'ensemble des résultats possibles est de la forme :

1. une 3-liste (ordre dans le tirage) à partir de $\mathbb{N}_{15}$ avec répétition possible.
2. une 5 liste (ordre dans le tirage) à partir de $\mathbb{N}_{15}$ sans répétition possible.
3. un sous ensemble de 4 éléments à partir de l'ensemble $\mathbb{N}_{15}$ privé des 5 éléments tirés précédemment

(En fait il s'agit d'un produit cartésien (donc une liste) à partir de ces 3 ensembles)

Exercice
Boules tirées dans une urne (bis)
On considère une urne composée de 15 boules, 5 vertes, 5 bleues et 5 rouges.
On en tire 3 avec remise, puis 5 sans remise et enfin une poignée de 4 boules.
Pouvez-vous décrire un exemple donné par une expérience ?
Quelle est la forme de la l'ensemble des résultats possibles ?

Correction
On peut noter de 1 à 5 les vertes, puis de 6 à 10 les bleues et de 11 à 15 les rouges.
Puis on permute les résultats entre les mêmes couleurs (ce qui n'est pas facile…)

Exercice
Nous lançons deux dés à 6 faces (un rouge, un bleu). Combien de lancers différents existe-il ? Combien de score différents peut-on réaliser en sommant les deux résultats ?

Correction
Pour la première question on s'intéresse à E, mis en bijection avec $F = \mathbb{N}_6 \times \mathbb{N}_6$, l'ensemble des couples obtenues à partir de $\mathbb{N}_6$. Cette bijection est celle qui donne pour chaque lancer le nombre obtenu par le dé rouge, puis le nombre obtenu par le dé bleu.
Pour la seconde question on s'intéresse à E', mis en bijection avec $F' = \{2,3\dots12\}$, l'ensemble des entiers compris entre 2 et 12. Cette bijection est celle qui donne pour chaque lancer la somme des deux dés.
Il n'y a évidemment pas de bijection possible entre F et F' (ou entre E et E', de manière équivalent.

Savoir faire - Méthode : description des expériences
Ce qui nous intéresse c'est de **décrire les résultats possibles** d'une expérience.
C'est souvent une excellente idée de donner un exemple de description et de mesurer au moment de son écriture si nous avons à faire à une liste, un ensemble, des répétitions possibles, comment les paramètres se combinent les uns avec les autres…
On note E, l'ensemble des résultats possibles ; la description de ces expériences permet de préciser la nature de l'ensemble E (ensemble, liste …?)
Enfin, pour dénombrer l'ensemble des résultats possibles, il « suffit » de calculer le cardinal de E

Pour aller plus loin - Deux citations concernant les modèles
« Un modèle est une interprétation abstraite, simplifiée et idéalisée d'un objet du monde réel ou d'une description de la réalité. » David Ruelle.
« La science est la seule activité humaine où le mot "modèle" a le sens inverse de celui que lui donne la langue usuelle. Est modèle ce que l'on imite ou qui mérite d'être imité. Il a avec la réalité le même type de rapport que celui qu'entretient un "modèle réduit" avec l'objet dont il est la reproduction plus aisément manipulable. L'inversion de sens est frappante et mérite d'être méditée... Que la science comme activité consiste essentiellement à se construire des objets sous la forme de modèles est en revanche une vérité incontestable, bien que trop peu connue des non-scientifiques. (...) Le modèle scientifique est une imitation humaine de la nature que le savant prend bientôt pour "modèle" - au sens ordinaire - de celle-ci. » Jean-Pierre Dupuy

Pour aller plus loin - Ensemble ou liste
Nous reprendrons les définitions par la suite.
A avoir en tête, d'ores et déjà :
- *un ensemble est noté entre accolade, les éléments ne se répètent pas et il y a une indifférence à l'ordre :* $\{1,2,3\} = \{3,2,1\} = \{1,1,1,2,2,3\}$
- *une p-liste (ou p-uplet) est noté entre parenthèse, sans précision contraire les éléments peuvent se répéter et l'ordre compte :* $(1,2,3) \neq (1,3,2)$ *ou encore* $(1,2) \neq (1,1,1,2,2)$

2. Ensembles finis

2.1. Cardinal d'un ensemble

Ensemble fini

On rappelle ici des résultats vus en début d'année.

Heuristique - Principe du calcul du cardinal
La notion de cardinal d'un ensemble repose sur le fait suivant :

S'il existe une bijection de $[\![1,p]\!]$ sur $[\![1,n]\!]$ alors $n = p$.

Dénombrer, c'est déterminer le cardinal d'un ensemble fini.
L'ensemble $\mathbb{N}_n$ est le représentant principal de tous les ensembles en bijection avec lui (classe d'équivalence)

Définition - Ensemble fini ou infini
On dit qu'un ensemble non vide E est fini s'il existe $n \in \mathbb{N}^*$ tel que E soit en bijection avec $[\![1,n]\!]$ (i.e. il existe $f : E \to [\![1,n]\!]$ bijective).
Par convention $\emptyset$ est un ensemble fini.
Un ensemble qui n'est pas fini est dit infini.

Cardinal d'un ensemble fini

Proposition - Taille des ensembles
Soient $n, p \in \mathbb{N}^*$.
- S'il existe une application injective $f : [\![1,p]\!] \to [\![1,n]\!]$ alors $p \leqslant n$.
- S'il existe une bijection de $[\![1,p]\!]$ sur $[\![1,n]\!]$ alors $n = p$.

Démonstration
On va démontrer le résultat par récurrence sur $p \in \mathbb{N}^*$.
$\mathscr{P}_p$: « Pour tout $n \in \mathbb{N}$, si il existe une injection de $[\![1,p]\!] \to [\![1,n]\!]$ alors $p \leqslant n$. »
- (Pour tout $n \geqslant 1$.
  Toute fonction de $\{1\}$ dans $\mathbb{N}_n$ est une injection et $n \geqslant 1$.)
  Si $n = 0$, il n'y a pas d'injection. On a $\mathscr{P}_1$ par contraposée.
- Soit $p \in \mathbb{N}$. Supposons que $\mathscr{P}_p$ est vraie.
  Soit $n \in \mathbb{N}$ et supposons que $f : \mathbb{N}_{p+1} \to \mathbb{N}_n$ est injective.
  Notons $r = f(p+1) \in \mathbb{N}_n$ et $\varphi : \mathbb{N}_n \to \mathbb{N}_n$, $s \mapsto \begin{cases} s & \text{si } s \notin \{r,n\} \\ n & \text{si } s = r \\ r & \text{si } s = n \end{cases}$.
  Alors φ est une bijection de $\mathbb{N}_n$, donc est injective. Donc $\psi = \varphi \circ f$ est une injection de $\mathbb{N}_{p+1}$ sur $\mathbb{N}_n$.
  Puis $\psi(p+1) = \varphi \circ f(p+1) = \varphi(f(p+1)) = \varphi(r) = n$ et pour tout $t \in \mathbb{N}_p$, $\psi(t) \in \mathbb{N}_{n-1}$.
  Ainsi on a une injection $\overline{\psi} : \mathbb{N}_p \to \mathbb{N}_{n-1}$, $x \mapsto \psi(x)$. Et donc d'après $\mathscr{P}_p$: $p \leqslant n-1$.
  Par conséquent : $p+1 \leqslant n$. Ainsi $\mathscr{P}_{p+1}$ est vraie.

Puis θ est une bijection de $[\![1,p]\!]$ sur $[\![1,n]\!]$,
alors comme θ est injective : $p \leqslant n$.
et comme θ^{-1} est également injective : $n \leqslant p$.
Ainsi $p = n$.
□

Corollaire - Invariant
Soit E un ensemble. $n, p \in \mathbb{N}$. S'il existe une bijection de E sur $[\![1,n]\!]$ et une bijection de E sur $[\![1,p]\!]$ alors $n = p$.

On peut alors donner la définition suivante :

Définition - Cardinal
Si E est fini, l'élément n de $\mathbb{N}$ tel que E soit en bijection avec $[\![1,n]\!]$, s'appelle le cardinal de E, noté Card E (ou $|E|$, $\sharp(E)$).
On peut alors noter $E = \{x_1, \dots, x_n\}$.
Par convention, Card $\emptyset = 0$.

Remarque - Relation d'équivalence
La relation $\mathscr{R}$ définit sur l'ensemble des ensembles :

$$E \mathscr{R} F \iff \exists\, \varphi : E \to F, \text{ bijective}$$

est une relation d'équivalence (A démontrer!).
Les classes d'équivalence ont pour représentant principaux les ensembles $[\![1,n]\!] = \mathbb{N}_n$.
La fonction Card est une fonction invariante et caractéristique des classes d'équivalence Par transitivité de cette relation d'équivalence :

Proposition - Critère d'égalité des cardinaux
Si E et F sont deux ensembles finis et $f : E \to F$ une bijection, alors Card E = Card F.

Corollaire - Injection
Soit E un ensemble et $n \in \mathbb{N}$. S'il existe une injection de E sur $[\![1,n]\!]$, alors E est fini et card$E \leqslant n$.

Sous-ensembles

Proposition - Sous-ensemble. Critère d'égalité
Tout sous-ensemble A d'un ensemble fini E est fini. On a

Card $A \leqslant$ Card E avec égalité si et seulement si $A = E$.

Démonstration
Soit $\Phi : E \mapsto \mathbb{N}_n$, une bijection. Sa fonction réciproque est notée Φ^{-1}.
On peut écrire $E = \{x_1, x_2, \dots x_n\}$ où $n =$ Card E et $\Phi(x_k) = k$.
L'application $\psi : A \to \mathbb{N}_n$, $x \mapsto k = \Phi(x)$ est injective.
Donc A est nécessairement fini, sinon il existerait une injection d'un ensemble infini sur un ensemble fini.
On note $\Psi_1 : \mathbb{N}_p \to A$, bijective
et de même $B = E \setminus A$ est fini, on note $\Psi_2 : \mathbb{N}_r \to B$ bijective.
Enfin, l'application $\Psi : \mathbb{N}_{p+r} \to E$, $k \mapsto \begin{cases} \Psi_1(k) \in A & \text{si } k \leqslant p \\ \Psi_1(k) \in B & \text{si } k > p \end{cases}$ est une bijection.
Donc Card $(E) = n = p + r =$ Card $(A) +$ Card (B). Et par ailleurs :
Card $(A) =$ Card $(E) \iff r = 0 \iff B = \emptyset \iff A = E$ □

Pour aller plus loin - En langage verbal
*Une méthode additive correspond verbalement à un **OU**.*
*Une méthode multiplicative correspond verbalement à un **ET**.*

Heuristique - Trois types de méthode pour le dénombrement
Ce théorème est fondamental, beaucoup de dénombrements sont basés dessus. On a en fait deux grandes méthodes de dénombrement :
- **Méthode 1 - directe** :
  on montre que E en bijection avec un ensemble de cardinal connu.
- **Méthode 2 - addititve** :
  on écrit E comme une réunion disjointe (partition finie) d'ensembles de cardinaux connus.
- **Méthode 3 - multiplicative** :
  on écrit E comme un produit cartésien d'ensemble de cardinaux connus.

Il arrive aussi que les trois méthodes soient exploitées ensemble dans un même problème

2.2. Dénombrement par applications (entre ensembles finis)

Proposition - Relation entre cardinaux
Soient E, F des ensembles et f une application de E dans F.
- Si f est injective et F fini, alors E est fini
  et Card E = Card $(f(E)) \leqslant$ Card F.
  S'il y a égalité, f est bijective.
- Si f est surjective et E fini, alors F est fini
  et Card F = Card $(f(E)) \leqslant$ Card E.
  S'il y a égalité, f est bijective.

Démonstration
D'abord deux remarques :
- Si f est injective, alors $f(E)$ et E ont même cardinal.
  En effet, si $p =$ Card (E), $\varphi \circ f^{-1} : f(E) \to \mathbb{N}_p$ est bijective.
  $\forall\, y \in f(E), \exists!\, x \in E$ tq $y = f(x)$ (injectivité de f) et $\varphi \circ f^{-1}$ est bijective comme φ.
- Si f est surjective, alors $f(E)$ et F ont même cardinal.
  En effet, tout simplement : $f(E) = F$

Par conséquent, si f est invective, $f(E) \subset F$ et donc Card $E =$ Card $(f(E)) \leqslant$ Card F.
L'égalité des cardinaux assure Card $(E) =$ Card $(f(E)) =$ Card F, donc $F = f(E)$
et f est surjective. On en conclue que f est bijective.
De même si f est surjective, comme Card $F =$ Card $(f(E)) \leqslant$ Card (E),
(cette dernière inégalité est vraie pour tout f),
L'égalité des cardinaux donne Card $(f(E)) =$ Card (E), donc si $x \neq x'$, $f(x) \neq f(x')$,
et ainsi f est nécessairement injective et donc bijective. □

Le théorème suivant est comparable à un théorème donnant une équivalence semblable, lorsque f est un endomorphisme ($\dim(E) = \dim(F)$)

Théorème - Critère d'équivalence
Si E et F sont finis de **même cardinal** et f une application de E dans F, alors

f injective $\iff$ f surjective $\iff$ f bijective.

Savoir faire - Montrer qu'un ensemble est fini
Pour montrer qu'un ensemble E est fini, on peut
- soit montrer que $E \subset F$ avec F fini ;
- soit chercher une injection de E dans F fini. Si de plus on a une bijection et que l'on connait Card F, alors on a Card E.

Savoir faire - Calculer, théoriquement, le cardinal d'un ensemble fini
La fonction caractéristique (ou indicatrice) possède beaucoup d'intêrets :

— elle donne le cardinal d'un ensemble $F \subset E$:

$$\text{Card } F = \sum_{x \in E} \mathbb{1}_F(x)$$

— on a la relation $x \in F \Leftrightarrow \mathbb{1}_F(x) = 1$

2.3. Dénombrement par calcul du cardinal d'une réunion. Addition.

Proposition - Cardinal du complémentaire
Soit A une partie de E fini. Alors

$$\mathbb{1}_{\complement_E(A)} = 1 - \mathbb{1}_A \qquad \text{et} \qquad \text{Card } (\complement_E A) = \text{Card } E - \text{Card } A$$

Démonstration
On exploite la fonction caractéristique.

$$x \in \complement_E(A) \Leftrightarrow \mathbb{1}_A(x) = 0$$

Donc $\mathbb{1}_{\complement_E(A)} = 1 - \mathbb{1}_A$.
Enfin

$$\text{Card } (\complement_E(A)) + \text{Card } (A) = \sum_{x \in E} \mathbb{1}_{\complement_E(A)}(x) + \mathbb{1}_A(x) = \sum_{x \in E} 1 = \text{Card } (E)$$

□

Théorème - Réunion d'ensembles
Soit E un ensemble (non nécessairement fini)

— Soient A, B deux sous-ensembles finis. Alors $A \cup B$ est fini et

si $A \cap B = \emptyset$ alors $\text{Card } (A \cup B) = \text{Card } A + \text{Card } B$

sinon

$$\text{Card } (A \cup B) = \text{Card } A + \text{Card } B - \text{Card } (A \cap B).$$

— Si $A_1, \dots, A_n$ sont des parties deux à deux disjointes de E alors

$$\text{Card } (A_1 \cup \dots \cup A_n) = \text{Card } \Big(\bigcup_{i=1}^{n} A_i \Big) = \sum_{i=1}^{n} \text{Card } A_i$$

Pour aller plus loin - Formule du crible
Soient $n \in \mathbb{N}$ et $E_1, E_2 \dots E_n$, n ensembles finis.
Alors $\bigcup_{k=1}^{n} E_k$ est un ensemble fini,

$$Card\Big(\bigcup_{k=1}^{n} E_k \Big) = \sum_{h=1}^{n} (-1)^{h-1} \sum_{\{i_1 \dots i_h\} \in \binom{\mathbb{N}_n}{h}} \text{Card}(E_{i_1} \cap \dots E_{i_h})$$

En fait cette formule est relativement simple! Le h indique que les ensembles considérés possèdent h éléments!

$$\begin{aligned} \text{Card}\Big(\bigcup_{k=1}^{n} E_k \Big) = {} & \text{Card} E_1 + \text{Card} E_2 + \dots + \text{Card} E_n \\ & - \text{Card}(E_1 \cap E_2) - \text{Card}(E_1 \cap E_3) - \dots \\ & \quad - \text{Card}(E_{n-1} \cap E_n) \\ & + \text{Card}(E_1 \cap E_2 \cap E_3) + \dots \\ & \quad + \text{Card}(E_{n-2} \cap E_{n-1} \cap E_n) \\ & \dots \\ & \pm \text{Card}(E_1 \cap E_2 \cap E_3 \dots E_n) \end{aligned}$$

Savoir faire - Formule du crible
Comme au programme ne figure pas la formule du crible de Poincaré (cas non disjoints des ensembles), il faut donc savoir se remettre toujours dans de telles conditions.
Donc si les (A_i) ne sont pas disjoints deux à deux, on décompose en sous-ensembles disjoints.
(Ou bien on exploite les fonctions caractéristiques)

Démonstration
$x \in A \cap B \Leftrightarrow \mathbb{1}_A(x) = 1$ et $\mathbb{1}_B(x) = 1 \Leftrightarrow \mathbb{1}_A(x) \times \mathbb{1}_B(x) = 1$
Donc $\mathbb{1}_{A \cap B} = \mathbb{1}_A \times \mathbb{1}_B$.
Par passage au complémentaire :

$$\begin{aligned} \mathbb{1}_{A \cup B} = 1 - \mathbb{1}_{\complement_E A \cup B} &= 1 - \mathbb{1}_{\complement_E(A) \cap \complement_E(B)} = 1 - \mathbb{1}_{\complement_E(A)} \times \mathbb{1}_{\complement_E(B)} = 1 - (1 - \mathbb{1}_A) \times (1 - \mathbb{1}_B) \\ &= \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \times \mathbb{1}_B = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_{A \cap B} \end{aligned}$$

Donc en sommant pour tout $x \in E$:

$$\text{Card } (A \cup B) = \text{Card } A + \text{Card } B - \text{Card } (A \cap B)$$

Puis,

$$\text{Card } \Big(\bigcup_{i=1}^{n+1} A_i \Big) = \text{Card } \Big(\bigcup_{i=1}^{n} A_i \Big) + \text{Card } (A_{i+1}) - \text{Card } \left(\Big(\bigcup_{i=1}^{n} A_i \Big) \bigcap A_{i+1} \right)$$

Puis si les ensembles sont disjoints, alors par récurrence, on retrouve la formule annoncée :

$$\forall\, n \in \mathbb{N} \qquad \text{Card } (A_1 \cup \dots \cup A_n) = \text{Card } \Big(\bigcup_{i=1}^{n} A_i \Big) = \sum_{i=1}^{n} \text{Card } A_i$$

□

Exercice

Montrer que $1 - \mathbb{1}_{A_1 \cup A_2 \cdots \cup A_n} = \prod_{i=1}^{n} (1 - \mathbb{1}_{A_i})$.

En déduire la formule du crible de Poincaré

Correction
On a

$$1 - \mathbb{1}_{A_1 \cup A_2 \cdots \cup A_n} = \mathbb{1}_{\overline{A_1 \cup A_2 \cdots \cup A_n}} = \mathbb{1}_{\overline{A_1} \cap \overline{A_2} \cdots \cap \overline{A_n}} = \prod_{i=1}^{n} \mathbb{1}_{\overline{A_i}} = \prod_{i=1}^{n} (1 - \mathbb{1}_{A_i})$$

Si on passe au développement polynomiale de ce produit (k représente le nombre de fois que l'on prend des $\mathbb{1}_{A_i}$) :

$$1 - \mathbb{1}_{A_1 \cup A_2 \cdots \cup A_n} = \sum_{k=0}^{n} 1 \times \sum_{I \subset \binom{\mathbb{N}_n}{k}} \prod_{i \in I} (-1)^k \times \mathbb{1}_{A_i} = \sum_{k=0}^{n} 1 \times (-1)^k \times \sum_{I \subset \binom{\mathbb{N}_n}{k}} \mathbb{1}_{\bigcap_{i \in I} A_i}$$

Si l'on passe à la somme des éléments pour $x \in E$:

$$\text{Card } A_1 \cup A_2 \cdots \cup A_n = \sum_{k=0}^{n} (-1)^{k+1} \times \sum_{I \subset \binom{\mathbb{N}_n}{k}} \text{Card } \left(\bigcap_{i \in I} A_i \right)$$

Rappel :

Définition - Partition
Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties non vides de E. On dit que $(A_i)_{i \in I}$ est une partition de E si

1. $E = \bigcup_{i \in I} A_i$
2. $i \neq j \Rightarrow A_i \cap A_j = \emptyset$

On note $E = \biguplus_{i \in I} A_i$

Remarque - Classes d'équivalence
En début d'année, nous avons déjà rencontré la définition de partition d'un ensemble. Nous avons vu qu'une relation d'équivalence $\mathscr{R}$ sur un ensemble E, « partitionne » cet ensemble en classes d'équivalence qui forme une partition de E.
Si celle-ci sont finies et nombres finis (nécessairement si E est fini) on a alors :

$$\text{Card } (E) = \sum_{x \text{ représentant de } E/\mathscr{R}} \text{Card } (O(x))$$

Proposition - Dénombrement par partition
Si E est un ensemble de cardinal fini et si $(A_i)_{i \in I}$ est une partition de E.
Alors $\text{Card } (E) = \sum_{i \in I} \text{Card } (A_i)$

Pour aller plus loin - Lemme des bergers
Soit $f : E \to F$, surjective tel qu'il existe $k \in \mathbb{N}$ tel que
$\forall\, y \in F$, $card\{f^{-1}(y)\} = k$.
Alors $card(F) = \dfrac{card(E)}{k}$.

2.4. Dénombrement par calcul du cardinal d'un produit cartésien. Multiplication.

Les résultats suivants sont démontrés comme des applications des résultats précédents. Mais il faut bien les voir comme de nouveaux résultats sur lesquels s'appuyer pour faire du dénombrement (de même la multiplication dérive de l'addition, mais lorsqu'on doit calculer 5×7, on ne fait plus $7+7+7+7+7\dots$).

Théorème - Cardinal de produit cartésien
Soient E, F deux ensembles finis avec Card $E = n$, Card $F = p$.
Alors $E \times F$ est fini et

$$\text{Card}\,(E \times F) = \text{Card}\,E \times \text{Card}\,F = np$$

plus généralement si les E_i sont finis

$$\text{Card}\,(E_1 \times \cdots \times E_n) = \text{Card}\,E_1 \times \cdots \times \text{Card}\,E_n.$$

Démonstration
On note $\mathscr{R}_F$, la relation sur $E \times F$ définie par :

$$(x,y)\mathscr{R}_F(x',y') \iff y = y'$$

Alors l'ensemble $E \times F$ est partitionné en Card F classes d'équivalence. Chacune possède exactement Card E éléments.
Donc Card $(E \times F)$ = Card (E) × Card (F).
Puis par récurrence (relativement directe) : Card $(E_1 \times \cdots \times E_n)$ = Card $E_1 \times \cdots \times$ Card E_n □

Pour aller plus loin - Principe des bergers
Dans la littérature mathématiques classiques, on parle ici du principe des bergers. Cela s'écrit : Soit $f : X \to Y$, surjective. Supposons que Card $Y = q$ et pour tout $y \in Y$, $f^{-1}(y)$ est de cardinal p.
Alors X est de cardinal $p \times n$.
Saurez-vous voir le lien ? On l'appelle aussi parfois dans ce cours, le principe de décomposition

Savoir faire - Quand est-ce que l'on voit apparaître un produit cartésien ?
Dans les exercices, lorsque l'on peut dire on tire PUIS on tire (à nouveau) PUIS … on tire (une dernière fois), alors c'est que l'on est en train de créer une liste des résultats.
Cela correspond exactement à notre modèle.
Ainsi de manière générale, dès qu'il y a PUIS, on effectue une MULTIPLICATION.

3. Listes et combinaisons

Dans cette partie, nous appliquons essentiellement le troisième principe (celui du produit, ou de décomposition) pour dénombrer quelques situations fréquentes. On commence par les définir, puis on se concentre sur chacune.

3.1. Définitions des différents types d'ensemble

Définition - Liste, permutation, combinaison
Soit E un ensemble. On appelle
- p-liste (ou p-uplet) d'éléments de E tout élément de E^p ;
- permutation de E (E fini) toute bijection de E sur E ;
- combinaison à p éléments de E (E fini) toute partie (ensemble) à p éléments de E.

Exemple - de 2-listes sans répétition
Les 2-listes sans répétition de $\{1;2;3;4\} = \mathbb{N}_4$ sont : (1;2), (2;1), (1;3), (3;1), (1;4), (4;1), (2;3), (3;2), (2;4), (4;2), (3;4) et (4;3).
On constate qu'elles sont au nombre de $12 = 4 \times 3$.

Exemple - de combinaison à 2 éléments à partir de $\mathbb{N}_4$
Les combinaison à 2 éléments de $\{1;2;3;4\} = \mathbb{N}_4$ sont : $\{1;2\}, \{1;3\}, \{1;4\}, \{2;3\}, \{2;4\}, \{3;4\}$.
On constate qu'elles sont au nombre de $6 = \frac{12}{2}$.

Remarque - Vocabulaire
On parle aussi parfois de p-uplet au lieu de p-liste.
Une 2-liste (ou 2-uplet) s'appelle un couple.
Une 3-liste (ou 3-uplet) s'appelle un triplet…

3.2. Dénombrement d'un ensemble de listes avec répétition

Comme une p-liste (avec répétition possible) est un élément du produit cartésien E^p, on peut affirmer (même si cela est la répétition de 2.4.) :

Théorème - Nombre de p-liste (répétition possible)
Soit E un ensemble fini de cardinal n.
Le nombre de p-listes d'éléments de E est $n \times n \times \cdots \times n = n^p$.
Le nombre de p-listes, élément de $E_1 \times E_2 \times \cdots E_p$ est Card $E_1 \times \cdots \times$ Card E_p

Exemple - Trajets !
Les localités X et Y sont reliés par trois routes : a, b et c.
Les localités Y et Z sont reliés par deux routes : d et e.
Combien existe-t-il de trajets de X à Z passant par Y ?
Un tel trajet est repéré par un couple (r_1, r_2) où r_1 est la route prise pour aller de X à Y et r_2 de Y à Z.
Donc $r_1 \in \{a,b,c\}$ et $r_2 \in \{d,e\}$. Donc $(r_1, r_2) \in \{a,b,c\} \times \{c,d\}$.
Il y a donc $3 \times 2 = 6$ trajets possibles.

Exercice
Combien de mots différents de 7 lettres alternant consonnes et voyelles peut-on former
1. si la première lettre est une consonne ?
2. si la première lettre est une voyelle ?

Correction
Notons V, l'ensemble des voyelles et C l'ensemble des consonnes.
Alors Card$V = 6$ et Card$C = 20$.
1. Dans ce cas un mot sera exactement une 7-liste de $C \times V \times C \times V \times C \times V \times C$.
   Il y a donc $20 \times 6 \times 20 \times 6 \times 20 \times 6 \times 20 = 20^4 \times 6^3 = 160\,000 \times 216 = 34\,560\,000$
2. Dans ce cas un mot sera exactement une 7-liste de $V \times C \times V \times C \times V \times C \times V$.
   Il y a donc $6^4 \times 20^3 = 1\,296 \times 8\,000 = 10\,368\,000$

Exercice
Un piano à queue à 88 touches. De combien de manières différentes peut-on jouer une mélodie de 7 sons consécutifs ?

Correction
Il s'agit de compter le nombre de 7-liste avec répétitions possibles à partir d'un ensemble de 88 éléments.
Il y a donc maintenant 88^7 mélodies différentes.

Attention - p^n ou n^p ?
Ce cours sur le dénombrement est composé de nombreux résultats à connaître.
L'expérience montre que lorsque l'élève n'a pas bien compris les résultats, mais juste appris les formules en temps voulu, il ne les connaît plus plus tard dans l'année, et en particulier au moment du concours.
Comprenez bien qu'il s'agit de choisir ici, une touche de piano : 88 choix, puis une autre : encore 88 choix …. Finalement, il y a 88^7 choix mélodies possibles.
Dans la partie précédente : il s'agissait de choisir ici, une touche de piano : 88 choix, puis une autre différente : 87 choix …. Finalement, il y a $88 \times 87 \times \ldots 82$ choix de mélodies possibles.
Autrement dit : *si vous avez un doute sur la formule, REFLECHISSEZ!*

Théorème - Nombre d'applications
Soient E, F deux ensembles finis avec Card $E = n$, Card $F = p$.
Alors $\mathscr{F}(E,F)$ est fini et

$$\text{Card}\,\mathscr{F}(E,F) = (\text{Card}\,F)^{\text{Card}\,E} = p^n.$$

Et $\mathscr{P}(E)$ est fini et
$$\text{Card}\,\mathscr{P}(E) = 2^{\text{Card}\,E} = 2^n.$$

Démonstration
Pour le comprendre, il suffit de noter $E = \{x_1, x_2 \dots x_p\}$ le premier ensemble.
Une application f de E dans F correspond exactement à l'ensemble des couples : $\Big\{\big(x_1, f(x_1)\big), \big(x_2, f(x_2)\big) \dots \big(x_n, f(x_n)\big)\Big\}$ ou encore, puisque les x_i sont classés :
une application est une p-liste $(f(x_1), f(x_2) \dots, f(x_n))$ où chaque $f(x_i) \in F$ n'est pas nécessairement unique.
Il s'agit donc bien d'un arrangement de p éléments (avec répétitions) à partir de F.
□

Exercice
Soit E un ensemble de n éléments.
Démontrer que le nombre de sous-ensembles de E est 2^n.

Correction
Les sous-ensembles de E correspondent exactement aux applications de E dans $\{0,1\}$.
La correspondance est obtenu par la *fonction caractéristique*. A tout sous-ensemble E' de $E.$, on associe la fonction
$$\mathbb{1}_{E'} : \begin{array}{ccc} E & \longrightarrow & \{0,1\} \\ x & \longmapsto & \begin{cases} 0 & \text{si } x \notin E' \\ 1 & \text{si } x \in E' \end{cases} \end{array}.$$

3.3. Dénombrement de permutation d'un ensemble E

Analyse - Représentation d'une permutation
Considérons l'ensemble $E = \{a, b, c, d, e\}$ à 5 éléments.
Une permutation de E est donc une bijection φ de E dans E.
Alors $\varphi(a) \in E$, $\varphi(b) \in E \dots$ et $\varphi(e) \in E$ et ces cinq images sont toutes différentes, sinon l'application ne serait pas injective.
On peut alors représenter φ de la manière suivante (par exemple) :
$$\begin{array}{ccccccc} & a & b & c & d & e \\ \varphi & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & a & d & e & c & b \end{array}$$
ou encore plus simplement : $\varphi(a,b,c,d,e) = (a,d,e,c,b)$
D'où la proposition suivante (qui explique mieux le nom)

Proposition - Permutation (autre point de vue)
Soit E un ensemble à n éléments.
Toute n-liste (ordonnée) des n éléments distincts de E représente une permutation de E.
Et réciproquement.

Remarque - Mot clés
Les deux mots clés ici sont **ordonnée** et **distincts**.
Ces deux mots répondent aux deux dernières questions de notre exercice introductif.
Ce qui est important également, est le fait qu'*ici* on considère tous les éléments de E, sans en oublier …

Exemple - Permutations de $\{a,b,c,d\}$
Notons $E = \{a,b,c,d\}$. Les permutations de E sont représentées par :
abcd abdc acbd acdb adbc adcb bacd badc bcad bcda bdac bdca
cabd cadb cbad cbda cdab cdba dabc dacb dbac dbca dcab dcba
il y en a 24 (= 4!).

Proposition - Nombre de permutations
Soit E un ensemble de n éléments.
Alors **le nombre de permutations de E est $n!$**.

Démonstration
On démontrer ce résultat par récurrence. Notons, pour tout entier $n \geqslant 1$, $\mathscr{P}_n$:"tout E de n éléments possède $n!$ permutations".
— Si E ne possède qu'un élément x, alors il n'y a qu'une bijection de E dans E : $\varphi : x \mapsto x$.
donc, comme $1! = 1$, $\mathscr{P}_1$ est vraie.
— Soit $n \in \mathbb{N}^*$. Supposons que $\mathscr{P}_n$ est vraie.
Soit E un ensemble à $n+1$ éléments, supposons $E = \{x_1, x_2 \dots x_n, x_{n+1}\}$.
On note S_X, l'ensemble des permutation de X (fini).
$$S_{E_{n+1}} = \bigcup_{x \in E_{n+1}} \big(\{x\} \times S_{E_{n+1} \setminus \{x\}}\big)$$
La réunion est disjointe, donc d'après $\mathscr{P}_n$:
$$\text{card}(S_{E_{n+1}}) = \sum_{x \in E_{n+1}} (1 \times n!) = n! \times \text{card}(E_{n+1}) = (n+1)\,n! = (n+1)!$$
Donc $\mathscr{P}_{n+1}$ est vraie.
La récurrence est démontrée. □

Exemple - Simple
Quel est le nombre de dispositions possibles de cinq personnes sur un banc de cinq places?
Il s'agit de compter le nombre de permutation de ces cinq personnes. il y en a donc $5! = 120$.
Exercice
Combien existe-t-il d'anagrammes du mot "compris" ?

Correction
il s'agit de permuter les 7 lettres (distincts) de ce mot.
Il y a $7! = 5040$ anagrammes distincts.

3.4. Dénombrement d'un ensemble de p-listes sans répétition

Théorème - Nombre de p-liste (sans répétition)
Soit E un ensemble fini de cardinal n.
Le nombre de p-listes d'éléments distincts de E est $n \times (n-1) \times \cdots \times (n-p+1) = \dfrac{n!}{(n-p)!}$ si $p \leqslant n$, 0 sinon.
Par convention $0! = 1$.

Pour aller plus loin - Nombre d'arrangement
Le nombre $\dfrac{n!}{(n-p)!}$, parfois noté A_n^p s'appelle le nombre d'arrangement de p éléments distincts parmi n

Démonstration
Soit E un ensemble de n éléments. Notons A_n^p le nombre d'arrangements à p éléments distincts.
Notons $\mathscr{P}$, l'ensemble des permutations de E. Alors on sait que $\text{Card}\mathscr{P} = n!$.
Pour chacune de ces permutations, considérons les p premiers termes.
Nous obtenons alors la liste des arrangements de p éléments distincts à partir E.
Mais dans cette liste, chacun des arrangements possibles figurent exactement $(n-p)!$ fois, puisqu'il s'agit du nombre de permutations des $(n-p)$ derniers termes de chaque permutations considérées.
Ainsi $(n-p)! \times A_n^p = n!$ et donc $A_n^p = \dfrac{n!}{(n-p)!}$ □

Remarque - Explication de la démonstration
Voici un exemple illustratif de la démonstration, pour $n = 4$ et $p = 2$.
Considérons E de la forme $\{a,b,c,d\}$.
Les arrangements sont alors :
*ab*cd *ab*dc *ac*bd *ac*db *ad*bc *ad*cb
*ba*cd *ba*dc *bc*ad *bc*da *bd*ac *bd*ca
*ca*bd *ca*db *cb*ad *cb*da *cd*ab *cd*ba
*da*bc *da*cb *db*ac *db*ca *dc*ab *dc*ba

Il y a $A_4^2 \times 2! = 4!$ permutations et donc $A_4^2 = \dfrac{4!}{2!} = 12$ arrangements.

Exercice
Un piano à queue à 88 touches. De combien de manières différentes peut-on jouer une mélodie de 7 sons consécutifs sans jouer deux fois la même note ?

Correction
Il s'agit de compter le nombre de 7-liste sans répétition dans un ensemble de 88 éléments.
Il y a donc maintenant A_{88}^7 mélodies différentes.

Pour aller plus loin - Factorielles (ou puissances) montantes
On trouve parfois aussi la notation $a^{\overline{n}}$ (ou $(a)_n$). Dans un contexte de dénombrement, elle représente le nombre :
$$a^{\overline{n}} = a \times (a+1) \times \cdots \times (a+n-1)$$
Cette définition est vraie, même si a n'est pas un nombre entier.
Mais si a est entier, on a donc $a^{\overline{n}} = \frac{(a+n-1)!}{(a-1)!}$.
On note aussi parfois :
$$a^{\underline{n}} = a \times (a-1) \times \cdots \times (a-n+1)$$

Corollaire - Nombre d'applications injectives
Soient E et F deux ensembles finis, Card $(E) = p$, Card $(F) = n$, alors : le nombre d'applications injectives de E dans F est $n\times(n-1)\times\cdots\times(n-p+1) = \frac{n!}{(n-p)!}$ si $p \leqslant n$, 0 sinon ;

Démonstration
Pour le comprendre, il suffit de noter $E = \{x_1, x_2 \dots x_p\}$ le premier ensemble.
Une injection f de E dans F correspond exactement à l'ensemble des couples : $\{(x_1, f(x_1)),$ $(x_2, f(x_2)\dots(x_n, f(x_n)\}$ ou encore, puisque les x_i sont classés :
une injection est une p-liste $(f(x_1), f(x_2)\dots, f(x_n))$ où chaque $f(x_i) \in F$ est unique.
Il s'agit donc bien d'un arrangement de p éléments à partir de F □

3.5. Dénombrement d'un ensemble de sous-ensemble à p éléments (combinaison)

Théorème - Nombre de combinaison et coefficient binomial
Soit E un ensemble fini de cardinal n. Pour $p \leqslant n$, on note $\binom{E}{p}$ l'ensemble des parties à p éléments de E. On a

$$\text{Card}\binom{E}{p} = \binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}.$$

Ce nombre est appelé nombre de combinaisons de p éléments parmi n et se lit « p parmi n ».

Remarque - Autre notation
On peut aussi trouver la (vieille) notation $C_n^p = \binom{n}{p}$ (attention alors à l'inversion de n et p).

Démonstration
Notons $\binom{n}{p}$ le nombre de combinaisons simples de p éléments parmi n.
Si l'on permute les éléments de chaque combinaison simple, on obtient tous les arrangements simples.
Il y a donc $p!$ fois plus d'arrangements que de combinaisons.
Donc $A_n^p = p! \times \binom{n}{p}$ et donc $\binom{n}{p} = \frac{n!}{(n-p)!p!}$. □

Remarque - Ensemble non ordonné
Le nombre de combinaison apparait lorsque l'on décompte un nombre de situations où les éléments élémentaires ne sont pas ordonnés. Cela peut se produire de deux façons :
- tous les éléments sont « tirés » ensemble (une poigné). Aucun ordre n'est possible
- les éléments sont tirés successivement, mais l'ordre ne compte pas (pour une raison ou une autre, clairement spécifiée dans l'énoncé)

Exercice
Quel est le nombre de main avec 3 as, si l'on distribue un jeu de 32 cartes ?

Correction
Une main favorable est exactement composé de
- trois parmi les quatre as : $\binom{4}{3}$ possibilités
- 2 parmi les 28 autres cartes (non as) : $\binom{28}{2}$ possibilités.

Il y a donc $\binom{4}{3}\binom{28}{2}$ mains favorables.

Sur cet exemple, on voit le principe de décomposition en action.

Savoir faire - Dénombrement et principe de décomposition
Il s'agit décrire *exactement* (c'est à dire tous les éléments, sans les compter plusieurs fois) l'ensemble des situations possibles.
On écrit :
« Une situation … (qui correspond à nos attentes) est parfaitement définie par :

1. le choix de …
   (combien d'éléments de disponible? combien d'éléments choisis? Y-a-t-il remise ou non? est-ce une liste ou un ensemble?),
   soit n_1 possibilités
   Puis
2. le choix de ……, soit n_2 possibilités
   Puis
   ⋮
k. le choix de ……, soit n_k possibilités

Il y a donc $n_1 \times n_2 \times \cdots \times n_k$ situations possibles. »

Exercice
De combien de manières peut-on choisir parmi 30 personnes une équipe de 6 personnes en fixant parmi elles un capitaine ?

Correction
Principe de décomposition : une équipe est parfaitement définie par
- Le choix du capitaine : $\binom{30}{1} = 30$ possibilités.
- Le choix des 5 autres joueurs : $\binom{29}{5}$ possibilités.

Il y a donc $30 \times \frac{29!}{5!24!} = 29\times7\times27\times26\times25 (= 3\,562\,650)$ équipes possibles.
Autre façon de raisonner :
Principe de décomposition : une équipe est parfaitement définie par
- Le choix des 6 autres joueurs : $\binom{30}{6}$ possibilités.
- Le choix du capitaine parmi les 6 joueurs : $\binom{6}{1} = 6$ possibilités.

Il y a donc $\frac{30!}{6!24!} \times 6 = 29\times7\times27\times26\times25$ équipes possibles.
Dernière façon de raisonner (avec le coefficient multinomial) :
Une équipe est parfaitement définie par un "anagramme" de 5 équipiers, 1 capitaine et 24 rien.
Il y a donc $\frac{30!}{1!5!24!} = 29\times7\times27\times26\times25$ équipes possibles.

Savoir faire - Nature du coefficient binomial
Puisque le coefficient binomial exprime le nombre de quelque chose, il s'agit toujours d'un nombre entier, ainsi les calculs fractionnaires *se simplifieront toujours*.
Il faut donc toujours commencer par simplifier les calculs avant d'effectuer les premières multiplications

Exemple - Calculer $\binom{9}{5}$
On a $\binom{9}{5} = \frac{9!}{5!4!} = \frac{9\times8\times7\times6}{4\times3\times2\times1} = 9\times2\times7 = 126$, ce n'est pas un calcul compliqué!

3.6. Propriétés du coefficient binomial (rappels)

Proposition - Propriétés
On a vu :

$$\binom{n}{0}=1;\quad \binom{n}{1}=n;\quad \binom{n}{2}=\frac{n(n-1)}{2};$$

pour $p\leqslant n$, $\binom{n}{p}=\binom{n}{n-p}$

pour $1\leqslant p\leqslant n$ $\binom{n}{p}=\binom{n-1}{p-1}+\binom{n-1}{p}$

$$\sum_{p=0}^{n}\binom{n}{p}=2^n$$

Par convention, si $p>n$, $\binom{n}{p}=0$

(cela a du sens : selon la définition et dans le triangle de Pascal...)

Remarque - Binôme de Newton
En utilisant la distributivité de × par rapport à +, l'associativité et la commutativité de + et la commutativité de × (en fait $ab=ba$ suffit) on obtient par dénombrement la formule du binôme de Newton dans $\mathbb{R}$ ou $\mathbb{C}$ (et en fait dans tout ensemble muni de deux opérations ayant les propriétés utilisées) :

$$(a+b)^n=\sum_{p=0}^{n}\binom{n}{p}a^p b^{n-p}$$

d'où la dénomination de *coefficients binomiaux* pour les $\binom{n}{p}$.

Remarque - Nombre de chemins
Au chapitre 2, nous avions également fait le lien entre les coefficients binomiaux est le nombre de chemin avec k succès pour n répétitions d'épreuve de Bernoulli

Pour aller plus loin - Factorielles montantes et binôme de Newton
Montrer que, pour tout a et b qui commutent dans un anneau :

$$(a+b)^{\overline{n}}=\sum_{k=0}^{n}\binom{n}{k}a^{\overline{k}}b^{\overline{n-k}}$$

4. Exercices d'applications

4.1. Tableau des dénombrements classiques

Savoir faire - Questions à se poser
On considère un ensemble E de cardinal n. On effectue alors un tirage de p éléments (avec des hypothèses évoluantes)

	Ordre?	Répétition?	Nombre de cas	Ex. classique
Nombres de permutations (Arrangement **total**)	OUI	NON	$n!$	Nbre de bijections
Nbres de p-liste sans répétition (Arragenments simples)	OUI	NON	$A_n^p=\frac{n!}{(n-p)!}$	Nbre d'applications injectives
Nombres de p-liste (Arrangements avec répétition)	OUI	OUI	n^p	Nbre d'applications
Nombre de sous ensembles (Combinaisons simples)	NON	NON	$\binom{n}{p}=\frac{n!}{p!(n-p)!}$	Pioche d'une poignée

Il faut savoir remplir ce tableau de **façon intuitive** (et non uniquement grâce à la mémoire).

Exercice
On considère une urne de 10 boules, 6 rouges et 4 bleues.
Combien existe-t-il de façons différentes de tirer 4 boules dans l'urne dont au moins deux serait rouges.

1. si le tirage se fait simultanément ?
2. si le tirage se fait une à une et avec remise ?
3. si le tirage se fait une à une et sans remise ?

La méthode est toujours la même. A chaque fois on prendra un paramètre ou **un conditionnement** : on supposera que le nombre de boules bleues tirées vaut k avec k variant de 0 à 2.

Correction

1. Si $k=0$, on a tiré que du rouge : 4 parmi 6 (rouges) et 0 parmi 4 (bleues). $C(k=0)=\binom{6}{4}\binom{4}{0}=15$.
   De même $C(k=1)=\binom{6}{3}\binom{4}{1}=20\times4=80$, $C(k=2)=\binom{6}{2}\binom{4}{2}=15\times6=90$, Donc dans ce cas le nombre de cas possible est : $\sum_{k=0}^{2}\binom{6}{4-k}\binom{4}{k}=185$.
2. Si $k=0$, on a tiré que du rouge : une 4-liste parmi 6 (rouges) et 0 parmi 4 (bleues). $A(k=0)=6^4\times4^0=1296$.
   De même $A(k=1)=6^3\times4\times4=3456$, on multiplie ici par $4=\binom{3+1}{1}$ car la boule bleue peut se trouver à quatre endroits différents par rapport aux trois rouges triées.
   $A(k=2)=6^2\times4^2\times6=3456$, on multiplie ici par $6=\binom{2+2}{2}$ car les boules bleues (déjà ordonnées) peuvent se trouver à six endroits différents par rapport aux deux rouges triées.
   Donc dans ce cas le nombre de cas possible est : $\sum_{k=0}^{2}\binom{4}{k}6^{4-k}\times4^k=8208$.
3. Si $k=0$, on a tiré que du rouge : une 4-liste sans répétition parmi 6 (rouges) et 0 parmi 4 (bleues). $A(k=0)=A_6^4A_4^0=\frac{6!}{2!}\frac{4!}{4!}=360$.
   De même $A(k=1)=A_6^3A_4^1\times4=1920$, on multiplie ici par $4=\binom{3+1}{1}$
   $A(k=2)=A_6^2A_4^2\times6=2160$, on multiplie ici par $6=\binom{2+2}{2}$
   Donc dans ce cas le nombre de cas possible est : $\sum_{k=0}^{2}\binom{4}{k}A_6^{4-k}A_4^k=4440$.

A noter
$\sum_{k=0}^{4}\binom{6}{4-k}\binom{4}{k}=\binom{4}{10}=210$

A noter
$\sum_{k=0}^{4}\binom{4}{k}6^{4-k}\times4^k=(6+4)^4=10000$

A noter
$\sum_{k=0}^{4}\binom{4}{k}A_6^{4-k}A_4^k=A_{10}^4=5040$

Exercice
Soit E un ensemble fini de cardinal n. Déterminer le nombre de couples $(X,Y)\in\mathscr{P}(E)^2$ tels que $X\subset Y$.

Correction
A priori, on peut procéder en deux temps :
- choisir X, il peut être n'importe quel ensemble entre $\emptyset$ et E. Il y a 2^n choix possibles.
- une fois que X est choisit, il faut choisir Y, mais cela dépend de X et en particulier (du nombre) de ses éléments.

On doit faire mieux :
- On choisit k de 0 à n. Il faudra faire une réunion des cas.
- On choisit X à k éléments. Il y a $\binom{n}{k}$ choix possibles.
- Une fois que X est choisit, il faut choisir Y, c'est un ensemble de la forme $X\cup Z$, avec Z sous-ensemble de $E\setminus X$.
  Il y a donc autant de choix possibles que de Z, i.e. 2^{n-k}

Il y a donc $\sum_{k=0}^{n}\binom{n}{k}2^{n-k}=(1+2)^n=3^n$ possibilités.

Une autre façon de raisonner : à chaque élément de E, associer 0 s'il est dans aucun ensemble X et Y, 1 si il est dans X mais pas Y et 2 s'il est dans X et Y.
Il s'agit donc de dénombrer le nombre d'applications de E dans $\{0,1,2\}$.

4.2. Coefficient multinomial

Analyse - Anagramme de mots avec lettres dédoublées
On cherche le nombre d'anagramme, non plus de « compris », mais du mot « excellence ».
Le problème ici est qu'il a deux 4 « e » et 2 « l ».
Si l'on souhaite appliquer la même méthode, il faut considérer le mot "$e_1xce_2l_1l_2e_3nce_4$".
Dans ce cas les 10 lettres sont différentes et il y a 10! anagrammes.
Parmi ceux-ci, il y a le mot "$e_1xce_2l_1l_2e_3nce_4$" et le mot "$e_1xce_2l_2l_1e_3nce_4$".
Ainsi, parmi les 10! permutations, nous avons dénombré 2! fois trop de mots à cause des permutations de « l ».
De même, parmi les 10! permutations, nous avons dénombré 4! fois trop de mots à cause des permutations de « e ».
Finalement, il y a $\frac{10!}{4!2!(1!1!1!1!)}=75\,600$ anagrammes du mot "excellence".

Savoir faire - Permutations avec répétition
Le nombre de permutations de n éléments avec k sous groupes tels que :
- le premier sous groupe est composé de n_1 éléments identiques (ou indiscernables)

— le deuxième sous groupe est composé de n_2 éléments identiques (ou indiscernables)
— …,
— le k^e sous groupe est composé de n_k éléments identiques (ou indiscernables)
vérifiant donc $\sum_{i=1}^{k} n_i = n$,
est égal à : $\dfrac{n!}{n_1!n_2!\dots n_k!}$.

Remarque - Coefficient multinomial
Le nombre $\dfrac{n!}{n_1!n_2!\dots n_k!}$ est appelé coefficient multinomial.

Remarque - Autre expression
Le nombre de permutations de n éléments, répartis dans k classes dont
— n_1 sont de classe 1,
— n_2 sont de classe 2,
— …,
— n_k sont de classe k,
indiscernables dans chaque classe est $\dfrac{n!}{n_1!n_2!\dots n_k!}$

Exemple - A écrire
Les $\dfrac{5!}{2!1!2!} = 30$ permutations des 5 éléments a, a, b, c et c sont :

$aabcc$	$aacbc$	$aaccb$	$abacc$	$abcac$	$abcca$	$acabc$	$acacb$	$acbac$	$acbca$
$accab$	$accba$	$baacc$	$bacac$	$bacca$	$bcaac$	$bcaca$	$bccaa$	$caabc$	$caacb$
$cabac$	$cabca$	$cacab$	$cacba$	$cbaac$	$cbaca$	$cbcaa$	$ccaab$	$ccaba$	$ccbaa$

Exercice
Combien existe-t-il d'anagramme du mot "abracadabra" ?

Correction
C'est un ensemble de 11 lettres avec 5 a, 2 b, 1 c, 1 d et 2 r.
Il y a donc

$$\frac{11!}{5!2!2!1!1!} = \frac{11\times10\times9\times8\times7\times6\times\cancel{5!}}{\cancel{5!}\times2!2!} = \frac{11\times(5\times\cancel{2})\times9\times(4\times\cancel{2})\times7\times6}{\cancel{2}\times\cancel{2}} = 83\,160$$

anagrammes d'abracadabra

Exercice
Dans un anneau, avec a, b, c et d qui commutent, exprimer

$$(a+b+c+d)^{10}$$

Correction
$(a+b+c+d)^{10} = \sum_{i+j+k+\ell=10} \frac{10!}{i!j!k!\ell!} a^i b^j c^k d^\ell$

4.3. Séries génératrices

Formule de Vandermone

On commence par une première formule (importante) qui nous conduit vers une méthode plus générale.

Proposition - Formule de Vanderermonde
Soient $n, m, p \in \mathbb{N}^*$ avec $p \leqslant \min(n,m)$.
Alors $\displaystyle\sum_{i=0}^{p} \binom{n}{i}\binom{m}{p-i} = \binom{n+m}{p}$ (Formule de Vandermonde)

Démonstration
Soient $n, m, p \in \mathbb{N}^*$ avec $p \leqslant \min(n,m)$.
Montrer que $\displaystyle\sum_{i=0}^{p} \binom{n}{i}\binom{m}{p-i} = \binom{n+m}{p}$ (Formule de Vandermonde) Nous ferons une démonstration basée sur les combinaisons en exploitant le principe de décomposition.
Soit E un ensemble à $n+m$ éléments.
On peut diviser E en deux ensembles : E_n, de n éléments et E_m de m éléments.
Tout sous-ensemble à p éléments de E est composé de deux sous-ensembles : l'un de E_n à i éléments et l'un de E_m, possédant alors nécessairement $p-i$ éléments.
Réciproquement, tout concaténation d'un sous-ensemble à j éléments de E_n et à $p-j$ éléments de E_m donne un sous-ensemble de p élément de E.
Donc les sous-ensemble à p éléments de E sont exactement ceux composés de deux sous-ensembles : l'un de E_n à i éléments et l'un de E_m, possédant alors nécessairement $p-i$ éléments.
Formellement :

$$\binom{E}{p} = \bigcup_{i=0}^{n} \Phi\left(\binom{E_n}{i}, \binom{E_m}{p-i}\right) \qquad \text{où } \Phi : (A,B) \mapsto A@B$$

Les premiers sont au nombre $\binom{n+m}{p}$, les seconds sont $\displaystyle\sum_{i=0}^{p}\left(\binom{n}{i}\times\binom{m}{p-i}\right)$.
— en effet : il faut choisir un sous ensemble de E_n puis un de E_m : donc on a une multiplication.
— pour tous les compter, il faut faire l'addition (c'est une réunion d'ensemble)
□

L'analyse suivante qui démontre le même résultat nous conduit à une nouvelle stratégie.

Analyse - Calcul de deux façons du développement de $(1+X)^{n+m}$
Soient $m, n \in \mathbb{N}$ et $p \leqslant \min(n,m)$.

1. Quel est le coefficient de X^p lorsque l'on développe $(1+X)^{n+m}$ est $\binom{n+m}{p}$
2. Quel est le coefficient de x^p lorsque l'on développe $(1+X)^n \times (1+x)^m$ est $\displaystyle\sum_{k=0}^{n}\binom{n}{k}\binom{m}{p-k}$
3. Il n'y a qu'une faon d'écrire le développement du polynôme sur la base des X^p, donc $\displaystyle\sum_{i=0}^{p}\binom{n}{i}\binom{m}{p-i} = \binom{n+m}{p}$

Cas générale

Heuristique - Fonction ou série génératrice
Voici une méthode qui fonctionne particulièrement bien en dénombrement.
On considère un problème de dénombrement, dont l'hypothèse dépend d'une variable entière n.
On note a_n, le dénombrement recherché et on crée la fonction :

$$f(x) = \sum_{n=0}^{+\infty} a_n x^n$$

Alors, la plupart des hypothèses se transpose en une propriété calculatoire de f.
Puis, on cherche alors la fonction f. Et enfin, il ne reste plus qu'à trouver ses coefficients (identification)

On peut même, sans soucis de convergence, étudier des séries génératrices, sorte de polynôme de degré infini

Définition - Série génératrice
On considère $u = (u_n)$, une suite à valeurs dans un corps $\mathbb{K}$.
On lui associe la série génératrice $S(u) = \displaystyle\sum_{n\in\mathbb{N}} u_n X^n$.
On note $\mathbb{K}[[X]]$, l'ensemble des séries génératrices.

Remarque - Inclusion algébrique
En fait, $\mathbb{K}[X] \subset \mathbb{K}(X) \subset \mathbb{K}[[X]]$.

Exemple - Série géométrique
On a pour $u_n = 1$, $S(u) = \sum_{n\in\mathbb{N}} X^n = \frac{1}{1-X}$
On a les règles opératoires suivantes qui permettent de passer de propriétés sur (u_n) à des propriétés sur S.

Proposition - Règles opératoires sur les séries génératrices
On généralise les opérations sur les polynômes aux opérations équivalentes sur les séries.
On a alors pour $\lambda \in \mathbb{K}$, $u, v \in \mathbb{K}^{\mathbb{N}}$:
— $S(u+v) = S(u) + S(v)$
— $S(\lambda u) = \lambda S(u)$
— $X^k S(u) = S(\underbrace{0,0,\dots 0}_{k}, u)$ (règle de décalage)
ou $S(u) = (u_0 - u_1 X - \dots u_{k-1}X^{k-1}) + X^k S\big((u_{n+k})\big)$
— $S'(u) = S\big((nu_n)_{n\geqslant 1}\big)$ = (règle de dérivation)
— $S(u) \times S(v) = S\big((\sum_{k=0}^{n} u_k v_{n-k})_{n\geqslant 0}\big)$ (règle de produit de Cauchy)
Si $u_0 \neq 0$, on peut même définir l'inverse de $S(u)$… (comme pour des DL)

Heuristique - Comme pour les polynômes…
On a montrer comme pour les polynômes, en exploitant la dérivation formelle, qu'il y a une unique façon d'écrire une série formelle.

On peut identifier

Proposition - Identification
Si $S(u) = S(v)$, alors pour tout $n \in \mathbb{N}$, $u_n = v_n$.

Application - Suite de Fibonacci
On considère la suite de Fibonacci vérifiant $F_{n+2} = F_{n+1} + F_n$ et $F_0 = F_1 = 1$.
On note $F(X) = S(F_n) = \sum_{n\in\mathbb{N}} F_n X^n$.

$$\begin{aligned} F(X) &= F_0 + F_1 X + X^2 \sum_{n\in\mathbb{N}} F_{n+2} X^n = F_0 + F_1 X + X^2 \sum_{n\in\mathbb{N}} (F_{n+1} + F_n) X^n \\ & F_0 + F_1 X + X(F(X) - F_0) + X^2 F(X) = (X + X^2) F(X) + (F_1 - F_0) X + F_0 \end{aligned}$$

On note $r_1 = \frac{-1+\sqrt{5}}{2}$ et $r_2 = \frac{-1-\sqrt{5}}{2}$, les racines de $X^2 - X - 1 = (X - r_1)(X - r_2)$. Donc $1 - X - X^2 = (1 - r_1 X)(1 - r_2 X)$. Et comme $F_1 - F_0 = 0$,

$$F(X) = \frac{(F_1 - F_0)X + F_0}{1 - X - X^2} = \frac{F_0}{(1 - r_1 X)(1 - r_2 X)}$$

On exploite la décomposition en éléments simples :

$$F(X) = \frac{1}{r_1 - r_2}\left(\frac{r_1}{1 - r_1 X} - \frac{r_2}{1 - r_2 X}\right) = \frac{1}{\sqrt{5}}\left(r_1 \sum_{n\in\mathbb{N}} r_1^n X^n - r_2 \sum_{n\in\mathbb{N}} r_2^n X^n\right)$$

On peut alors identifier : $F_n = \frac{1}{\sqrt{5}}\left(r_1^{n+1} - r_2^{n+1}\right)$.

Pour aller plus loin - « En toute rigueur… »
Les soucis d'analyse (de type convergence…) ne sont pas féconds ici. On s'en inspire, mais le formalisme est suffisant (comme pour la dérivation des polynômes qui ne demande pas de montrer la dérivabilité de l'objet).
Néanmoins, si vous êtes pris de remords, les séries entières vues l'année prochaines répondront à toutes ces questions.
C'est aussi pour préparer ce thème important de seconde année (séries entières) que nous proposons cette partie hors-programme (séries formelles)

Pour aller plus loin - Fonction (série) génératrice de plusieurs variables
Cela se généralise à plusieurs variables entières, on introduit alors plusieurs inconnues $x, y\dots$

Dérangement

Définition - Dérangement sur n
On fixe $n \in \mathbb{N}^*$. On appelle dérangement de l'ensemble $\mathbb{N}_n$, une permutation (bijection) de $\mathbb{N}_n$ sans points fixes.
On note D_n, le nombre de dérangement de $\mathbb{N}_n$

Le but est de trouver la valeur de D_n. Or ce qui semble naturel est une relation qui lie $n!$ à tous les D_k pour $k \leqslant n$.

Proposition - Relation (inversée)
Soit $n \in \mathbb{N}$. Alors $n! = \sum_{k=1}^{n} \binom{n}{k} D_k$, avec la convention que $D_0 = 1$.

Démonstration
L'ensemble des permutations se décomposent en permutations avec k points fixes, pour k de 0 à n.
Notons donc A_k, l'ensemble des permutations avec k points fixes : $S_n = \biguplus_{k=1}^{n} A_k$.
Donc $\text{card}(S_n) = \sum_{k=0}^{n} \text{card}(A_k)$.
Or les permutations avec k points fixes sont bijectivement décrits par :
— le choix de k éléments fixés. Il y a $\binom{n}{k}$ possibilités.
— le choix d'un dérangement des $n-k$ points non fixé. Il y a D_{n-k} possibilités.
(Si n points fixes, donc 0 dérangement, il faut compter $D_{n-n} = 0$.)
Ainsi $n! = \sum_{k=1}^{n} \binom{n}{k} D_{n-k} = \sum_{h=1}^{n} \binom{n}{n-h} D_h = \sum_{h=1}^{n} \binom{n}{h} D_h$. □

Cela ne semble pas répondre à la question.
Analyse - Stratégie!
On considère alors la série $D = \sum_{k=0}^{n} \frac{D_k}{k!} X^k$ et $E = \sum_{k=0}^{n} \frac{1}{k!} X^k$.
On a donc

$$D \times E = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} \frac{D_i}{i!(k-i)!}\right) X^k = \sum_{k=0}^{+\infty} \left(\frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} D_i\right) X^k = \sum_{k=0}^{+\infty} X^k = \frac{1}{1-X}$$

Et comme on sait que $E^{-1} = \exp(-X) = \sum_{k=0}^{n} \frac{1}{k!}(-1)^k X^k$, on a donc

$$D = \sum_{k=0}^{+\infty} \frac{(-1)^k}{k!} X^k \times \sum_{k=0}^{+\infty} X^k = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} \frac{(-1)^i}{i!}\right) X^k$$

On peut terminer en identifiant : $\frac{D_n}{n!} = \sum_{i=0}^{n} \frac{(-1)^i}{i!}$.

Exercice
Quelle est la limite du taux moyen de dérangement $\frac{D_n}{n!}$?

Correction
Il s'agit de $\lim \frac{D_n}{n!} \to e^{-1}$

Exercice
En exploitant les séries génératrices montrer également que $D_n - nD_{n-1} = (-1)^n$

Correction
On a $(1-X)D = E^{-1}$, les coefficients associés à X^n sont : $\frac{D_n}{n!} - \frac{D_{n-1}}{(n-1)!} = \frac{(-1)^n}{n!}$.
En multipliant par $n!$, on trouve le résultat recherché.

Application au p-partage

Définition - p-partage de n
On appelle p-partage de n, un p-uplet d'entier naturel $(n_1, n_2, \ldots p)$ tel que $n_1 + n_2 + \cdots + n_p = n$.
On note $E_p(n) = \sharp\{(n_1, n_2, \cdots n_p) \in \mathbb{N}^p \mid \sum_{i=1}^{p} n_i = n\}$.

Exemple - 3-partage de 5
Les 3-partage de 5 sont au nombre de 21, il s'agit de $(1,1,3)$, $(1,3,1)$, $(3,1,1)$, $(1,2,2)$, $(2,1,2)$, $(2,2,1)$, $(0,1,4)$, $(0,4,1)$, $(1,0,4)$, $(1,4,0)$, $(4,0,1)$, $(4,1,0)$, $(0,2,3)$, $(0,3,2)$, $(2,0,3)$, $(2,3,0)$, $(3,0,2)$, $(3,2,0)$, $(5,0,0)$, $(0,5,0)$, et $(0,0,5)$.

Proposition - Dénombrement des p-partage de n
Le nombre de p partage de n est $E_p(n) = \binom{p+n-1}{n}$.

Exemple - 3-partage de 5
On vérifie : il y a bien $\binom{3+5-1}{5} = \binom{7}{5} = \frac{7\times 6}{2} = 21$.

Démonstration
On note $F_p = \sum_{n=0}^{+\infty} E_p(n) X^n$.

$$\begin{aligned} F_p &= \sum_{n=0}^{+\infty} \left(\sum_{n_1+n_2+\cdots+n_p=n} 1 \right) X^n = \left(\sum_{n=0}^{+\infty} X^n \right)^p = \frac{1}{(1-X)^p} = (1-X)^{-p} \\ &= \sum_{n=0}^{+\infty} \binom{-p}{n} X^n = \sum_{n=0}^{+\infty} \frac{(-p)(-p-1)\cdots(-p-n+1)}{n!} (-1)^n X^n \\ &= \sum_{n=0}^{+\infty} \frac{(p+n-1)(p+n-2)\cdots(p+1)p}{n!} X^n = \sum_{n=0}^{+\infty} \binom{p+n-1}{n} X^n \end{aligned}$$

On identifie $E_p(n) = \binom{p+n-1}{n}$. □

5. Bilan

Synthèse

- ⇝ Les questions de dénombrements ne sont pas toujours évidentes à comprendre et souvent difficile à répondre synthétiquement. Il faut mettre en place une (méta-)stratégie.
- ⇝ Un premier réflexe à avoir : se demander comment décrire un exemple concret de situation répondant au problème. Il est bon alors d'être attentif au liberté pour choisir les paramètres qui ne manquent pas d'apparaitre.
- ⇝ Il apparait alors fondamentalement deux types classiques de calcul : l'addition-soustraction (réunion d'ensemble, méthode du crible de Poincaré, partitions…) et la multiplication (avec répétition : $n \times n \times \cdots \times n = n^p$ - sans répétition : $n(n-1)\ldots(n-p+1) = \frac{n!}{(n-p)!} = A_n^p = p!\binom{n}{p}$).
- ⇝ Tout le reste est raffinement de ces deux points. Une stratégie en particulier efficace est celle qui consiste à exploiter des bijections : elle transforme un point de vue en un autre *totalement équivalent* mais dont le calculs de nombres de cas différents est plus facile (anagramme et coefficients multinomiaux…) ou plus auto-math-ique (série génératrices…).

Savoir-faire et Truc & Astuce du chapitre

- — Savoir-faire - Méthode : description des expériences
- — Savoir-faire - Montrer qu'un ensemble est fini
- — Savoir-faire - Calculer, théoriquement, le cardinal d'un ensemble fini
- — Savoir-faire - Formule du crible
- — Savoir-faire - Quand est-ce que l'on voit apparaître un produit cartésien
- — Savoir-faire - Dénombrement et principe de décomposition
- — Savoir-faire - Nature du coefficient binomial
- — Savoir-faire - Questions à se poser
- — Savoir-faire - Permutations avec répétitions

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\mathscr{F}(E,F)$	Ensemble des applications de E vers F	Card $\mathscr{F}(E,F) =$ Card $F^{\text{Card } E}$	Avec $F = \{0,1\}$: Card $\mathscr{P}(E) = 2^n$ (nbre de sous-ensembles ou parties de E)
p-liste	Ensemble obtenu par produits cartésiens. La place de chaque élément est bloquée		Usage fondamentale en informatique
$\binom{E}{p}$	Sous-ensembles de E, ayant exactement p éléments	Card $\binom{E}{p} = \binom{\text{Card } E}{p} = \frac{n!}{p!(n-p)!}$ si Card $E = n$	Voir chapitre 2.
A_n^p	Nombre de p-liste sans répétition à partir d'un ensemble à n éléments	$A_n^p = \frac{n!}{(n-p)!}$	Appelé également nombre d'arrangement (sans répétition).
$\frac{n!}{p_1!p_2!\ldots p_k!}$	Coefficient multinomial (avec $p_1+p_2+\cdots+p_k = n$)	Généralisation du coefficient binomial	On le retrouve dans les anagrammes (et problèmes équivalents) ou le développement de $(a_1+a_2+\cdots+a_p)^n$
$K[[X]]$	Algèbre commutatifs des séries génératrices	Unicité (donc identification) et nombreuses règles opératoires…	Sorte de généralisation des polynômes (sans question de convergence).

Retour sur les problèmes

Chapitre 29

Un groupe fini : le groupe symétrique

Résumé -

Dans ce petit chapitre, nous étudions un groupe (fini) très particulier : le groupe des permutations d'un ensemble à n éléments. Il y aurait beaucoup de choses à écrire ici, mais on se contentera d'une sorte d'introduction. Cela est comme une base culturelle. Deux résultats parallèles : toute permutation est le produit de cycles ou bien le produit de transpositions.
A partir de l'un ou l'autre de ces points de vue, nous définissons la signature d'une permutation.
L'application de ces résultats sera immédiate dans le chapitre suivant lorsque nous définirons le déterminant des matrices (et endomorphismes)

Sommaire

1. Problèmes 592
2. Définitions 593
2.1. Rappels sur le groupe symétrique 593
2.2. Codages des permutations 593
2.3. Des permutations particulières 595
3. Décomposition d'une permutation 597
3.1. Partie génératrice d'un groupe 597
3.2. Décomposition en produit de cycles 598
3.3. Décompositions en produit de transpositions 600
4. Signature d'une permutation 601
4.1. Motivation : nombre d'inversions 601
4.2. Propriété caractéristique 602
4.3. Autres façons d'obtenir la signature de σ 603
5. Bilan 604

1. Problèmes

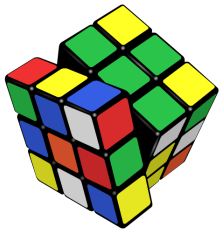
Problème 121 - Un groupe fini non commutatif

Le cours sur les groupes est un peu frustrant. On sent comme un univers derrière une porte, mais celle-ci n'a été qu'entrouverte. Dans le cours, nous avons vu deux types de groupes : les groupes linéaires (puis orthogonaux...) qui sont des groupes infinis voire « continus » (On parle de goupe de LIE). L'autre type de groupe correspond aux groupes finis ; nos exemples $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$, $\mathbb{U}_n$ ou $(F_p^*,\times)$ sont tous commutatifs.
Existe-t-il des groupes finis non abéliens ? Ils pourraient nous servir d'exemples sur les propriétés fortes de l'univers des groupes, si riche !

Problème 122 - Recherche d'invariant

En science, et particulièrement en mathématique, pour bien comprendre des objets, on s'intéresse aux invariants des transformations sur les objets.
Les objets qui sont liés par l'invariance forme en règle générale un groupe. Etudier ce groupe permet de mieux comprendre les objets ou les problèmes associés.
L'exemple historique est le groupe des racines d'un polynôme. S'il existe une formule qui donne les racines d'un polynôme en fonction des coefficients de ce polynôme, cette formule doit être *invariante* sous les permutations des racines !
Ainsi, pour le polynôme ax^2+bx+c, la formule des racines $\Delta=(x_1-x_2)^2$ est invariante par permutation.
Comment exploiter ces idées pour démontrer comme GALOIS et ABEL qu'il n'existe aucune formule générale d'expression des racines d'un polynôme de degré 5 ?

Représentation - Rubik's cup



Rubik's cube

Problème 123 - Rubik's cube

Lorsque l'on manipule le Rubik's cube, chaque manipulation est une bijection sur le cube.
Le cube est représentable par la donnée des positions des 26 petits cubes et leur orientation.
On a donc un (sous-) groupe de permutation d'un ensemble fini. La connaissance du groupe des permutations peut-il nous aider à résoudre tous les Rubik'cube ? Optimiser le nombre minimal de mouvement...

Problème 124 - Groupe engendré. Base ? Codage...

Une famille d'espaces vectoriels interessante à étudier est celle des espaces vectoriels de dimension finie.
Il existe une famille (finie) qui x tout l'espace vectoriel (infini).
Existe-t-il la même chose pour les groupes (et les groupes finis) ?
Par exemple,

$$\mathbb{U}_n = < e^{\frac{2i\pi}{n}} >:= \{\omega^k; k\in\mathbb{Z}\} \qquad (\omega = e^{\frac{2i\pi}{n}})$$

Précisément pour ce chapitre, peut-on engendrer les groupes de permutation à partir d'un ensemble fini de permutation ?
Lorsque cet ensemble fini possède plusieurs éléments $a_1,\dots a_k$, et que

ceux-ci ne commutent pas :

$$< a_1, a_2, \dots a_k >= \left\{ \prod_{i=1}^{d} a_i^{n_i} ; d \in \mathbb{N}, \forall\ i \in \mathbb{N}_d, n_i \in \mathbb{Z}, \alpha_i \in \{a_1, a_2, \dots a_k\} \right\}$$

? Problème 125 - Signature d'ordre 3 ?

On verra plus loin que si σ est une permutation de E, σ se décompose en produit de transpositions. La parité du nombre de transpositions est constante (la décomposition n'est pas unique, mais toute ont la même parité du nombre de transposition génératrice). On appelle signature de σ, la valeur de (-1) à la puissance le nombre de transpositions.
Peut-on décomposer toute permutation de E en produit de permutation particulière (par exemple composée d'un seule cycle de taille 3). Existe-t-il alors un invariant de ces décompositions (non uniques, très certainement) ?

2. Définitions

2.1. Rappels sur le groupe symétrique

Soit $n \geqslant 2$.

Définition - Groupe symétrique
On note S_n (ou $\mathfrak{S}_n$) l'ensemble des permutations de $[\![1,n]\!]$, c'est-à-dire l'ensemble des bijections de $[\![1,n]\!]$ dans $[\![1,n]\!]$.
$(S_n, \circ)$ est un groupe, non commutatif dès que $n > 2$, appelé groupe symétrique (d'ordre n).

Pour aller plus loin - Un meilleur point de vue
« Le bon point » de vue est celui, plus large, de la permutation sur X, un ensemble fini de n éléments ordonnées

On omet parfois $\circ$ dans les écritures et on écrit $\sigma \circ \sigma' = \sigma\sigma'$, on parle alors de « **produit** » plutôt que de composée.

Proposition - Cardinal
Card $S_n = n!$

Démonstration
Ce résultat a été démontré au chapitre précédent. □

2.2. Codages des permutations

Le codage classique

Savoir faire - Notation classique
Pour $\sigma \in S_n$, on note

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \dots & \sigma(n) \end{pmatrix}$$

On notera aussi plus efficacement (et classiquement) :

$$\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \dots & \sigma(n) \end{pmatrix}$$

Inspiré par les commandes Python, on pourrait écrire, $\sigma[4] = \sigma(4)$ (le quatrième élément de la liste σ) et plutôt encore : $\sigma[2:5]$, pour désigner $[\sigma(3)\,\sigma(4)\,\sigma(5)]$.

Histoire - Notation de Cauchy
Cette notation (en double ligne) est due à Cauchy (1812). Cauchy employait le mot de substitution au lieu de permutation. Il réalisait ainsi les premiers produits d'autre objets que des nombres. Il a sûrement eu ainsi une idée claire de ce qu'est un groupe…

Le codage matriciel

Proposition - Codage des permutations avec des matrices de $\mathscr{M}_n(\mathbb{K})$
On note Σ_n, l'ensemble des matrices carrées d'ordre n avec un et un seule 1 par ligne et par colonne.
L'application

$$\begin{array}{rccc} \Phi : & S_n & \longrightarrow & \Sigma_n \\ & \sigma & \longmapsto & S \end{array} \quad \text{telle que } \mathrm{Coef}_{i,j}(S) = {}^{i}[S]_j = \delta_{i,\sigma(j)}$$

est un morphisme bijective de groupes

Pour aller plus loin - Action de groupe S_n
On dit qu'un groupe G agit (à gauche) sur un ensemble E, si on dispose d'une application $(g,x) \mapsto g \cdot x$ de $G \times E$ dans E tel que $1 \cdot x = x$ et pour tout $g, g' \in G$, et tout $x \in E$: $g \cdot (g' \cdot x) = (g \times g') \cdot x$.
On remarquera que si $g \in G$, alors $x \mapsto \sigma_g(x) = g \cdot x$ est une bijection σ_g de E sur E.
Les représentations des permutations que l'on a choisit ici sont en fait des actions de groupes :
- *action de S_n sur l'ensemble $[\![1,n]\!]$.*
- *action de S_n sur l'ensemble des matrices.*
- *action des graphes uniflèches…*

Exemple - Matrice de $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$
Il y a un 1 en ligne i et colonne j, si $s(j) = i$.
Donc $\Phi(s)$ a un 1 :
- en colonne 1 et en ligne 2,
- en colonne 2 et en ligne 1,
- en colonne 3 et ligne 4,
- en colonne 4 et ligne 5
- et en ligne 5 et colonne 3.

Donc $M = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

Démonstration
Φ est bien défini, elle est clairement injective : si $\Phi(\sigma_1) = \Phi(\sigma_2)$ alors $\sigma_1 = \sigma_2$.
Elle est bijective (soit par dénombrement, soit par surjectivité triviale).
C'est un morphisme de groupe.

$$\mathrm{Coef}_{i,j}(\Phi(\sigma_1) \times \Phi(\sigma_2)) = \sum_{k=1}^{n} \mathrm{Coef}_{i,k}(\Phi(\sigma_1)) \times \mathrm{Coef}_{k,j}(\Phi(\sigma_2))$$

$$= \sum_{k=1}^{n} \mathrm{Coef}_{i,k}(\Phi(\sigma_1)) \times \delta_{k,\sigma_2(j)} = \mathrm{Coef}_{i,\sigma_2(j)}(\Phi(\sigma_1)) = \delta_{i,\sigma_1(\sigma_2(j))}$$

Ainsi, $\Phi(\sigma_1) \times \Phi(\sigma_2) = \Phi(\sigma_1 \circ \sigma_2)$ □

Remarque - Structure de groupe
Il faudrait montrer que $(\Sigma_n, \times)$ est un groupe. Mais cela découle directement de l'application Φ.
Exercice
Montrer que pour $S \in \Sigma_n$, S^{-1} s'obtient facilement à partir de S.
Que représente $\mathrm{Tr}(S)$?

Correction
Par morphisme de groupes, $S^{-1} = \Phi(\sigma^{-1})$

$$\mathrm{Coef}_{i,j}(S^{-1}) = \delta_{i,\sigma^{-1}(j)} = \delta_{\sigma(i),j} = \delta_{j,\sigma(i)} = \mathrm{Coef}_{j,i}(S)$$

Donc $S^{-1} = S^T$.
Et $\mathrm{Tr}(S)$ est le nombre de points fixes de S.

Le codage par graphes

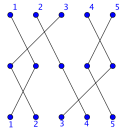
Savoir faire - Permutation et graphe
On écrit en ligne les éléments du départ (souvent en haut) et en bas, les (mêmes) éléments de l'arrivée en bas.
Puis on relie les éléments par des flèches.
Un graphe est celui d'une permutation ssi de chaque point du départ part une unique flèche et à chaque point de l'arrivée arrive une et une seule flèche.
Il s'agit du graphe de la matrice de permutation vue plus haut.

L'avantage très nette de cette représentation : le produit (composition) de permutation consiste simplement à glisser les représentations l'une sous l'autre.
Nous verrons un autre avantage plus loin.

Exercice

Faire la représentation graphique de $\sigma_1 \circ \sigma_2$ si $\sigma_1 = \begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}$ et $\sigma_2 = \begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$. En déduire la valeur de $\sigma_1 \circ \sigma_2$.

Correction



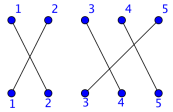
On a le graphe suivant : .

Et donc $\sigma_1 \circ \sigma_2 = \begin{pmatrix}1&2&3&4&5\\1&4&2&3&5\end{pmatrix}$

Représentation - Représentation graphique d'une permutation

Soit $s = \begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}$.

Sa représentation graphique est



2.3. Des permutations particulières

Deux permutations particulières : la transposition et le cycle.

Transpositions

Définition - Transposition
Soit $(a,b) \in [\![1,n]\!]^2$, $a \neq b$. La permutation $\tau_{a,b}$ définie par

$$\tau_{a,b}(a) = b,\ \tau_{a,b}(b) = a,\ \forall x \in [\![1,n]\!] \setminus \{a,b\}\ \tau_{a,b}(x) = x$$

s'appelle la transposition de a et b.

Remarque - Involution
On a $\tau_{a,b} \circ \tau_{a,b} = Id$.

Remarque - Transposition
Quelles sont les matrices associées aux transpositions?
Il s'agit des matrices de permutation vu en cours sur les opérations élémentaires (les noms devraient être unifiées...)

Exercice
Combien de transpositions de S_n existe-t-il ?

Correction
$\binom{n}{2} = \frac{n(n-1)}{2}$

Cycles

Définition - Cycle
Soient $a_1, \dots, a_p$ ($p \leqslant n$) des éléments distincts de $[\![1,n]\!]$.
La permutation σ telle que

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{p-1}) = a_p, \sigma(a_p) = a_1$$

$$\text{et } \forall x \notin \{a_1, a_2, \dots, a_p\},\ \sigma(x) = x$$

s'appelle un cycle de longueur p ou p-cycle, on le note $(a_1\, a_2 \dots a_p)$.
L'ensemble $\{a_1, a_2, \dots, a_p\}$ s'appelle le support du cycle.
Deux cycles sont dits disjoints si leurs supports sont disjoints.

Remarque - 2-cycle
Une transposition est un 2-cycle.

Remarque - Permutation circulaire de S_n
Un n-cycle élément de S_n, s'appelle aussi une permutation circulaire de $[\![1,n]\!]$.

Remarque - Quelle différence entre $(1,2,3)$ et $(2,3,1)$ de S_5?
Aucune. La première envoie 1 en 2, 2 en 3, puis 3 en 1.
Alors que la seconde envoie 2 en 3, 3 en 1 puis 1 en 2...

Analyse - Image réciproque d'une permutation réciproque
$(a_1\, a_2 \dots a_p) \circ (a_p\, a_{p-1} \dots a_1) = Id$. On peut le coder : $\rightarrow \circ \leftarrow = 1 \dots$
Qu'en déduire, matriciellement?
L'utilisation des orbites, dans la prochaine partie, permettra de répondre à la question : comment décomposer en produit de cycles?

Exemple - Quelques cycles

$$n = 4,\quad \sigma = \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix} = (3,2,4,1)$$

$$n = 6,\quad \sigma = \begin{pmatrix}1&2&3&4&5&6\\1&4&3&5&2&6\end{pmatrix} = (2,4,5)$$

$$n = 6,\quad \sigma = \begin{pmatrix}1&2&3&4&5&6\\2&3&1&5&4&6\end{pmatrix} = (1,2,3) \circ (4,5)$$

Exercice
Déterminer les bijections réciproques des bijections précédentes.

Correction
Il s'agit, respectivement des cycles : $(1,4,2,3)$, $(5,4,2)$ et $(4,5) \circ (3,2,1)$

Exercice
Combien de cycle de longueur k de S_n existe-t-il ?

Correction
$\frac{n!}{k(n-k)!}$, en particulier si $k = n$, on trouve $(n-1)!$ n-cycles possibles
Les exemples permettent d'affirmer :

Proposition - Commutation
Deux cycles (à supports) disjoints commutent.

Démonstration
Soit s_1 et s_2, deux cycles à supports disjoints.
Si i est dans le support du premier cycle, alors i et $s_1(i)$ sont dans ce support.
Et comme s_2 et s_1 sont disjoints : $s_2(s_1(i)) = s_1(i)$, alors que $s_1(s_2(i)) = s_1(i)$.
De même si i est dans le support du second cycle : $s_2(s_1(i)) = s_2(i)$,
alors que $s_1(s_2(i)) = s_2(i)$ car $s_2(i)$ n'est pas dans le support de s_1.
Enfin, si i n'est ni dans le support de s_1, ni dans celui de s_2,
alors $s_1(s_2(i)) = i = s_2(s_1(i))$.
Donc pour tout i, $(s_1 \circ s_2)(i) = (s_2 \circ s_1)(i)$ ainsi $s_1 \circ s_2 = s_2 \circ s_1$. □

Exercice
Ecrire les ensembles S_2 et S_3. Donner une permutation de S_4 qui ne soit pas un cycle.

Correction
$S_2 = \{(), (2,1)\}$, $S_3 = \{(), (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}$.
$\{(1,2),(3,4)\}$ est un double cycle...

Proposition - Classe de conjugaison
Soit σ une permutation de $\mathbb{N}_n$ et $c = (a_1 \dots a_k)$ un cyle.
Alors $\sigma \circ c \circ \sigma^{-1}$ est le cycle $\big(\sigma(a_1) \dots \sigma(a_k)\big)$

Démonstration
Si $s = \sigma \circ c \circ \sigma^{-1}$, alors $s(\sigma(a_i)) = \sigma(c(a_i)) = \sigma(a_{i+1})$ Et si $a \notin \{\sigma(a_1), \dots \sigma(a_k)\}$,
alors $\sigma^{-1}(a) \notin \{a_1, \dots a_k\}$, donc $c(\sigma^{-1}(a)) = \sigma^{-1}(a)$ et $s(a) = a$. □

Remarque - Nom arbitraire
Autrement écrit, si les noms sont choisis arbitrairement, les cycles sont équivalents, modulo la relation d'équivalence

$$a \mathscr{R} b \iff \exists\, \sigma \mid a = \sigma b \sigma^{-1} \iff a\sigma = \sigma b$$

Ordre

Définition - Ordre d'un élément
Soit G un groupe fini d'élément neutre e et $x \in G$.
On appelle ordre de x, le nombre $m = \min\{k \in \mathbb{N} \mid \sigma^k(x) = x$.
On appelle ordre de G, le nombre $m = \min\{k \in \mathbb{N} \mid \sigma^k = \mathrm{id}\}$.

Analyse - Existence de l'ordre d'un élément
Cet ordre existe nécessairement car

$$\{x^k; k \in \mathbb{Z}\} \subset G$$

est fini, donc il existe $k_1 < k_2$ tel que $x^{k_1} = x^{k_2}$, donc $x^{k_2-k_1} = e$.
Plus précisément on a un idéal de $\mathbb{Z}$:

$$\{h \in \mathbb{Z} \mid x^h = e\} = \mathrm{ordre}(x) \cdot \mathbb{Z}$$

Car c'est un sous-groupe de $\mathbb{Z}$ (il suffit de faire des divisions euclidiennes…).
Puis G est fini, on a alors si $k = ppcm\{\mathrm{ordre}(x), x \in G\}$, $\sigma^k = \mathrm{id}$. Donc $\mathrm{ordre}(G) | k$.
La réciproque est également vraie.

Proposition - Ordre d'un cycle
Si c est un cycle de longueur p,
alors $c^p = \mathrm{id}$.
Mieux : p est l'ordre du cycle.

Démonstration
Notons $\sigma = (a_1\ a_2 \cdots a_p)$.
Alors pour tout $i \in \mathbb{N}_p$, $\forall\ k \in [\![0, p-1]\!]$,

$$\sigma_k(a_i) = a_{\overline{i+k}}$$

Donc : $\sigma_k(a_i) = a_i \iff \overline{i+k} = i \iff k \equiv 0[p]$ □

3. Décomposition d'une permutation

3.1. Partie génératrice d'un groupe

Dans cette partie, nous rappelons un peu de vocabulaire. Il est valable pour toute la théorie des groupes (et non uniquement pour les groupes de permutation).

Définition - Sous-groupe engendré par une partie
Soit $(G, \star)$ un groupe et S, une partie de G.
On appelle sous-groupe de G, engendré par S, le plus petit sous-groupe de G (au sens de l'inclusion) qui contient S.
On le note $< S >$.
On a donc la caractérisation suivante :

$$< S >< G \text{ et } \big(S \subset H, H < G\big) \Rightarrow < S > \subset H$$

Comme pour les espaces vectoriels, on dispose d'une description explicite de $< S >$:

Proposition - Description explicite
Soit $(G, \star)$ un groupe et S, une partie de G non vide.

$$< S >= \left\{x_1^{\epsilon_1} \star x_2^{\epsilon_2} \cdot \star x_n^{\epsilon_n}; n \in \mathbb{N}, \forall\ i \in \mathbb{N}_n, x_i \in S, \epsilon_i \in \{-1, 1\}\right\}$$

Démonstration
Notons $T = \{x_1^{\epsilon_1} \star x_2^{\epsilon_2} \cdot \star x_n^{\epsilon_n}; n \in \mathbb{N}, \forall\ i \in \mathbb{N}_n, x_i \in S, \epsilon_i \in \{-1, 1\}\}$. Alors
— $S \subset T$: $\forall\ x \in S$, on prend $n = 1$, $x_1 = x$ et $\epsilon_1 = 1$, on a $x \in H$.
— T est bien un sous-groupe de G.
T contient S donc est non vide.
Soit $t = x_1^{\epsilon_1} \star x_2^{\epsilon_2} \cdot \star x_n^{\epsilon_n}$ et $t' = x_1'^{\epsilon_1} \star x_2'^{\epsilon_2} \cdot \star x_m'^{\epsilon_m} \in T$.
alors $t \star t'^{-1} = x_1^{\epsilon_1} \star x_2^{\epsilon_2} \cdot \star x_n^{\epsilon_n} x_1'^{-\epsilon_1} \star x_2'^{-\epsilon_2} \cdot \star x_m'^{-\epsilon_n} \in T$.
— Soit H, sous-groupe de G, contenant S.
Soit $n \in \mathbb{N}$, et $\forall\ i \in \mathbb{N}_n$, $x_i \in S \subset H$ et enfin $\epsilon_j \in -1, 1$.
Alors comme H est un groupe, $\forall\ i \in \mathbb{N}_n$, $x_i^{\epsilon_i} \in H$, puis $x_1^{\epsilon_1} \star x_2^{\epsilon_2} \cdot \star x_n^{\epsilon_n} \in H$.
Donc $T \subset H$
T vérifie la propriété caractéristique : $T =< S >$ □

Exercice
Dans $(G, +) = \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$, on considère $r \in [\![0, n-1]\!]$.
Montrer que $< r >= G$ si et seulement si $r \wedge n = 1$

Correction
On applique le théorème de BÉZOUT.
Ce n'est pas trivial…

3.2. Décomposition en produit de cycles

Analyse - Quelques exemples
Pour $n \geqslant 3$ on a par exemple :

$$\begin{aligned}(1\ 2\ 3) &= (1\ 2) \circ (2\ 3) = \tau_{1,2} \circ \tau_{2,3} \\ &= (1\ 3) \circ (1\ 2) = \tau_{1,3} \circ \tau_{1,2}\end{aligned}$$

Si les cycles ne sont pas à supports disjoints :

Proposition - Chasles
Soit a_i, a_j, a_k distincts.
Alors $(a_j\ a_i) \circ (a_i\ a_k) = (a_j\ a_i\ a_k)$

Démonstration
$\sigma = (a_j\ a_i) \circ (a_i\ a_k)$
$\sigma(a_i) = a_k, \sigma(a_k) = a_j$ et $\sigma(a_j) = a_i$ □

Cette formule peut d'étendre à des cycles plus large.
Exercice
Montrer que $(a_1\ a_2\ a_3) \circ (a_3\ a_4\ a_1) = (a_2\ a_3\ a_4)$

Correction
$(a_1\ a_2\ a_3) \circ (a_3\ a_4\ a_1) = (a_2\ a_3\ a_1) \circ (a_1\ a_3\ a_4) = (a_2\ a_3)(a_3\ a_1)(a_1\ a_3)(a_3\ a_4) = (a_2\ a_3)(a_3\ a_4) = (a_2\ a_3\ a_4)$

Définition - Orbite de x
Soit σ une permutation de $[\![1, n]\!]$.
La relation définie sur $[\![1, n]\!]$ par

$$x \mathscr{R}_\sigma y \iff \exists k \in \mathbb{Z}, y = \sigma^k(x)$$

est une relation d'équivalence.
Pour $x \in [\![1, n]\!]$, il existe un unique $p \in \mathbb{N}^*$ tel que $x, \sigma(x), \ldots, \sigma^{p-1}(x)$ soient deux à deux distincts et $\sigma^p(x) = x$.
La classe d'équivalence de x pour la relation $\mathscr{R}_\sigma$ est alors l'ensemble $\{x, \sigma(x), \ldots, \sigma^{p-1}(x)\}$, appelé **orbite** de x.

Démonstration
On démontre juste l'existence de p.
Comme $\{\sigma^k(x), k \in \mathbb{N}\} \subset [\![1,n]\!]$, il s'agit d'un ensemble fini.
On note $k_1 < k_2 \in \mathbb{N}$ tels que $\sigma^{k_1}(x) = \sigma^{k_2}(x)$,
et donc comme σ est une bijection inversible :

$$x = (\sigma^{-1})^{k_1} \circ \sigma^{k_1}(x) = \sigma^{k_2-k_1}(x)$$

Donc p existe.
On peut montrer alors que $\{k \in \mathbb{Z} \mid \sigma^k(x) = x\}$ *est un sous-groupe de* $\mathbb{Z}$*, donc de la forme* $p\mathbb{Z}\ldots$ □

Exercice
Montrer qu'il s'agit bien d'une relation d'équivalence

Correction
Avec $k = 0$, $\mathscr{R}_\sigma$ est reflexive.
Avec $h = -k$, $\mathscr{R}_\sigma$ est symétrique.
Enfin, avec $h = k_1 + k_2$, $\mathscr{R}_\sigma$ est symétrique.

Théorème - Décomposition en produit de cycles à supports disjoints
Toute permutation autre que l'identité se décompose, de manière unique à l'ordre près des facteurs, en un produit de cycles (de longueur $\geqslant 2$) à supports deux à deux disjoints.
Plus précisément, ces cycles sont entièrement déterminés par σ : leur nombre est égal au nombre d'orbites non réduites à un élément de σ et ils sont égaux aux restrictions de σ à chacune des orbites.

Démonstration
Unicité : Supposons qu'il existe $c_1,\ldots,c_p$ cycles à supports deux à deux disjoints, de longueurs respectives $\ell_1,\ldots,\ell_p$ tels que $\sigma = \prod_{i=1}^{p} c_i$.
Soit $x \in [\![1,n]\!]$.
Si x appartient au support de c_{i_0} pour $i_0 \in [\![1,p]\!]$, alors il est invariant par les autres c_i (supports disjoints) et $\sigma(x) = c_{i_0}\left(\prod_{i\neq i_0} c_i\right)(x) = c_{i_0}(x)$, $\sigma(x)$ étant dans le support de c_{i_0}, on a alors de même $\sigma^2(x) = c_{i_0}^2(x)$ et ainsi de suite, d'où $c_{i_0} = (x\,\sigma(x)\cdots\sigma^{\ell_{i_0}-1}(x))$.
Si x n'appartient au support d'aucun c_i il est invariant par σ.
D'où l'unicité à l'ordre près (ils commutent car les supports sont disjoints).
Existence : Réutilisons ce qui précède pour construire la décomposition de σ.
Soit p le nombre d'orbites de σ de cardinal supérieur ou égal à 2, $p \geqslant 1$ car $\sigma \neq Id$. Par définition des classes d'équivalence, ces orbites sont deux à deux disjointes. Soit c_i le cycle obtenu par restriction de σ à la i-ième de ces orbites.
Posons $\sigma' = \prod_{i=1}^{p} c_i$.
Soit $x \in [\![1,n]\!]$ invarant par σ. L'orbite de x est $\{x\}$, donc x est invariant par tous les $c_i$et donc par σ'. D'où $\sigma(x) = \sigma'(x)$.
Soit $x \in [\![1,n]\!]$ non invariant par σ. Il existe alors un unique i_0 tel que x appartient au support de c_{i_0}. Par commutativité du produit des cycles c_i, on a $\sigma'(x) = c_{i_0}\left(\prod_{i\neq i_0}\right)(x) = c_{i_0}(x) = \sigma(x)$ (invariant par c_i pour $i \neq i_0$.
On en conclut que $\sigma = \sigma' = \prod_{i=1}^{p} c_i$. □

Savoir faire - Comment décrire une permutation en produit de cycles
On suppose que la permutations est écrite classiquement sous la forme d'une liste double.
On peut imaginer que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ s_1 & s_2 & s_3 & s_4 & \ldots \end{pmatrix}$ On procède, en plusieurs temps, en suivant le chemin…
- On est choisit librement premier élément du cycle : il ne doit pas être un point fixe.
  On le note k $\quad\Longrightarrow (k,\quad)$
- On se dirige alors en s_k. $\quad\Longrightarrow (k, s_k\quad)$
- On se dirige ensuite en $s(s_k)$. $\quad\Longrightarrow (k, s_k, s(s_k)\quad)$
- …
- On continue ainsi jusqu'à trouver à nouveau k.

Si la permutation considérée est « juste » un cycle, l'écriture est terminée.
Mais on ne sait jamais…

Sinon, on cherche alors parmi les nombres qui n'était pas dans le premier cycle, si certains ne sont pas des points fixes. Si c'est le cas, on commence ainsi un nouveau cycle, à support disjoint.

Exercice
Soit $A \in \mathscr{M}_n(\mathbb{K})$ une matrice qui possède exactement un 1 par ligne et par colonne et que des zéros sinon.
Montrer qu'il existe k tel que $A^k = I_n$.

Correction
Une telle matrice A est une matrice de permutation. On note s cette permutation.
Notons $d = PPCM(\ell_1,\ldots\ell_k)$, le PPCM des longueurs de chacune des k orbites de s.
Alors $s^d = \mathrm{id}$ et $A^d = I_n$.

3.3. Décompositions en produit de transpositions

Transpositions quelconques

On commence par une proposition :

Proposition - Décomposition
Un p-cycle est un produit (i.e. une composée) de $p-1$ transpositions :

$$(a_1\, a_2 \ldots a_p) = (a_1\, a_2)(a_2\, a_3)\ldots(a_{p-1}\, a_p)$$

Démonstration
Il suffit de faire le calcul. On note $\sigma = (a_1, a_2, \ldots a_p)$.
- si $i \notin \{a_1, a_2, \ldots a_p\}$, alors $\sigma(i) = i$.
  Et $\forall\, j \in [\![1, p-1]\!]$, $(a_j, a_{j+1})(i) = i$ car $i \neq a_j$ et $i \neq a_{j+1}$.
- si $i = a_j$ $(j \neq p)$ alors $\sigma(i) = \sigma(a_j) = a_{j+1}$.
  On a alors $(a_1\, a_2)(a_2\, a_3)\ldots(a_{p-1}\, a_p)(i) = (a_1\, a_2)(a_2\, a_3)\ldots(a_{j-1}\, a_j)(a_j\, a_{j+1})(a_j) = (a_1\, a_2)(a_2\, a_3)\ldots(a_{j-1}\, a_j)(a_{j+1} = a_{j+1}$.
- si $i = a_p$, alors $\sigma(i) = a_1$.
  Et, par récurrence : $(a_1\, a_2)(a_2\, a_3)\ldots(a_{p-1}\, a_p)(i) = (a_1\, a_2)(a_2\, a_3)\ldots(a_{p-2}\, a_{p-1})(a_{p-1}) = \cdots = (a_1\, a_2)(a_2\, a_3)\ldots(a_{k-1}\, a_k)(a_k) = (a_1\, a_2)(a_2) = a_1$

Ainsi, dans tous les cas $\sigma(i) = (a_1\, a_2)(a_2\, a_3)\ldots(a_{p-1}\, a_p)(i)$. □

On en déduit, associé avec la partie précédente

Théorème - Engendrement des transpositions
Toute permutation se décompose en produit de transpositions.
Autrement écrit : si on note T_n l'ensemble des transpositions de $\mathbb{N}_n$.
Alors $< T_n >= S_n$

Exemple - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 4 & 5 & 7 \end{pmatrix}$

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 4 & 5 & 7 \end{pmatrix} \\ &= (1,2,3)(4,6,5) \\ &= (1,2)(2,3)(4,6)(6,5) \end{aligned}$$

Exercice
Déterminer la permutation $(a_1\, a_p) \circ (a_1\, a_{p-1}) \circ \cdots \circ (a_1\, a_2)$ où les a_i sont des entiers tous distincts compris entre 1 et n, ainsi que la permutation $(a_1\, a_2 \ldots a_q) \circ (a_q\, a_{q+1} \ldots a_p)$ où $1 < q < p$.

Correction
$(a_1\, a_p) \circ (a_1\, a_{p-1}) \circ \cdots \circ (a_1\, a_2) = (a_p, a_1, a_2, \ldots a_{p-1})$.
$(a_1\, a_2 \ldots a_q) \circ (a_q\, a_{q+1} \ldots a_p) = (a_p, a_1, a_2, \ldots a_{q-1}, a_q, a_{q+1} \ldots a_{p-1})$.
Il n'y a vraiment pas unicité dans les décompositions.

Exercice
Soit $\tau = (a\, b) \in S_n$ et $\sigma = (a\, a_1\, a_2 \ldots a_p) \in S_n$ un cycle de longueur $p+1$. Donner la décomposition en produit de cycles à supports disjoints de $\tau\sigma$. Comparer le nombre

Pour aller plus loin - Jeu du Taquin (1)
Dans le jeu du taquin, on permute deux à deux une case d'une grilles de 15 cases et la case vide.



d'orbites de σ et celui de $\tau\sigma$.

Correction
$\tau\circ\sigma=(b,a,a_1,\dots a_p)$. Toujours une seule orbite, mais plus grosse…

Exercice
Pour $(i,j)\in[\![2,n]\!]^2$, calculer $\tau_{1i}\circ\tau_{1j}\circ\tau_{1i}$ et montrer que les transpositions de la forme τ_{1i} engendrent le groupe symétrique S_n (c'est-à-dire que toute permutation se décompose comme produit de transpositions de la forme τ_{1i}).

Correction
On notera déjà que comme $\tau_{1i}=\tau_{1i}^{-1}$, on étudie en fait le commutant de τ_{1i} et τ_{1j} : $\tau_{1i}^{-1}\circ\tau_{1j}\circ\tau_{1i}$. Il ne vaut pas $\tau_{i,j}$ a priori.
$\tau_{1i}\circ\tau_{1j}\circ\tau_{1i}=\tau_{i,j}$. Si $i=j$, on retrouve l'identité, ce qui est logique…

Transpositions $\tau_{i,i+1}$

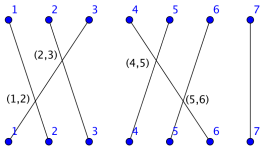
Analyse - Un deuxième algorithme?
La démonstration découle en deux temps :

1. Toute permutation est un produit unique de cycles disjoints
2. Tout cycle est un produit de transpositions

Mais ce qui pourrait être efficace : trouver un algorithme de décomposition. Idéalement, il pourrait être efficace (avec le moins de transpositions possibles)…
Il suffit de faire le graphe de la transformation et pour chaque croisement l'indiquer en marge par une transposition.
S'il y a un croisement de n segments ($n>3$), alors on retarde artificiellement l'un des croisements…

Exercice
Appliquer la méthode présentée pour exprimer à nouveau $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&6&4&5&7\end{pmatrix}$ en produit de transpositions.

Correction
La représentation graphique est la suivante :



On trouve alors $\sigma=(5,6)(1,2)(4,5)(2,3)$. (Pour mieux comprendre, on pourrait plus styliser le graphe).

Proposition - Décomposition par transposition simple
Toute permutation est le produit de transpositions de la forme $\tau_{i,i+1}$.
Autrement écrit :
Pour tout $\sigma\in\mathscr{S}_n$, il existe $i_1,\dots i_r\in\mathbb{N}_{n-1}$ tel que $\sigma=\tau_{i_1,i_1+1}\circ\cdots\circ\tau_{i_r,i_r+1}$.
Ou encore : si on note T_n^i l'ensemble des transpositions de la forme de $\tau_{i,i+1}$ de S_n.
Alors $<T_n^i>=S_n$

Exercice
A démontrer

Correction

4. Signature d'une permutation

4.1. Motivation : nombre d'inversions

Pour aller plus loin - Groupe alterné
L'ensemble des permutation de S_n dont la signature vaut 1 forme un sous-groupe de S_n (à démontrer). C'est le groupe alterné A_n. Il joue un rôle important en particulier dans l'étude des groupes…

Heuristique - Parité de changements
Il arrive, très souvent, qu'on s'intéresse au nombre de changement d'ordre dans une permutation.
On avait un ensemble bien ordonné $(1\,2\,\dots\,n)$ et en bout de course, il se trouve tout mélangé.
Combien de changement a-t-il fallut faire? Ce nombre ne peut pas être fixe, car deux transpositions identiques conduisent à la situation initiale. Donc le seul nombre auquel on peut avoir accès est la parité de ce nombre de changements.

Définition - Une première définition
Soit σ, une permutation de $\mathbb{N}_n$.
On appelle signature de σ, le nombre

$$\epsilon(\sigma)=\prod_{i<j}\text{signe}\big(\sigma(j)-\sigma(i)\big)$$

Pour aller plus loin - Avec les graphes
A chaque croisement de n brins correspond $\binom{n}{2}$ transpositions.
Il suffit donc de faire le graphe de la permutation, de compter le « nombre » K de tels croisements. La signature est alors $(-1)^K$

Exemple - Signature de $\begin{pmatrix}1&2&3&4&5\\1&3&5&4&2\end{pmatrix}$
Il y a 4 inversions d'ordre : $2-4=\sigma(5)-\sigma(4)$, $2-5=\sigma(5)-\sigma(3)$, $2-3=\sigma(5)-\sigma(2)$, $4-5=\sigma(4)-\sigma(3)$.
Donc $\epsilon(\sigma)=(-1)^4=1$.

Vers une formule générale.

Analyse - Calcul pour savoir si $i<j$
On cherche à savoir si le signe de $i<j$.
L'information est donnée par le signe de $(j-i)$. En terme de calcul, on a

$$\text{signe}(j-i)=\frac{j-i}{|j-i|}$$

Proposition - Formule (sans la fonction signe)
Soit σ, une permutation de $\mathbb{N}_n$.
Alors $\epsilon(\sigma)=\displaystyle\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}=\prod_{\{i,j\}\in\binom{\mathbb{N}_n}{2}}\frac{\sigma(j)-\sigma(i)}{j-i}$

Pour aller plus loin - Jeu du Taquin (2)
En fait les seuls permutations possibles au taquin conservent la signature ($\epsilon(\sigma)=1$).
En effet, il s'agit d'un produit de transposition de la forme $(i,16)$ et comme 16 doit reprendre sa place initiale en bout de course, il faut un nombre pair de telles transpositions. Toutes les configurations ne sont pas obtenables.
C'est la raison pour laquelle Sam Loyd (créateur du jeu) avait promis à la fin du XIX-ième siècle, mille dollars a qui réussissait à inverser les cases 14 et 15 (seulement). Ce qui est impossible car il s'agit d'une unique transposition, donc de signature égale à -1.

Démonstration
$\epsilon(\sigma)=\displaystyle\prod_{i<j}\text{signe}\big(\sigma(j)-\sigma(i)\big)=\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{|\sigma(j)-\sigma(i)|}$.
Comme σ est bijective, on trouve : $\displaystyle\prod_{i<j}(|\sigma(j)-\sigma(i)|)=\prod_{k=1}^{n-1}k!=\prod_{i<j}(j-i)$.
Donc : $\epsilon(\sigma)=\displaystyle\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}$ □

4.2. Propriété caractéristique

Théorème - Caractérisation de ϵ
ϵ est une application de S_n dans $\{-1,1\}$ telle que
- $\epsilon(\tau)=-1$ pour toute transposition τ ;
- $\epsilon(\sigma\sigma')=\epsilon(\sigma)\epsilon(\sigma')$ pour toutes permutations σ et σ'.

Elle est la seule application à vérifier ces propriétés.

Corollaire - Morphisme de groupes
ϵ est donc un morphisme de groupes, du groupe $(S_n, \circ)$ dans le groupe $(\{-1,1\}, \times)$.

Démonstration
ϵ est bien une application de S_n dans $\{-1,1\}$.
Si τ est la transposition $(i\ j)$, on suppose SPG que $i<j$.
alors, comme pour tout $k \neq i,j$, $\tau(k)=k$:

$$\epsilon(\tau) = \prod_{k=1}^{i-1} \frac{j-k}{i-k} \prod_{k=i+1}^{n} \frac{k-j}{k-i} \times \prod_{k=1}^{j-1} \frac{i-k}{j-k} \prod_{k=j+1}^{n} \frac{k-i}{k-j} \times \frac{i-j}{j-i} = -1$$

Soit σ, σ' deux permutations quelconques

$$\begin{aligned}\epsilon(\sigma\circ\sigma') &= \prod_{i<j} \frac{\sigma\circ\sigma'(j)-\sigma\circ\sigma'(i)}{j-i} = \prod_{i<j} \frac{\sigma\circ\sigma'(j)-\sigma\circ\sigma'(i)}{\sigma'(j)-\sigma'(i)} \times \frac{\sigma'(j)-\sigma'(i)}{j-i} \\ &= \prod_{i<j} \frac{\sigma\circ\sigma'(j)-\sigma\circ\sigma'(i)}{\sigma'(j)-\sigma'(i)} \times \prod_{i<j} \frac{\sigma'(j)-\sigma'(i)}{j-i} = \epsilon(\sigma')\times\epsilon(\sigma)\end{aligned}$$

On fait un changement de variable bijective : $(i', j') = (\sigma'(i), \sigma'(j))$.
Puisque toute permutation s'écrit comme produit de transposition. Il ne peut y avoir qu'au plus une application vérifiant les deux caractéristiques. □

4.3. Autres façons d'obtenir la signature de σ

Avec les transpositions

On exploite le morphisme de groupe :

Corollaire - Calcul de $\epsilon(\sigma)$
Soit $\sigma \in S_n$, $\sigma = \tau_1 \dots \tau_k$ une décomposition en transpositions.
Alors $\epsilon(\sigma) = (-1)^k$ (en particulier la parité de k est déterminée par σ).

Exemple - $\epsilon\left(\begin{pmatrix}1&2&3&4&5&6&7\\3&5&7&2&1&4&6\end{pmatrix}\right)$

Pour $\sigma = \begin{pmatrix}1&2&3&4&5&6&7\\3&5&7&2&1&4&6\end{pmatrix}$ on a $\sigma = (2,5)(2,4)(4,6)(6,7)(7,3)(1,3)$
d'où $\epsilon(\sigma) = (-1)^6 = 1$.

Avec les orbites

On décompose les orbites en produit de transpositions

Corollaire - Signature et décomposition de cycles
Soient $c_1, \dots, c_p$ des cycles à supports disjoints de longueurs respectives $\ell_1, \dots, \ell_p$. Alors la permutation $\sigma = c_1 c_2 \dots c_p$ a pour signature

$$\epsilon(\sigma) = (-1)^{\sum_{i=1}^{p}(\ell_i - 1)} = (-1)^{n-p}.$$

Démonstration
$\epsilon(\sigma) = \prod_{i=1}^{p} \epsilon(c_i)$.
On exploite le fait que chaque orbite de longueur ℓ est un produit de $\ell-1$ transpositions.
Donc $\epsilon(\sigma) = \prod_{i=1}^{p} (-1)^{\ell_i - 1}$. On ajoute les r points fixes, donc des cycles de longueurs 1. $\sum_{i=1}^{p}(\ell_i - 1) = \sum_{i=1}^{p+r}(\ell_i - 1) = \sum_{i=1}^{p+r} \ell_i - (p+r) = n-(p+r)$ □

Attention - Le nombre de cycle p
On insiste : dans la formule $\epsilon(\sigma) = (-1)^{n-p}$, p est le nombre de cycles qui décompose σ.
Il faut compter les cycles point fixe parmi ceux-ci!

Exemple - $\epsilon\left(\begin{pmatrix}1&2&3&4&5&6&7\\3&5&7&2&1&4&6\end{pmatrix}\right)$, avec les orbites

On a $\sigma = (1,3,7,6,4,2,5)$ on a $\epsilon(\sigma) = (-1)^{7-1} = 1$.

5. Bilan

Synthèse

⇝ On appelle permutation d'un ensemble E, toute application bijective de E dans E; le mot est reservé au situation où E est fini. Quitte à appeler $x_1, x_2 \dots x_n$ les éléments de E, une permutation est du type : $\forall\ i \in \mathbb{N}_n$, $\varphi : x_i \mapsto x_j$, qui se résume en $j = \sigma(i)$ avec $i, j \in \mathbb{N}_n$.
Finalement les permutations peuvent « se voir » comme des applications bijectives de $\mathbb{N}_n$ sur $\mathbb{N}_n$.

⇝ L'ensemble des applications forme un groupe avec la loi $\circ$.
Une fois passé la question : « comment coder (de plusieurs façons) les éléments de ce groupe? », nous voyons que toutes les permutations se décomposent :
— en produit de cycles (de manière unique)
— en produit de transpositions (non unique)

⇝ Bien que le nombre de transpositions qui décompose une permutation σ n'est pas unique, il n'est pas quelconque : sa parité est imposé par σ. Cette imposition s'appelle la signature de σ. Le groupe $(S_n, \circ)$ se décompose (toujours - pour tout $n \in \mathbb{N}$) donc en un sous-groupe le groupe alterné $(A_n, \circ)$ ($\sigma \in A_n \Leftrightarrow \epsilon(\sigma) = 1$), multiplié par l'image de ϵ (i.e. $\{-1,1\}$).
$\epsilon(\sigma)$ peut se calculer avec la décomposition en produit de cycles (ou orbites).

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Notation classique
— Savoir-faire - Permutation et graphe
— Savoir-faire - Comment décrire une permutation en produit de cycles

Notations

Notations	*Définitions*	*Propriétés*	*Remarq*
$\sigma = (a_1\ a_2 \cdots a_p)$	Cycle. $\forall\ i \in \mathbb{N}_{p-1}$, $\sigma(a_i) = a_{i+1}$ et $\sigma(a_p) = a_1$	Les cycles à supports disjoints commutent	$(a_p\ a_1\ a$
	$\forall\ i \in \mathbb{N}_{p-1}$, $\sigma(a_i) = a_{i+1}$ et $\sigma(a_p) = a_1$ enfin $\sigma(b) = b$ si $b \notin \{a_1, a_2 \dots a_p\}$ (support de σ)	σ se décompose en produit de cycles à support disjoints. $\sigma^p = \mathrm{id}$	$(a_1\ a_2\ a$
$< S >$	Plus petit sous-groupe contenant S	$< S >= H \iff [H$ groupe et $S \subset H'$ (groupe)$\Rightarrow H \subset H']$	$< \tau_{i,j} >$
$\epsilon(\sigma)$	Signature de σ	$\epsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^k = (-1)^{n-p}$	si $\sigma = \prod$ (τ trans

Retour sur les problèmes

137. S_3 est (le plus) petit groupe non commutatif (6 éléments).
138. Voir un cours de grands... ou sur wikipédia, ou avec un peu de chance un prochain DS...

139. Cela aide à mieux comprendre, pas forcément à être le plus rapide. Voir TD.

140. On appelle le rang d'un groupe G est le plus petit cardinal d'une partie génératrice de G :

$$\text{rg } G = \min\{|X| \mid < X >= G\}$$

Ici par exemple S_n est de rang 2.

141. La signature d'ordre 3 ne marche pas en toute généralité. D'ordre 4, en exploité les nombres i et $-i$?

Chapitre 30

Déterminants

Résumé -

Il s'agit d'élargir la définition du déterminant vue pour des matrices d'ordre $n = 2$ à tout ordre n.
Mais pour cela, nous faisons un détour vers les formes n-linéaires alternés. Il n'y a qu'une possibilité (à un facteur multiplicatif près). Et ainsi, on obtient beaucoup plus qu'une formule généralisée. On trouve une formule explicite et plein de petits trucs intéressants dont :

- *la formule polynomiale hyper-symétrique (d'où la référence au groupe des permutations $\mathfrak{S}_n$)*
- $\det(AB) = \det A \times \det B$
- *Par blocs :* $\det\begin{pmatrix} A & C \\ O & D \end{pmatrix} = \det A \times \det D$
- *une formule explicite (à usage théorique, exclusivement...) du calcul de A^{-1}...*

Sommaire

1. Problèmes 608
2. Applications multilinéaires 609
2.1. Définitions 609
2.2. Expression d'une forme n-linéaire alternée relativement à une base donnée 610
3. Déterminant 611
3.1. Déterminant de n vecteurs 611
3.2. Déterminant d'un endomorphisme 613
3.3. Déterminant d'une matrice 614
3.4. Conséquences pratiques pour le calcul des déterminants 616
4. Calculs et applications des déterminants 617
4.1. Formule de Cramer pour inverser un système 617
4.2. Déterminant de matrices par blocs 617
4.3. Développement suivant une ligne ou une colonne . 617
4.4. Calcul de l'inverse 620
4.5. Déterminant comme fonction polynomiale 621
5. Bilan 622

1. Problèmes

Un seul problème nous motive ici, mais il conduit à divers sous-problème. Existe-t-il une fonction qui pour une matrice donnée indique, par un calcul, si oui ou non, la matrice est inversible ?

? Problème 126 - Réflexion selon la dimension

Nous savons qu'une telle fonction existe pour les matrices de taille 2. Il s'agit de

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

$\det(A) = 0$ si et seulement si A n'est pas inversible.
Par ailleurs, on sait que le rang d'une matrice est égal à la taille de la plus grande sous-matrice inversible.
Est-il possible, de créer par récurrence la fonction $\det_n$ (recherchée) pour une matrice de rang n, connaissant l'expression de $\det_{n-1}$?

? Problème 127 - Réflexion selon la famille des colonnes

A est inversible si et seulement si $(C_1(A),\dots C_n(A))$ est une famille génératrice de $\mathcal{M}_{n,1}(\mathbb{K})$.
La fonction $\det(A)$ recherchée doit donc pouvoir être liée à une fonction sur les familles de vecteurs qui indiquent si une telle famille est une base.

$$d(X_1,\dots X_n) = 0 \Longrightarrow (X_1,\dots X_n) \text{ libre/base/génératrice de } \mathcal{M}_{n,1}(\mathbb{K})$$

Que dire de d, si $X_i = 0$ ou si X_j est une combinaison linéaire des autres $(X_k)_{k\neq j}$?
Que dire de d si l'on échange deux vecteurs X_i et X_j ?

? Problème 128 - Signification de la valeur du déterminant

Supposons qu'on ait trouvé $\det : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ tel que $\det(A) = 0$ si et seulement si A non inversible.
Mais alors que dire de A par rapport à A' si $\det(A) = 1$ et $\det(A') = 10$?

? Problème 129 - Multiplicativité de la fonction déterminant.

Supposons qu'on ait trouvé $\det : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ tel que $\det(A) = 0$ si et seulement si A non inversible.
Que peut-on dire de $\det(AB)$ en fonction de $\det(A)$ et de $\det(B)$?

? Problème 130 - Système de Cramer. Inversion d'une matrice avec le déterminant

On cherche un vecteur X solution du système $AX = b$.
Peut-on trouver exprimer (au moins théoriquement) chaque coordonnée x_i de X en fonction de $\det A$ et de quelque chose d'autre ? Quoi ? Est-ce un calcul simple ?
Et plus largement (mais de manière équivalente), peut-on exprimer (au

moins théoriquement avec un calcul simple) A^{-1} en fonction de A et $\det(A)$? En fonction d'autres nombres ?

2. Applications multilinéaires

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

2.1. Définitions

Définition - Application n-linéaire
Soient E, F deux $\mathbb{K}$-espaces vectoriels.
On dit que $\Phi : E^n \to F$ est une application n-linéaire si

$$\forall (X_1,\dots,X_n) \in E^n, \forall (X,Y) \in E^2, \forall (\lambda,\mu) \in \mathbb{K}^2, \forall\, i \in [\![1,n]\!]$$
$$\Phi(X_1,\dots,X_{i-1},\lambda X+\mu Y, X_{i+1},\dots,X_n)$$
$$= \lambda\Phi(X_1,\dots,X_{i-1},X,X_{i+1},\dots,X_n) + \mu\Phi(X_1,\dots,X_{i-1},Y,X_{i+1},\dots,X_n)$$

c'est-à-dire si $\forall i \in [\![1,n]\!], \Phi_i : X \mapsto \Phi(X_1,\dots,X_{i-1},X,X_{i+1},\dots,X_n)$ est linéaire.
On note $\mathscr{L}_n(E,F)$ l'ensemble des applications n-linéaires de E^n dans F.

Définition - Forme n-linéaire
Si Φ est une application n-linéaire de E^n dans $\mathbb{K}$,
on dit que Φ est une forme n-linéaire sur E. ($\mathscr{L}_n(E,\mathbb{K}) = \mathscr{L}_n(E)$)

Définition - Forme n-linéaire symétrique ou antisymétrique
On dit que Φ, forme n-linéaire sur E, est :
— symétrique si

$$\forall \sigma \in S_n, \forall (X_1,\dots,X_n) \in E^n, \quad \Phi(X_{\sigma(1)},\dots,X_{\sigma(n)}) = \Phi(X_1,\dots,X_n)$$

— antisymétrique si

$$\forall \sigma \in S_n, \forall (X_1,\dots,X_n) \in E^n, \quad \Phi(X_{\sigma(1)},\dots,X_{\sigma(n)}) = \epsilon(\sigma)\Phi(X_1,\dots,X_n)$$

Proposition - Caractérisation et permutation
Φ est symétrique si et seulement si,
lorsque l'on échange deux vecteurs, le résultat est inchangé.
Φ est antisymétrique si et seulement si,
lorsque l'on échange deux vecteurs, le résultat se transforme en son opposé.

Démonstration
C'est immédiat pour les deux sens directs.
Pour les réciproques (formes symétriques ou antisymétriques), cela provient de la décomposition d'une permutation en produit de transpositions. □

Définition - Forme n-linéaire alternée
Une forme n-linéaire Φ sur E est dite alternée si
$\forall (X_1,\dots,X_n) \in E^n, \forall (i,j) \in [\![1,n]\!]^2, i \neq j,$
$X_i = X_j \Rightarrow \Phi(X_1,\dots,X_i,\dots,X_j,\dots,X_n) = 0$

Histoire - Bourbaki et déterminant.
L'exposition faite ici sur la notion du déterminant suit une forme très moderne de la pensée. Elle remonte à la période de Nicolas Bourbaki. Nous encourageons le lecteur à découvrir qui est Nicolas Bourbaki…

Théorème - Equivalence : alternée et antisymétrique
Soit Φ une forme n-linéaire sur E. Alors on a

$$\Phi \text{ antisymétrique} \iff \Phi \text{ alternée.}$$

Démonstration
Φ est antisymétrique,
$\Longrightarrow \Phi(X_1,\dots,X_i,\dots,X_n) = -\Phi(X_1,\dots,X_i,\dots,X_i,\dots,X_n)$
$\Longrightarrow \Phi(X_1,\dots,X_i,\dots,X_i,\dots,X_n) = 0$ dès que $i = j$
$\Longrightarrow \Phi$ est alternée.
Φ est alternée,
$\Longrightarrow \forall\, i,j \in \mathbb{N}_n, \Phi(\cdot,X_i,\cdot,X_j,\cdot)+\Phi(\cdot,X_j,\cdot,X_i,\cdot) = \Phi(\cdot,X_i,\cdot,X_j,\cdot)+\Phi(\cdot,X_i,\cdot,X_i,\cdot)+\Phi(\cdot,X_j,\cdot,X_j,\cdot)+\Phi(\cdot,X_j,\cdot,X_i,\cdot) = \Phi(\cdot,X_i+X_j,\cdot,X_i+X_j,\cdot) = 0$, par linéarité
$\Longrightarrow \Phi$ est antisymétrique □

2.2. Expression d'une forme n-linéaire alternée relativement à une base donnée

On sait qu'une application linéaire est parfaitement définie par l'image d'une base. Qu'en est-il d'une forme n-linéaire (antisymétrique) ?

Analyse - Ecriture sur une base pour une forme alternée
Soient E un $\mathbb{K}$-e.v. de dimension $n \geqslant 2$, $\mathscr{E} = (e_1,\dots,e_n)$ une base de E, $\Phi \in \mathscr{A}_n(E)$, $(X_1,\dots,X_n) \in E^n$.

$$\begin{aligned}
\Phi(X_1,\dots,X_n) &= \Phi\Big(\sum_{i_1=1}^n x_{i_1 1}e_{i_1},\dots,\sum_{i_n=1}^n x_{i_n n}e_{i_n}\Big)\\
&= \sum_{i_1=1}^n x_{i_1 1}\Phi\Big(e_{i_1},\sum_{i_2=1}^n x_{i_2 2}e_{i_2},\dots,\sum_{i_n=1}^n x_{i_n n}e_{i_n}\Big) \text{ par linéarité par rapport à la première v}\\
&= \sum_{i_1=1}^n x_{i_1 1}\sum_{i_2=1}^n x_{i_2 2}\Phi\Big(e_{i_1},e_{i_2},\dots,\sum_{i_n=1}^n x_{i_n n}e_{i_n}\Big) \text{ par linéarité par rapport à la deuxième}\\
&\vdots\\
&= \sum_{i_1=1}^n\sum_{i_2=1}^n\cdots\sum_{i_n=1}^n x_{i_1 1}x_{i_2 2}\dots x_{i_n n}\Phi\Big(e_{i_1},e_{i_2},\dots,e_{i_n}\Big)\\
&= \sum_{\sigma:[\![1,n]\!]\to[\![1,n]\!]} x_{\sigma(1),1}x_{\sigma(2),2}\dots x_{\sigma(n)n}\Phi(e_{\sigma(1)},\dots,e_{\sigma(n)})
\end{aligned}$$

car $(1,\dots,n) \mapsto (i_1,\dots,i_n)$ définit une application σ, et une seule, de $[\![1,n]\!]$ dans $[\![1,n]\!]$.

Φ est alternée donc σ non injective $\Rightarrow \Phi(e_{\sigma(1)},\dots,e_{\sigma(n)}) = 0$ et σ étant une application de $[\![1,n]\!]$ fini dans lui même,

$$\sigma \text{ injective} \Leftrightarrow \sigma \text{ bijective} \Leftrightarrow \sigma \in \mathfrak{S}_n$$

d'où

$$\begin{aligned}
\Phi(X_1,\dots,X_n) &= \sum_{\sigma\in\mathfrak{S}_n} x_{\sigma(1),1}x_{\sigma(2),2}\dots x_{\sigma(n)n}\Phi(e_{\sigma(1)},\dots,e_{\sigma(n)})\\
&= \sum_{\sigma\in\mathfrak{S}_n} x_{\sigma(1),1}x_{\sigma(2),2}\dots x_{\sigma(n)n}\epsilon(\sigma)\Phi(e_1,\dots,e_n) \text{ car } \Phi \text{ antisymétrique}
\end{aligned}$$

Cette analyse donne la démonstration de la proposition suivante :

Proposition - Ecriture selon une base
Soient E un $\mathbb{K}$-e.v. de dimension $n \geqslant 2$, $\mathscr{E} = (e_1,\dots,e_n)$ une base de E.
On considère $\Phi \in \mathscr{A}_n(E)$ (forme n-linéaire alternée).
Soit $(X_1,\dots,X_n) \in E^n$. Alors

$$\Phi(X_1,\dots,X_n) = \sum_{\sigma\in\mathfrak{S}_n} x_{\sigma(1),1}x_{\sigma(2),2}\dots x_{\sigma(n)n}\epsilon(\sigma)\Phi(e_1,\dots,e_n)$$

où $\forall\ j \in \mathbb{N}_n,\ X_j = \sum_{i=1}^{n} x_{i,j} e_i$

3. Déterminant

3.1. Déterminant de n vecteurs

Définition - Déterminant de n vecteurs
Soient E un $\mathbb{K}$ev de dimension n, $\mathscr{E} = (e_1, \dots, e_n)$ une base de E.
Soient $X_1, \dots, X_n$ n vecteurs de E, $X_j = \begin{pmatrix} x_{1j} \\ \vdots \\ x_{nj} \end{pmatrix}_{\mathscr{E}}$.
On appelle déterminant de $(X_1, \dots, X_n)$ dans la base $\mathscr{E}$ le scalaire

$$\det_{\mathscr{E}}(X_1, \dots, X_n) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) x_{\sigma(1),1} \dots x_{\sigma(n),n}.$$

On note

$$\det_{\mathscr{E}}(X_1, \dots, X_n) = \begin{vmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{vmatrix}.$$

Remarque - Pour $n = 2$ ou $n = 3$ on a
Comme les permutations de $\{1,2\}$ sont $\sigma_1 = \mathrm{id}$, de signature égale à 1 et $\sigma_2 = (1,2)$ de signature égale à -1, on a

$$\begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix} = +1 x_{1,1} x_{2,2} - 1 x_{2,1} x_{1,2}$$

C'est la formule bien connue.
Comme les permutations de $\{1,2,3\}$ sont $\sigma_1 = \mathrm{id}$, $\sigma_2 = (1,3,2)$ et $\sigma_3 = (1,2,3)$ de signature égale à 1 et $\sigma_4 = (1,2)$, $\sigma_5 = (1,3)$ et $\sigma_6 = (2,3)$ de signature égale à -1, on a

$$\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix} = +1 x_{1,1} x_{2,2} x_{3,3} + x_{3,1} x_{1,2} x_{2,3} + x_{2,1} x_{3,2} x_{1,3} - 1 x_{2,1} x_{1,2} x_{3,3} - x_{1,3} x_{2,2} x_{3,1} - x_{1,1} x_{2,3} x_{3,2}$$

C'est la formule moins bien connue.

Histoire - Découverte
La notion de déterminant a été découverte par Leibniz. Il cherchait une méthode (la plus abstraite possible) pour résoudre un système linéaire de n équations à n inconnues (avec $n \leqslant 5$). Dans ce cas, la notion de déterminant émerge naturellement. Il a alors démontré toutes les formules qui suivent sauf $\det(A \times B) = \det(A)\det(B)$.
Très étonnement, exactement au même moment, dans le Japon replié sur lui-même, le mathématicien Seki Kowa (1642-1708) faisait des découvertes comparables…

Théorème - Propriété (essentielle) du déterminant
Soient E un $\mathbb{K}$-e.v. de dimension n, $\mathscr{E} = (e_1, \dots, e_n)$ une base de E. Alors

$$\begin{array}{rccc} \det_{\mathscr{E}} : & E^n & \to & \mathbb{K} \\ & (X_1, \dots, X_n) & \mapsto & \det_{\mathscr{E}}(X_1, \dots, X_n) \end{array}$$

est une forme n-linéaire alternée telle que $\det_{\mathscr{E}}(e_1, \dots, e_n) = 1$.

Démonstration

- $\det_{\mathscr{E}}$ est n-linéaire :

$$\begin{aligned} \det_{\mathscr{E}}(X_1, \dots, \lambda X_i + \mu Y_i, \dots, X_n) &= \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) x_{\sigma(1),1} \dots (\lambda x_{\sigma(i),i} + \mu y_{\sigma(i),i}) \dots x_{\sigma(n)n} \\ &= \lambda \det_{\mathscr{E}}(X_1, \dots, X_i, \dots, X_n) + \mu \det_{\mathscr{E}}(X_1, \dots, Y_i, \dots, X_n) \end{aligned}$$

On obtient ainsi la linéarité par rapport à la i-ième variable.

- $\det_{\mathscr{E}}$ est alternéeé :
Soit $i \neq j$ tels que $X_i = X_j$ et soit $\tau = \tau_{i,j}$. Notons $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \epsilon(\sigma) = +1\}$, alors l'application

$$\begin{array}{ccc} \mathfrak{A}_n & \to & \mathfrak{S}_n \setminus \mathfrak{A}_n \\ \sigma & \mapsto & \sigma \circ \tau \end{array}$$

est une bijection et $\mathfrak{S}_n \setminus \mathfrak{A}_n = \{\sigma\tau, \sigma \in \mathfrak{A}_n\}$ d'où

$$\det_{\mathscr{E}}(X_1, \dots, X_n) = \sum_{\sigma \in \mathfrak{A}_n} \prod_{k=1}^{n} x_{\sigma(k),k} - \sum_{\sigma \in \mathfrak{A}_n} \prod_{k=1}^{n} x_{\sigma\tau(k),k}.$$

Or

si $k = i$, $x_{\sigma\tau(k),k} = x_{\sigma(j),i} = x_{\sigma(j),j}$ car $X_i = X_j$
si $k = j$, $x_{\sigma\tau(k),k} = x_{\sigma(i),j} = x_{\sigma(i),i}$
et pour $k \neq i, j$, $x_{\sigma\tau(k),k} = x_{\sigma(k),k}$

d'où

$$\prod_{k=1}^{n} x_{\sigma(k),k} = \prod_{k=1}^{n} x_{\sigma\tau(k),k}$$

et $\det_{\mathscr{E}}(X_1, \dots, X_n) = 0$.
- $\det_{\mathscr{E}}(e_1, \dots, e_n) = 1$:

$$\det_{\mathscr{E}}(e_1, \dots, e_n) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{k=1}^{n} \delta_{\sigma(k),k} = 1$$

car $\epsilon(Id) = 1$ et $\prod_{k=1}^{n} \delta_{\sigma(k),k} = 0$ si $\sigma \neq Id$ (il existe alors k tel que $\delta_{\sigma(k),k} = 0$).

□

Théorème - Structure algébrique de $\mathscr{A}_n(E)$
Soient E un $\mathbb{K}$-e.v. de dimension n, $\mathscr{E} = (e_1, \dots, e_n)$ une base de E.
Alors l'ensemble $\mathscr{A}_n(E)$ des formes n-linéaires alternées est une droite vectorielle, engendrée par $\det_{\mathscr{E}}$.
$\det_{\mathscr{E}}$ est l'unique forme n-linéaire alternée Φ telle que $\Phi(e_1, \dots, e_n) = 1$, les autres formes n-linéaires alternées lui sont proportionnelles.

Démonstration
Soit $n \geqslant 2$. Soient $\Phi \in \mathscr{A}_n(E)$, $(X_1, \dots, X_n) \in E^n$. On a déjà vu que

$$\Phi(X_1, \dots, X_n) = \sum_{\sigma \in \mathfrak{S}_n} x_{\sigma(1),1} x_{\sigma(2),2} \dots x_{\sigma(n)n} \epsilon(\sigma) \Phi(e_1, \dots, e_n)$$

d'où

$$\Phi(X_1, \dots, X_n) = \Phi(e_1, \dots, e_n) \det_{\mathscr{E}}(X_1, \dots, X_n)$$

soit $\Phi = \Phi(e_1, \dots, e_n)\det_{\mathscr{E}}$; d'où $\mathscr{A}_n(E) \subset \mathrm{vect}(\det_{\mathscr{E}})$.
On vérifie aisément que $\forall \lambda \in \mathbb{K}, \Phi = \lambda \det_{\mathscr{E}}$ est n-linéaire alternée de E^n dans $\mathbb{K}$
d'où $\mathscr{A}_n(E) = \mathrm{vect}(\det_{\mathscr{E}})$ est un $\mathbb{K}$-espace vectoriel de dimension 1 et

$$\Phi(e_1, \dots, e_n) = 1 \Leftrightarrow \Phi = \det_{\mathscr{E}}.$$

□

Pour aller plus loin - Valeur numérique du déterminant
Il est dommage de réduire l'intérêt du déterminant : sa valeur exacte est une information plus importante (et plus précise) que celui de savoir s'il est nul ou non.
En dimension 2, $\det_{\mathscr{E}}(\vec{u}, \vec{v})$ donne la valeur du double de l'aire du triangle de côté $\vec{u}$ et $\vec{v}$. On retrouve bien que le déterminant est nul si et seulement si ces deux vecteurs sont colinéaires.
En dimension 3, il s'agit de la valeur (orientée) du volume élémentaire porté par les trois vecteurs $\vec{u}$, $\vec{v}$ et $\vec{w}$.
De manière générale, le déterminant $\det_{\mathscr{E}}(\mathscr{B})$ indique la valeur du « n-volume » élémentaire définie par les vecteurs de $\mathscr{B}$ dans $\mathscr{E}$.
Cela donne un sens à l'inégalité d'Hadamard :

$$\det_{\mathscr{E}}(\mathscr{B}) \leqslant \prod_{u \in \mathscr{B}} \|u\|_{2,E}$$

Théorème - Changement de base
Soient E un $\mathbb{K}$-e.v. de dimension n, $\mathscr{E} = (e_1, \dots, e_n)$ et $\mathscr{E}' = (e'_1, \dots, e'_n)$ des bases de E. Soit $(X_1, \dots, X_n) \in E^n$. Alors

$$\det_{\mathscr{E}'}(X_1, \dots, X_n) = \det_{\mathscr{E}'}(e_1, \dots, e_n) \times \det_{\mathscr{E}}(X_1, \dots, X_n) \qquad (*)$$

c'est-à-dire

$$\det_{\mathscr{E}'} = \det_{\mathscr{E}'}(\mathscr{E}) \times \det_{\mathscr{E}}$$

Démonstration
$\det_{\mathscr{E}'}$ est une forme n-linéaire alternée d'où $\det_{\mathscr{E}'} = \lambda \det_{\mathscr{E}}$ et $\det_{\mathscr{E}'}(\mathscr{E}) = \lambda \det_{\mathscr{E}}(\mathscr{E}) = \lambda$. □

Théorème - Caractérisation des bases
Soient E un $\mathbb{K}$-e-v. de dimension n, $\mathscr{E}$ une base de E, $\mathscr{B} = (X_1, \dots, X_n)$ une famille de n vecteurs de E. Alors

$$\mathscr{B} \text{ base de } E \iff \det_{\mathscr{E}}(\mathscr{B}) \neq 0$$

Démonstration
Si $\mathscr{B}$ n'est pas une base, alors elle n'est pas libre.
Il existe i tel que X_i est combinaison linéaire des X_j pour $j \neq i$.
Dans le calcul de $\det \mathscr{B}$, on remplace alors X_i par cette combinaison linéaire.
On applique la linéarité, on retrouve une CL de déterminants avec deux colonnes identiques
Donc le déterminant recherché est nul.
Ainsi $\det_{\mathscr{E}}(\mathscr{B}) = 0$
Si $\mathscr{B}$ est une base, alors on applique la formule précédente en $(X_i) = \mathscr{B}$,
on a donc $1 = \det_{\mathscr{B}}(\mathscr{E}) \times \det_{\mathscr{E}} \mathscr{B}$.
Nécessairement, $\det_{\mathscr{E}} \mathscr{B} \neq 0$ □

Définition - Orientation d'un espace
Soit $\mathscr{B}_0$ une base donnée de E et $\mathscr{B}$ une autre base. On sait que $\det_{\mathscr{B}_0}(\mathscr{B}) \neq 0$.
Les bases de E se classent donc en deux ensembles : celles telles que $\det_{\mathscr{B}_0}(\mathscr{B}) > 0$ et celles telles que $\det_{\mathscr{B}_0}(\mathscr{B}) < 0$.
On oriente donc E en choisissant une base $\mathscr{B}_0$ de référence qui sera dite directe,
les bases $\mathscr{B}$ telles que $\det_{\mathscr{B}_0}(\mathscr{B}) > 0$ sont dites directes,
les bases $\mathscr{B}$ telles que $\det_{\mathscr{B}_0}(\mathscr{B}) < 0$ sont dites indirectes.

Pour aller plus loin - Avoir même orientation
Il s'agit d'une relation d'équivalence, qui partitionne l'ensemble des bases en deux familles disjointes : les bases directes et les bases indirectes

3.2. Déterminant d'un endomorphisme

Définition - Déterminant d'un endomorphisme
Soient E un $\mathbb{K}$-ev de dimension n, $\mathscr{E} = (e_1, \dots, e_n)$ une base de E.
Soit $u \in \mathscr{L}(E)$.
Le scalaire $\det_{\mathscr{E}}(u(e_1), \dots, u(e_n))$ est indépendant de $\mathscr{E}$. On le note $\det(u)$ ou $\det u$ (déterminant de l'endomorphisme u) et

$$\forall (X_1, \dots, X_n) \in E^n, \det_{\mathscr{E}}(u(X_1), \dots, u(X_n)) = \det(u) \times \det_{\mathscr{E}}(X_1, \dots, X_n) \qquad (**)$$

Il faut faire une démonstration, bien que ce soit une définition : l'indépendance selon la base

Démonstration
On considère

$$f_u : \begin{array}{ccc} E^n & \to & \mathbb{K} \\ (X_1, \dots, X_n) & \mapsto & \det_{\mathscr{E}}(u(X_1), \dots, u(X_n)) \end{array}$$

On vérifie que f_u est n-linéaire, alternée (car $X_i = X_j \Rightarrow u(X_i) = u(X_j)$). f_u vérifie donc

$$f_u(X_1, \dots, X_n) = f_u(e_1, \dots, e_n) \times \det_{\mathscr{E}}(X_1, \dots, X_n)$$

d'où

$$\det_{\mathscr{E}}(u(X_1), \dots, u(X_n)) = \det_{\mathscr{E}}(u(\mathscr{E})) \times \det_{\mathscr{E}}(X_1, \dots, X_n)$$

On a alors appliqué $(*)$ avec $u(X_i)$ au lieu de X_i Soit $\mathscr{E}' = (e'_1, \dots, e'_n)$ une autre base de E. On a alors

$$\det_{\mathscr{E}}(u(\mathscr{E}')) = \det_{\mathscr{E}}(u(\mathscr{E})) \times \det_{\mathscr{E}}(\mathscr{E}')$$

or $\det_{\mathscr{E}'} = \det_{\mathscr{E}'}(\mathscr{E}) \times \det_{\mathscr{E}}$ d'où

$$\begin{aligned} \det_{\mathscr{E}'}(u(\mathscr{E}')) &= \det_{\mathscr{E}'}(\mathscr{E}) \times \det_{\mathscr{E}}(u(\mathscr{E}')) \\ &= \det_{\mathscr{E}'}(\mathscr{E}) \times \det_{\mathscr{E}}(u(\mathscr{E})) \times \det_{\mathscr{E}}(\mathscr{E}') \\ &= \det_{\mathscr{E}'}(\mathscr{E}') \times \det_{\mathscr{E}}(u(\mathscr{E})) \\ &= \det_{\mathscr{E}}(u(\mathscr{E})) \end{aligned}$$

□

Théorème - Déterminant et inverse d'endomorphisme
Soient E un $\mathbb{K}$-e.v. de dimension n, $u \in \mathscr{L}(E)$.
On a $u \in GL(E) \Leftrightarrow \det u \neq 0$.

Démonstration
On a la suite d'équivalences suivantes :

$$\begin{aligned} u \in GL(E) &\iff (u(e_1), \dots, u(e_n)) \text{ base de } E \\ &\iff \det_{\mathscr{E}}(u(e_1), \dots, u(e_n)) \neq 0 \\ &\iff \det u \neq 0 \end{aligned}$$

□

Proposition - Premiers résultats
Soient $u, v \in \mathscr{L}(E)$, $\lambda \in \mathbb{K}$ où E est un $\mathbb{K}$-e.v. de dimension n. Alors
— $\det Id_E = 1$
— $\det(\lambda u) = \lambda^n \det u$
— $\det(u \circ v) = \det u \times \det v$
— Si $u \in GL(E)$ alors $\det(u^{-1}) = \dfrac{1}{\det u}$

Démonstration
• $\det_{\mathscr{E}}(e_1, \dots, e_n) = 1 \Rightarrow \det Id_E = \det_{\mathscr{E}}(Id(e_1), \dots, Id(e_n)) = 1$.
• $\det(\lambda u) = \det_{\mathscr{E}}(\lambda u(e_1), \dots, \lambda u(e_n)) = \lambda^n \det u$ car n-linéaire.
• Si $v \notin GL(E)$, alors $u \circ v$ non plus. On a $\det v = 0 = \det(u \circ v) = \det u \times \det v$.
Si $v \in GL(E)$, $\det(u \circ v) = \det_{\mathscr{E}}(u(v(e_1)), \dots, u(v(e_n))) = \det u \times \det_{\mathscr{E}}(v(e_1), \dots, v(e_n)) = \det u \times \det v$
$(**)$ avec v car $v(\mathscr{B})$ est bien une base.
• Enfin si u est inversible, alors $u^{-1} \circ u = Id_E$ donc d'après la proposition précédente $\det(u^{-1} \circ u) = \det(u^{-1}) \det(u) = 1$. □

Attention - Non linéarité
$\det(u + v)$ est en général différent de $\det u + \det v$.
Contre-exemple à avoir en tête :
$\det(Id_E + Id_E) = \det(2Id_E) = 2^n \neq 1 + 1$ pour $n \geqslant 2$.

Remarque - Morphisme de groupes
L'application

$$\det : \begin{array}{ccc} (GL(E), \circ) & \to & (\mathbb{K}^*, \times) \\ u & \mapsto & \det u \end{array}$$

est un morphisme de groupe ; c'est ce que signifie la dernière propriété.
Exercice
Montrer que $\mathscr{SL}(E) = \{u \in \mathscr{L}(E) \mid \det(u) = 1\}$ est un groupe.
On l'appelle le groupe spécial linéaire.

Correction
On montre qu'il s'agit d'un sous-groupe de $\mathscr{GL}(E)$, les éléments inversibles de l'anneau $(\mathscr{L}(E), +, \circ)$.
— $\mathrm{id}_E \in \mathscr{SL}(E)$
— Si $u, v \in \mathscr{SL}(E)$, alors $uv^{-1} \in \mathscr{GL}(E)$ et $\det(uv^{-1}) = \frac{\det u}{\det v} = 1$

3.3. Déterminant d'une matrice

Définition - Déterminant d'une matrice
Soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n} \in \mathscr{M}_n(\mathbb{K})$.
On note $\mathscr{E} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$ et $C_1, \dots, C_n$ les vecteurs colonnes de A (éléments de $\mathbb{K}^n$).

On pose alors

$$\det A = \det_{\mathscr{E}}(C_1,\dots,C_n) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n} a_{\sigma(i)i}, \text{ noté } \det A = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

Truc & Astuce pour le calcul - Cas $n=2$ ou $n=3$

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{array}{l} a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} \\ \quad - a_{13}a_{22}a_{31} - a_{23}a_{32}a_{11} - a_{33}a_{12}a_{21}. \end{array}$$

(règle de Sarrus).

Théorème - Commutativité de det **et de** $u \mapsto \mathscr{M}_{\mathscr{B}}(u)$
Soient E un $\mathbb{K}$-e.v. de dimension n, $\mathscr{E}$ une base de E, $u \in \mathscr{L}(E)$ et $A = \mathscr{M}(u,\mathscr{E})$. Alors

$$\det u = \det A.$$

Démonstration
$\det u = \det_{\mathscr{E}}(u(e_1),\dots,u(e_n))$.

Or par définition on a $u(e_j) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}_{\mathscr{E}}$, donc

$$\det u = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n} a_{\sigma(i)i} = \det A.$$

□

Proposition - Premières propriétés
Soient $A, B \in \mathscr{M}_n(\mathbb{K})$, $\lambda \in \mathbb{K}$. Alors

- $\det I_n = 1$
- $\det(\lambda A) = \lambda^n \det A$
- $\det(AB) = \det A \times \det B$
- A est inversible si et seulement si $\det A \neq 0$ et alors $\det(A^{-1}) = \frac{1}{\det A}$
- deux matrices semblables ont même déterminant
- $\det({}^tA) = \det A$

Démonstration
Soient u et v les endomorphismes de $\mathbb{K}^n$ canoniquement associés à A et B.

- $\det I_n = \det Id_{\mathbb{K}^n} = 1$
- $\det(\lambda A) = \det(\lambda u) = \lambda^n \det u = \lambda^n \det A$
- $\det(AB) = \det(u\circ v) = \det u \times \det v = \det A \times \det B$
- A inversible $\Leftrightarrow u \in GL(\mathbb{K}^n) \Leftrightarrow \det u \neq 0 \Leftrightarrow \det A \neq 0$

  et alors $A^{-1} = Mat(u^{-1},\mathscr{E})$ d'où $\det(A^{-1}) = \det(u^{-1}) = \frac{1}{\det u} = \frac{1}{\det A}$
- $A = PBP^{-1}$ avec $P \in GL_n(\mathbb{K}) \Rightarrow \det A = \det P \times \det B \times \det(P^{-1}) = \det B$

(où A, B représentent un même endomorphisme u dans deux bases différentes, donc ont pour déterminant $\det u$)

- $$\begin{aligned} \det({}^tA) &= \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{j=1}^{n} [{}^tA]_{\sigma(i),i} \\ &= \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{j=1}^{n} a_{i,\sigma(i)} \\ &= \sum_{\sigma'\in S_n} \epsilon(\sigma'^{-1})\prod_{i=1}^{n} a_{i,\sigma'^{-1}(i)} \text{ car } \forall\sigma\in S_n, \exists!\sigma'\in S_n \,|\, \sigma = \sigma'^{-1} \\ &= \sum_{\sigma'\in S_n} \epsilon(\sigma')\prod_{j=1}^{n} a_{\sigma'(j),j} \text{ car } \sigma'^{-1}([\![1,n]\!]) = [\![1,n]\!] \\ &= \det A \end{aligned}$$

Pour aller plus loin - Le groupe $SL_n(\mathbb{K})$
$GL_n(\mathbb{K})$, groupe des matrices inversibles admet comme sous-groupe, le groupe spécial linéaire.
Il s'agit de l'ensemble des matrices de déterminant égal à 1.

$$SL_n(\mathbb{K}) = \{M \in \mathscr{M}_n(\mathbb{K}) \mid \det(M) = 1\}$$

On rappelle qu'une matrice de transvection est de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ (avec $i \neq j$).
On montre alors que

- *$\forall\, i \neq j$, $\lambda \in \mathbb{K}$, $T_{i,j}(\lambda) \in SL_n(\mathbb{K})$.*
- *Mieux : $\{T_{i,j}(\lambda)\}$ engendre le groupe $SL_n(\mathbb{K})$ (on exploite au mieux l'algorithme du pivot de Gauss)*
- *Toute matrice M est de la forme $M = (I_n + (\det M - 1)E_{n,n}) \times S$, avec $S \in SL_n(\mathbb{K})$*

□

Corollaire - Déterminant en lignes
Si $L_1,\dots,L_n$ désignent les lignes de A, alors $\det A$ est le déterminant des vecteurs lignes de A i.e. $\det A = \det({}^tL_1,\dots,{}^tL_n)$.

Démonstration
${}^tL_i$ est la i-ième colonne de ${}^tA$ et on a $\det A = \det({}^tA)$. □

3.4. Conséquences pratiques pour le calcul des déterminants

Savoir faire - Liste des bonnes habitudes

1. On ne change pas le déterminant d'une matrice en ajoutant à l'un des vecteurs colonnes (resp. lignes) une combinaison linéaire des autres vecteurs colonnes (resp.lignes).
2. Le déterminant d'une matrice dépend linéairement de chacun des vecteurs colonnes (resp. lignes).
3. Si on effectue une permutation σ sur les vecteurs colonnes (resp. lignes) le déterminant est multipliés par $\epsilon(\sigma)$ (par -1 dans le cas d'un échange de deux colonnes ou deux lignes)
4. Le déterminant d'une matrice diagonale est le produit des éléments diagonaux.

Exemple - Opération sur les colonnes

$$\begin{vmatrix} 1 & 2 & 1 & 4 \\ 1 & 1 & 2 & 4 \\ 1 & 2 & 3 & 6 \\ 1 & 1 & 4 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 3 & 0 \\ 1 & 1 & 4 & -5 \end{vmatrix} \text{ car } \det(C_1,C_2,C_3,C_4) = \det(C_1,C_2,C_3,C_4 - C_1 - C_2 - C_3).$$

Exemple - Dépendance linéaire

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 2 & 6 & 2 & 1 \\ 2 & 3 & 1 & 0 \\ 2 & 6 & 1 & 0 \end{vmatrix} = 2\times 3 \times \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 1 & 0 \end{vmatrix} + 2\times 3 \times \begin{vmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 1 & 0 \end{vmatrix} \text{ car}$$

$$\det(C_1,C_2,C_3,C_4' + C_4'') = 2\times 3 \times \det(\tfrac{C_1}{2},\tfrac{C_2}{3},C_3,C_4') + 2\times 3 \times \det(\tfrac{C_1}{2},\tfrac{C_2}{3},C_3,C_4'').$$

On démontre le résultat concernant les matrices diagonales :

Démonstration
Par la définition on a

$$\det A = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n} a_{\sigma(i),i}$$

or comme A est diagonale,

$$\forall i, a_{\sigma(i),i} \neq 0 \Leftrightarrow \forall i, \sigma(i) = i \Leftrightarrow \sigma = Id.$$

□

Exercice

Avec les règles précédentes, montrer que $\begin{vmatrix} a-b-c & 2a & 2a \\ 2b & b-c-a & 2b \\ 2c & 2c & c-a-b \end{vmatrix} = (a+b+c)^3$.

Correction
En faisant $L_3 \leftarrow L_1 + L_2 + L_3$, le déterminant est inchangé :

$$\Delta = \begin{vmatrix} a-b-c & 2a & 2a \\ 2b & b-c-a & 2b \\ 2c & 2c & c-a-b \end{vmatrix} = \begin{vmatrix} a-b-c & 2a & 2a \\ 2b & b-c-a & 2b \\ a+b+c & a+b+c & a+b+c \end{vmatrix} = (a+b+c)\begin{vmatrix} a-b-c & 2a & 2a \\ 2b & b-c-a & 2b \\ 1 & 1 & 1 \end{vmatrix}$$

Puis en faisant $L_1 \leftarrow L_1 - 2aL_3$, $L_2 \leftarrow L_2 - 2bL_3$, le déterminant est inchangé :

$$\Delta = (a+b+c)\begin{vmatrix} -a-b-c & 0 & 0 \\ 0 & -b-c-a & 0 \\ 1 & 1 & 1 \end{vmatrix} = (a+b+c)^3$$

puisqu'il s'agit d'une matrice triangulaire inférieure, son déterminant vaut le produit des éléments de la diagonale.

4. Calculs et applications des déterminants

4.1. Formule de Cramer pour inverser un système

Proposition - Formule de Cramer
Considérons le système $AX = b$ avec $A \in GL_n(\mathbb{K})$ et $b, X \in \mathcal{M}_{n,1}(\mathbb{K})$.
Alors pour tout $i \in \mathbb{N}_n$, $[X]_i = \dfrac{\det(C_1(A)\cdots C_{i-1}(A), b, C_{i+1}(A)\cdots C_n(A))}{\det A}$

Démonstration
Considérons la matrice écrite en bloc (colonne)

$$B = \left(C_1(A)\cdots C_{i-1}(A), b, C_{i+1}(A)\cdots C_n(A)\right)$$

Or $b = AX = \sum_{i=1}^{n} x_i C_i(A)$ si $[X]_i = x_i$.
On a donc, par linéarité par rapport à la colonne i :

$$\det B = \sum_{k=1}^{n} x_k \det\left(C_1(A)\cdots C_{i-1}(A), C_k(A), C_{i+1}(A)\cdots C_n(A)\right) = 0\cdots + 0 + x_i \det A + 0 + \cdots$$

On trouve des déterminants nuls : il y a deux fois les mêmes colonnes.
Et donc $[X]_i = x_i = \dfrac{\det B}{\det A}$ □

Histoire - Redécouverte



C'est le mathématicien suisse Gabriel Cramer (1704-1752) qui remit au goût du jour la notion de déterminant. Les découvertes de Leibniz ayant été (dans un premier temps) oubliées. Ainsi les formules de Cramer (voir plus bas) sont en fait des formules de Leibniz. On doit également à Cramer la définition de la signature d'une permutation.

4.2. Déterminant de matrices par blocs

Proposition - Matrices triangulaires par blocs
Soit $M \in \mathcal{M}_n(\mathbb{K})$. On suppose que M peut s'écrire par blocs $M = \begin{pmatrix} A & C \\ O & B \end{pmatrix}$ où A et B sont des matrices carrées. Alors on a

$$\det M = \det A \det B.$$

Démonstration
On suppose que $A \in \mathcal{M}_r(\mathbb{K})$On note $\Phi : (c_1, \dots c_r) \mapsto \det\begin{pmatrix} c_1 \cdots c_r & C \\ 0 & B \end{pmatrix}$.
Alors Φ est r-linéaire alternée, donc proportionnelle au déterminant : $\Phi = K \times \det$
Notons que $\Phi(c_1(I_r), \cdots c_r(I_r)) = K\det(I_r) = K$ et :

$$\Phi(c_1(I_r), \cdots c_r(I_r)) = \sum_{\sigma\in\Sigma_n} \epsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i),i} = \sum_{\sigma=(1,\dots,1,\sigma')\mid \sigma'\in\Sigma_{r-n}} \epsilon(\sigma') \prod_{i=1}^{r} 1 \prod_{i=r+1}^{n} m_{\sigma'(i-r)+r,i-r} = \det B$$

Puis $K \times \det(A)\Phi(c_1(A), \cdots, c_r(A)) = \det\begin{pmatrix} A & C \\ O & B \end{pmatrix} = \det M$.
□

Remarque - Transposé
En transposant le résultat précédent, on a donc également : $\det\begin{pmatrix} A & O \\ D & B \end{pmatrix} = \det A \det B$.

4.3. Développement suivant une ligne ou une colonne

En appliquant alors par récurrence le résultat précédent, on obtient la

Proposition - Déterminant d'une matrice triangulaire
Le déterminant d'une matrice diagonale ou triangulaire est le produit des éléments diagonaux.

Démonstration
Supposons par exemple que T soit triangulaire inférieure (sinon, on considère la matrice transposée).
Notons, pour $k \in \{0, n\}$, $\delta_k = a_{n,n}a_{n-1,n_1}\dots a_{k+1,k+1}\det(T_k)$,
où T_k est obtenue en enlevant les $n-k$ dernières lignes et $n-k$ dernières colonnes à T.
Comme T_k présente une dernière colonne de 0 sauf en ligne k, où se trouve $a_{k,k}$, on peut appliquer le lemme :

$$\det(T_k) = a_{k,k}\det(T_{k+1}) \Rightarrow \delta_k = \delta_{k+1}$$

Donc par invariance :

$$\det(T) = \det(T_0) = \delta_0 = \delta_n = \prod_{k=1}^{n} a_{k,k}$$

□

Définition - Mineur et cofacteur
On appelle mineur d'indice (i, j) de A le déterminant de la sous-matrice de A obtenue en supprimant la i-ième ligne et la j-ième colonne de A.
On appelle cofacteur d'indice (i, j) le produit du mineur d'indice (i, j) par $(-1)^{i+j}$.

Théorème - Calcul du déterminant par développement
Soit $1 \leqslant k \leqslant n$. Alors, $A_{i,j}$ désignant le cofacteur d'indice (i, j) dans la matrice $A \in \mathcal{M}_n(\mathbb{K})$, on a :

$$\det A = \sum_{i=1}^{n} a_{ik}A_{i,k} \quad \text{développement suivant la k-ième colonne}$$

$$\det A = \sum_{j=1}^{n} a_{kj}A_{k,j} \quad \text{développement suivant la k-ième ligne}$$

Démonstration
Soit $A = (a_{ij})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant n}} \in \mathcal{M}_n(\mathbb{K})$. On note $C_1, \dots, C_n$ ses vecteurs colonnes et $\mathcal{E} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$.

Pour $k \in [\![1,n]\!]$ on a donc $C_k = \sum_{i=1}^{n} a_{ik} e_i$ et

$$\begin{aligned}\det A &= \det_{\mathcal{E}}(C_1,\dots,C_{k-1},C_k,C_{k+1},\dots,C_n)\\ &= \sum_{i=1}^{n} a_{ik}\det_{\mathcal{E}}(C_1,\dots,C_{k-1},e_i,C_{k+1},\dots,C_n)\end{aligned}$$

on pose $A_{ik} = \det_{\mathcal{E}}(C_1,\dots,C_{k-1},e_i,C_{k+1},\dots,C_n)$

$$= \begin{vmatrix} a_{11} & \dots & a_{1,k-1} & 0 & a_{1,k+1} & \dots & a_{1,n}\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ \vdots & & \vdots & 0 & \vdots & & \vdots\\ a_{i1} & \dots & a_{i,k-1} & 1 & a_{i,k+1} & \dots & a_{i,n}\\ \vdots & & \vdots & 0 & \vdots & & \vdots\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ a_{n1} & \dots & a_{n,k-1} & 0 & a_{n,k+1} & \dots & a_{n,n}\end{vmatrix}$$

$$= (-1)^{k+i}\begin{vmatrix} 1 & a_{i1} & \dots & a_{i,k-1} & a_{i,k+1} & \dots & a_{i,n}\\ 0 & a_{11} & \dots & a_{1,k-1} & a_{1,k+1} & \dots & a_{1,n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & a_{i-1,1} & \dots & a_{i-1,k-1} & a_{i-1,k+1} & \dots & a_{i-1,n}\\ 0 & a_{i+1,1} & \dots & a_{i+1,k-1} & a_{i+1,k+1} & \dots & a_{i+1,n}\\ \vdots & \vdots & & \vdots & \vdots & & \vdots\\ 0 & a_{n1} & \dots & a_{n,k-1} & a_{n,k+1} & \dots & a_{n,n}\end{vmatrix}$$

$$= (-1)^{k+i}\begin{vmatrix} a_{11} & \dots & a_{1,k-1} & a_{1,k+1} & \dots & a_{1,n}\\ \vdots & & \vdots & \vdots & & \vdots\\ a_{i-1,1} & \dots & a_{i-1,k-1} & a_{i-1,k+1} & \dots & a_{i-1,n}\\ a_{i+1,1} & \dots & a_{i+1,k-1} & a_{i+1,k+1} & \dots & a_{i+1,n}\\ \vdots & & \vdots & \vdots & & \vdots\\ a_{n1} & \dots & a_{n,k-1} & a_{n,k+1} & \dots & a_{n,n}\end{vmatrix}$$ d'après le lemme

Ici on a appliqué le cycle $(12\dots k)$ sur les colonnes, c'est une permutation de signature $(-1)^{k-1}$, de même le cycle $(12\dots i)$ sur les lignes, c'est permutation de signatures $(-1)^{i-1}$ □

Exercice

Calculer $\begin{vmatrix} 1 & 1 & -1 & 2\\ 3 & 0 & 1 & 2\\ 2 & 2 & 1 & 1\\ 1 & 1 & 3 & 1\end{vmatrix}$.

Correction

On développe par rapport à la seconde colonne (avec un 0) :

$$\begin{vmatrix} 1 & 1 & -1 & 2\\ 3 & 0 & 1 & 2\\ 2 & 2 & 1 & 1\\ 1 & 1 & 3 & 1\end{vmatrix} = (-1)1\begin{vmatrix} 3 & 1 & 2\\ 2 & 1 & 1\\ 1 & 3 & 1\end{vmatrix} + 0 - 2\begin{vmatrix} 1 & -1 & 2\\ 3 & 1 & 2\\ 1 & 3 & 1\end{vmatrix} + 1\begin{vmatrix} 1 & -1 & 2\\ 3 & 1 & 2\\ 2 & 1 & 1\end{vmatrix}$$

$$= -(3+1+12-2-9-2) - 2(1-2+18-6+3-2) + (1-4+6-2+3-4) = -3-24 = -27$$

Exercice

Soit $D_n = \begin{vmatrix} 1 & 1 & 0 & 0 & \dots & 0\\ 1 & 1 & 1 & 0 & \dots & 0\\ 0 & 1 & 1 & 1 & \dots & 0\\ \vdots & \vdots & \ddots & \ddots & \ddots & \\ \vdots & \vdots & \vdots & \ddots & \ddots & 1\\ 0 & 0 & \dots & 0 & 1 & 1\end{vmatrix}$ (déterminant d'ordre n avec des 1 sur la diagonale, juste au-dessus et juste en-dessous, des 0 autre part).

Déterminer une relation de récurrence entre D_n, D_{n-1} et D_{n-2}, en déduire D_n.

Correction

Si on fait un développement par rapport à la première ligne, on obtient :

$$D_n = 1D_{n-1} - 1\begin{vmatrix} 1 & 1 & 0 & 0 & \dots & 0\\ 0 & 1 & 1 & 0 & \dots & 0\\ 0 & 1 & 1 & 1 & \dots & 0\\ \vdots & \vdots & \ddots & \ddots & \ddots & \\ \vdots & \vdots & \vdots & \ddots & \ddots & 1\\ 0 & 0 & \dots & 0 & 1 & 1\end{vmatrix}$$

Et un développement par rapport à la première colonne (Il est important d'écrire une grande matrice) :

$$D_n = D_{n-1} - D_{n-2}$$

On reconnait une suite récurrente linéaire d'ordre 2, d'équation caractéristique : $x^2 - x + 1 = 0$.
Les racines sont $r_1 = \frac{1+i\sqrt{3}}{2} = e^{i\pi/3}$ et $r_2 = \overline{r_1} = \frac{1-i\sqrt{3}}{2} = e^{-i\pi/3}$.
Donc $\exists A, B$ tel que $\forall n \in \mathbb{N}$, $D_n = A\cos\frac{n\pi}{3} + B\sin\frac{n\pi}{3}$.
Puis $D_1 = 1$ et $D_2 = 0$, donc $\frac{1}{2}A + \frac{\sqrt{3}}{2}B = 1$ et $\frac{1}{2}A - \frac{\sqrt{3}}{2}B = 0$.
Donc en additionnant $A = 1$ et en soustrayant $B = \frac{1}{\sqrt{3}}$, donc $D_n = \cos\frac{n\pi}{3} + \frac{1}{\sqrt{3}}\sin\frac{n\pi}{3}$

4.4. Calcul de l'inverse

Soit $A = (a_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}} \in \mathcal{M}_n(\mathbb{K})$

Proposition - Relation linéaire

$$\forall j,k \in [\![1,n]\!],\ \sum_{i=1}^{n} a_{ij}A_{ik} = \delta_{j,k}\det A$$

$$\forall i,k \in [\![1,n]\!],\ \sum_{j=1}^{n} a_{ij}A_{kj} = \delta_{i,k}\det A$$

Démonstration
On a vu avec le développement du déterminant que pour tout $k \in \mathbb{N}_n$,

$$\det A = \sum_{i=1}^{n} a_{i,k}A_{i,k} = \sum_{j=1}^{n} a_{k,j}A_{k,j} =$$

Ce qui donne les formules précédentes dans les cas $j = k$ et $i = k$ respectivement.

Puis dans le cas $j \neq k$, alors $\sum_{i=1}^{n} a_{i,j}A_{i,k} = \det A'_{j,k}$ où $A'_{j,k}$ est obtenue à partir de la matrice A mais avec en k^e colonne, la j^e colonne initiale de A.
Donc $A'_{j,k}$ possède deux colonnes identiques et donc $\det(A'_{j,k}) = 0$.
De même pour la seconde formule sur les lignes. □

Pour aller plus loin - Inverser un système. Formule de Cramer (autre démonstration)
Supposons que l'on doit résoudre le système d'inconnue X : $AX = B$.
Il s'agit donc de calculer

$$X = A^{-1}B = \frac{1}{\det(A)}\ {}^t\mathrm{Com}A \times B$$

On a donc

$$x_i = \frac{1}{\det(A)}\sum_{j=1}^{n} Coef_{i,j}({}^t\mathrm{Com}(A))B_j$$

$$= \frac{1}{\det(A)}\sum_{j=1}^{n} A_{j,i}B_j$$

Or ce dernier calcul est le développement par rapport à la colonne i de la matrice A_i^B, obtenu à partir de la matrice A pour laquelle la i^e colonne a été remplacée par la colonne B

Définition - Comatrice
La matrice $(A_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}}$ est appelée la comatrice de A et notée $\mathrm{Com}A$.

Théorème - Expression de A^{-1} avec la compatrice
$\forall A \in \mathcal{M}_n(\mathbb{K})$, $A \times {}^t\mathrm{Com}A = {}^t\mathrm{Com}A \times A = (\det A)I_n$.
Donc, si $\det A \neq 0$ alors A est inversible et $A^{-1} = \frac{1}{\det A}\ {}^t\mathrm{Com}A$.

Démonstration
Le coefficient en ligne i et colonne j de $A \times {}^t\mathrm{Com}(A)$ est

$$\mathrm{Coef}_{i,j}(A \times {}^t\mathrm{Com}(A)) = \sum_{k=1}^{n}\mathrm{Coef}_{i,k}(A)\mathrm{Coef}_{k,j}({}^t\mathrm{Com}(A)) = \sum_{k=1}^{n} a_{i,k}A_{j,k} = \delta_{i,j}\det A = \mathrm{Coef}_{i,j}(\det A I_n)$$

d'après la seconde formule. On donc $A \times {}^t\mathrm{Com}(A) = \det(A)I_n$.
De même avec la première formule, on a ${}^t\mathrm{Com}A \times A = (\det A)I_n$. □

Exercice

Soit $A=\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ telle que $\det(A)\neq 0$. Déterminer A^{-1}.

Correction

On a, d'après la règle de Sarrus, $\delta = aei+bfg+cdh-afh-bdi-ceg$, puis

$$A^{-1}=\frac{1}{\delta}\begin{pmatrix} ei-hg & -bi+hc & bf-ce \\ -di+gf & ai-gc & -af+dc \\ dh-ge & -ah-bg & ae-db \end{pmatrix}$$

Savoir faire - Utilisation de A^{-1} avec la comatrice

Mis à part pour $n=2$, on n'utilise **pas** cette formule pour calculer A^{-1} car les calculs sont trop longs. Quelle est leur complexité?
$n!\times n$ pour δ et $(n-1)!\times(n-1)$ pour chacun des n^2 coefficients.
Donc au total : $n!n+n^2(n-1)(n-1)!=nn!(1+(n-1))=n^2n!\ldots$

4.5. Déterminant comme fonction polynomiale

Savoir faire - Si il y a x comme coefficient(s) de A

$\det A=\sum_{\sigma\in\mathfrak{S}_n}\epsilon(\sigma)\prod_{i=1}^{n}\mathrm{Coef}_{i,\sigma(i)}(A)$.
Si x^k se glisse parmi les coefficients de A_x, alors $\det A_x$ est nécessairement une fonction polynomiale en x.
On peut alors :

1. chercher son degré (d), en organisant bien notre réflexion
2. trouver des valeurs particulières pour des valeurs de x particulières et en nombre suffisant $(\geqslant d)$ pour en déduire une expression directe et explicite du déterminant.

Pour aller plus loin - Polynôme caractéristique d'une matrice

Considère le nombre $\chi(x)=\det(xI_n-A)$.
Alors comme xI_n-A est une matrice avec quelques x comme coefficients, son déterminant est une formule polynomiale en x.
On note χ_A ce polynôme. On montre qu'il est unitaire, de degré n. Il porte quasiment toutes les informations concernant A (mais pas les invariants de similitude...)

On va utiliser cette analyse pour démontrer la proposition suivante (déterminant de Vandermonde)

Proposition - Déterminant de Vandermonde

On note $A(x_1,x_2,..,x_n)$ la matrice qui suit :

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \ldots & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1} \end{pmatrix}$$

et $V(x_1,x_2,..,x_n)$ le déterminant cette matrice. Alors

$$V(x_1,x_2,..,x_n)=\prod_{(i,j)|1\leqslant i<j\leqslant n}(x_j-x_i)$$

Démonstration

Notons, pour $x\in\mathbb{K}$, $P(x)=V(x_1,x_2,\ldots,x_{n-1},x)$.
Alors par développement de V, P apparait comme un polynôme en x de degré $n-1$.
On le voit par exemple en développant par rapport à la dernière colonne.
Puis pour tout $i\in[\![1,n-1]\!]$, $P(x_i)=0$ car la matrice possède alors deux colonnes identiques : la i^e et la dernière.
Donc il existe A tel que $P=A\times\prod_{i=1}^{n-1}(x-x_i)$.
Enfin, ce A est le coefficient que l'on trouve devant x^{n-1} lorsqu'on développe le polynôme, donc

$A=V(x_1,x_2,\ldots x_{n-1})$.
On achève la démonstration par la mise en place d'un invariant (ou par récurrence).
Notons $R(x_1,\ldots x_n)=\frac{V(x_1,\ldots x_n)}{\prod_{j=2}^{n}(\prod_{i=1}^{j-1}(x_j-x_i)}$. Alors on vient de voir :

$$R(x_1,\ldots x_n)=\frac{V(x_1,x_2,\ldots x_{n-1})\prod_{i=1}^{n-1}(x_n-x_i)}{\prod_{j=2}^{n}(\prod_{i=1}^{j-1}(x_j-x_i)}=\frac{V(x_1,\ldots x_{n-1})}{\prod_{j=2}^{n-1}(\prod_{i=1}^{j-1}(x_j-x_i)}=R(x_1,\ldots x_{n-1})=R(x_1)=1$$

□

Histoire - Vandermonde

Alexandre-Théophile Vandermonde est né le 28 février 1735 à Paris et est mort le 1er janvier 1796 à Paris. Il est un mathématicien et chimiste français

Corollaire - Inversibilité de la matrice Vandermonde

$A(x_1,x_2,..,x_n)$ est inversible si et seulement si les x_i sont deux à deux distincts.

Exercice

Soit $n\in\mathbb{N}$. Soit $(\lambda_1,\lambda_2,\ldots\lambda_n)\in\mathbb{C}^n$.
On note $e_k:x\mapsto e^{\lambda_k x}$.
Montrer que la famille $(e_1,e_2,\ldots e_k)$ est libre si et seulement si $\forall\, i\neq j\leqslant n,\ \lambda_i\neq\lambda_j$

Correction

Soient $\mu_1,\mu_2,\ldots\mu_n\in\mathbb{C}$ tels que $f:=\sum_{k=1}^{n}\mu_k e_k=0$.

Alors f est dérivable $n-1$ fois et donc pour tout $h\in\mathbb{N}_{n-1}$, $f^{(h)}=\sum_{k=1}^{n}\mu_k\lambda_k^h e_k=0$.

En $x=0$, on a alors le système d'inconnue $\mu_1,\ldots\mu_n$: $(\mathscr{S}):\mu_k\lambda_k^h=0$.
Le déterminant de ce système homogène est un déterminant de Vandermonde...

5. Bilan

Synthèse

- ⇝ L'ensemble des fonctions n-linéaires, alternées de E^n ($\mathbb{K}$ ev) et à valeurs dans le corps $\mathbb{K}$ est un espace vectoriel.
  Il est de dimension 1. Toutes ces fonctions sont donc colinéaires, ou proportionnelles à une expression référante (base) : l'application déterminant.
- ⇝ Cette application de base s'appelle le déterminant de la famille des n vecteurs.
  Par extension, on peut aussi définir le déterminant d'une matrice (n vecteurs-colonnes de taille n) ou bien d'un endomorphisme $u\in\mathscr{L}(E)$ (par indépendance de cette valeur, selon la base considérée).
- ⇝ On a alors toute une famille de résultats dont deux résultats essentiels : $\det(u\circ v)=\det u\times\det v$ (ou équivalent pour les matrices) et $\det\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}=\det A\det C$. Les autres résultats sont plus évident ($\det A=\det A^T\ldots$).
- ⇝ Une méthode est souvent exploitée : le développement par rapport à une ligne ou une colonne. Ceci au niveau théorique (on en déduit par exemple : $A^{-1}=\frac{1}{\det A}(\mathrm{com}(A))^T$) ou au niveau pratique (Formules de Cramer, relation de récurrence...).
  On notera également que le déterminant peut être vu comme un polynôme supersymétrique de ces coefficients...

Savoir-faire et Truc & Astuce du chapitre

- Truc & Astuce pour le calcul - Cas $n = 2$ ou $n = 3$
- Savoir-faire - Liste des bonnes habitudes
- Savoir-faire - Utilisation de A^{-1} avec la comatrice
- Savoir-faire - Si il y a x comme coefficient(s) de A

Notations

Définitions	*Propriétés*	*Remarques*
Déterminant de $(X_1,\dots X_n)$ par rapport à la base E	$\det_E(X_1,\dots X_n) = \sum_{\sigma\in\Sigma_n} \epsilon(\sigma)\prod_{i=1}^{n}[X]_{i,\sigma(i)}$	où $\forall\ j\in\mathbb{N}_n$, $X_j = \sum_{i=1}^{n}[X]_{i,j}E_i$.
Déterminant de $A(\in\mathcal{M}_n(\mathbb{K}))$	$\det A = \sum_{\sigma\in\Sigma_n} \epsilon(\sigma)\prod_{i=1}^{n}[A]_{i}^{\sigma(i)}$	.
Cofacteur d'ordre (i,j) de A	$A_{i,j} = (-1)^{i+j}\det(A^{i\wedge j})$	où $A^{i\wedge j}$ est la matrice obtenue à partir de A privée de la ligne i et colonne j.
Comatrice de A : $\forall\ i,j\in\mathbb{N}_n$, ${}^{i}[\mathrm{com}A]_j = A_{i,j}$ (cofacteur)	$A\times(\mathrm{com}A)^T = I_n$.	
Déterminant de la matrice de VANDERMONDE $\begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{pmatrix}$	$V(x_1,\dots x_n) = \prod_{i<j}(x_j - x_i)$	

Retour sur les problèmes

142. C'est la formule du développement par rapport à une ligne ou une colonne. Elle donne la formule $\det_n(A) = \sum_i {}^{1}[A]_i \times \det_{n-1}(A^{1\wedge i})$.

    Elle se comprend très bien pour des matrices triangulaires supérieures.

143. Cours

144. On voit qu'il y a un agrandissement global de A vers A' d'un facteur 10.
    La formule du déterminant précise que celui-ci peut être concentré sur une seule colonne (ou ligne) : $C_i(A') = 10C_i(A)$ et $\forall\ j\neq i$, $C_j(A') = C_j(A)$ ou bien dilué sur toutes les colonnes (ou lignes) : $C_k({}^{a}r) = \sqrt[n]{10}\times C_k(A)$.

145. Cours : nécessairement $\det(AB) = \det A\det B$.

146. Cours : c'est la formule de Cramer ou bien l'inverse d'une matrice

Septième partie

Polynômes et fractions rationnelles

Chapitre 31

Structure algébrique de l'ensemble des polynômes

Résumé -

Ce chapitre est le premier d'un série de quatre chapitres autour des polynômes. Chacun de ces chapitres apporte un point de vue (très) différent sur le même objet. L'enjeu est de pouvoir passer d'une façon de voir à une autre; de ne pas s'enfermer dans un unique point de vue.

Dans ce chapitre, on motive l'intérêt de l'étude des polynômes : le calcul polynomiale (quitte à considérer plusieurs indéterminées) correspond peu ou prou au calcul dans tout anneau. C'est le lieu naturel du développement (distribution) dans une structure à deux lois. On verra aussi qu'il s'agit d'un espace vectoriel dans une famille génératrice est $(1, X, X^2, \dots)$ *(nous en reparlerons au chapitre sur les espaces vectoriels).*

On se concentre donc ici aux opérations formelles à partir de polynôme : somme et produit, puis composition et enfin dérivation…

Sommaire

1. Problèmes 628
2. L'algèbre $\mathbb{K}[X]$ 629
2.1. Construction 629
2.2. $\mathbb{K}[X]$ comme $\mathbb{K}$ espace-vectoriel 629
2.3. $\mathbb{K}[X]$ comme anneau 630
2.4. Composée 631
2.5. Remarques sur le corps $\mathbb{K}$ 632
3. Degré 633
3.1. Définition 633
3.2. Arithmétique des degrés 633
3.3. Intégrité de $\mathbb{K}[X]$ et éléments inversibles 634
3.4. Valuation 635
4. Dérivation d'un polynôme 635
4.1. Définition 635
4.2. Dérivation d'opérations polynomiales 636
4.3. Dérivation d'ordre supérieur 637
4.4. Applications 637
5. Bilan 639

$\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$. (On pourrait généraliser les définitions à un autre corps.)

1. Problèmes

Problème 131 - Polynômes et calculs algébriques

Etant donné un anneau A, il est possible de calculer $(a-b)\times(c-d)$. Et le résultat de ce calcul : $ac+bd-ad-bc$ est en fait *indépendant* de l'anneau considéré.
D'une certaine façon, le résultat ne dépend que du calcul lui-même.
Existe-t-il un ensemble des opérations algébriques et des résultats qui en découle? Par exemple, que peut-on dire de $(1+a+a^2+a^3)(1-a)$. Est-ce que le résultat dépend si $a\in\mathbb{Z}$, ou $a\in\mathbb{R}$, $\mathbb{C}$ ou encore $a\in\frac{\mathbb{Z}}{p\mathbb{Z}}$ ou bien a une matrice, une fonction (endomorphisme), un graphe, un arbre?

Problème 132 - Lois sur les polynômes

Si l'on considère deux polynômes $A=\sum_{k=0}^{n} a_k X^k$ et $B=\sum_{k=0}^{r} b_k X^k$, quelles sont les opérations naturelles que l'on peut faire avec ces polynômes $(+,\times,/,\circ\dots)$? Est-ce que l'ensemble des polynômes est stable pour ces lois?
Et la dérivation?

Problème 133 - Expression algébrique

En prolongeant le problème précédent, si $A=\sum_{k=0}^{n} a_k X^k$ et $B=\sum_{k=0}^{r} b_k X^k$, quelle est l'expression du coefficient devant X^h pour les polynômes $A+B$, $A\times B$ et $A\circ B$?
Est-ce une expression simple que l'on a intérêt à retenir (par exemple pour calculer des DL)? Quelle notation mérite alors d'être instaurée?

Problème 134 - Degré infini. Séries formelles

Pour éviter tout problème, les polynômes sont définis avec des degrés (valeur maximale à partir de laquelle tout est nulle).
Les lois algébriques que nous verrons peuvent-ils se noter avec de degré infini? Peut-on créer une algèbre de polynôme de degrés non nécessairement finis (séries formelles)?

Problème 135 - Dérivation algébrique ?

La formule de Taylor permet, étant donnée une fonction f d'obtenir un DL au voisinage de a, sous forme polynomiale :

$$f(x)=\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(x-a)^k+o\big((x-a)^n\big)$$

Pour $a=0$, cela donne en particulier une expression du coefficient devant x^k. Mais il s'agit de dérivée la fonction f. Cette opération de dérivation s'obtient par un passage à la limite, totalement dépendant de l'ana-

lyse. Dans ce chapitre, nous aimerions exploiter ce genre de relation pour obtenir explicitement $[P]_k$. Il faut alors définir algébriquement une opération sur les polynômes qui coïncide avec la dérivation en analyse.
Comment définir $\Delta : P \mapsto P'$ et quelles sont ses propriétés ?

2. L'algèbre $\mathbb{K}[X]$

2.1. Construction

Heuristique - Problème opératoire. Mise en place de la structure

On considère l'ensemble E des suites d'éléments de $\mathbb{K}$ nulles à partir d'un certain rang. Ce sont les suites presque nulles, vues dans le chapitre sur les espaces vectoriels

— $(E,+)$, où $+$ désigne l'addition usuelle des suites, est un sous-groupe du groupe commutatif $(\mathbb{K}^{\mathbb{N}},+)$ car $(0)_{n\in\mathbb{N}} \in E$ et la différence de deux suites nulles à partir d'un certain rang est une suite nulle à partir d'un certain rang.
— $(E,+,.)$ est alors un s.e.v. de $\mathbb{K}^{\mathbb{N}}$, de vecteur nul la suite nulle.
— On définit également le produit de Cauchy de deux éléments $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$ de E par :

$$(a_n)_{n\in\mathbb{N}} \times (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}} \text{ où } \forall n\in\mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{\substack{(p,q)\in\mathbb{N}^2\\ p+q=n}} a_p b_q$$

$\times$ est interne dans E car $\exists N_1 \mid k \geqslant N_1 \Rightarrow a_k = 0, \exists N_2 \mid k \geqslant N_2 \Rightarrow b_k = 0$,
d'où pour $n \geqslant N_1 + N_2 - 1, k \in [\![0,n]\!]$, on a $k \geqslant N_1$ ou $n-k \geqslant N_2$ donc $c_n = 0$.
— On vérifie alors que $(E,+,\times)$ est un anneau commutatif :
$\times$ est commutative ;
$\times$ est associative : en posant, pour $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$ éléments de E, $(d_n) = (a_n) \times (b_n)$ et $(f_n) = (d_n) \times (c_n)$ on a

$$f_n = \sum_{\substack{(p,q)\in\mathbb{N}^2\\ p+q=n}} d_p c_q = \sum_{\substack{(p,q)\in\mathbb{N}^2\\ p+q=n}} \Big(\sum_{\substack{(\ell,m)\in\mathbb{N}^2\\ \ell+m=p}} a_\ell b_m \Big) c_q$$
$$= \sum_{\substack{(\ell,m,q)\in\mathbb{N}^3\\ \ell+m+q=n}} a_\ell b_m c_q$$

Par commutativité et symétrie du résultat on obtient :

$$(a_n) \times \Big((b_n) \times (c_n)\Big) = \Big((b_n) \times (c_n)\Big) \times (a_n) = (f_n) = \Big((a_n) \times (b_n)\Big) \times (c_n)$$

L'élément neutre est la suite $\epsilon = (1,0,0,\dots)$ définie par $\epsilon_0 = 1$ et $\forall n \geqslant 1, \epsilon_n = 0$:
en effet pour $(a_n)_{n\in\mathbb{N}} \in E$, en posant $(c_n) = \epsilon \times (a_n)$ on $c_n = \sum_{k=0}^{n} \epsilon_k a_{n-k} = \epsilon_0 a_n = a_n$.
$\times$ est distributive par rapport à $+$
— De plus pour $\lambda \in \mathbb{K}$:

$$\lambda.\Big((a_n) \times (b_n)\Big) = \Big(\lambda.(a_n)\Big) \times (b_n) = (a_n) \times \Big(\lambda.(b_n)\Big)$$

On dit que $(E,+,\times,.)$ est une $\mathbb{K}$-algèbre commutative.

2.2. $\mathbb{K}[X]$ comme $\mathbb{K}$ espace-vectoriel

Définition - Notation de Kronecker

On utilise le symbole de Kronecker $\delta_{i,j} = \delta_i^j = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ si } i \neq j \end{cases}$

On a alors $\epsilon = (\delta_n^0)_{n\in\mathbb{N}}$.

Définition - Polynôme

On pose $X = (\delta_n^1)_{n\in\mathbb{N}}$, On vérifierait que $X^p = (\delta_n^p)_{n\in\mathbb{N}}$.

Pour aller plus loin - Ensemble $\mathbb{C}$

Cauchy définit l'ensemble des nombres complexes comme l'ensemble quotient $\mathbb{R}[X]/(X^2+1)$.
Cela signifie qu'un nombre complexe est un polynôme avec identification $X^2 = -1$.
Ainsi les nombres $(a+ib)\times(c+id)$ s'identifie aux calculs

$$(a+bX)\times(c+dX) = ac + X(ad+bc) + bdX^2$$

Mais comme $X^2 = -1$ on trouve $(ac-bd) + (ad+bc)X$, le polynôme identifié à $(ac-bd) + (ad+bc)i = (a+ib)\times(c+id)$.
En terme de calculs effectués, les calculs de $\mathbb{C}$ sont bien des calculs de $\mathbb{R}[X]$…

On écrira désormais $P = (a_0, a_1, \dots, a_n, 0, \dots)$ sous la forme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k$$

où $X^0 = \epsilon$ est identifié à 1.
On identifiera le scalaire $\lambda \in \mathbb{K}$ avec $\lambda\epsilon = (\lambda, 0, 0, \dots)$ (c'est-à-dire que l'on a une bijection évidente entre $\mathbb{K}$ et les suites nulles à partir du rang 1).
On trouve aussi l'écriture $\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{+\infty} a_k X^k$ où $a_k = 0$ pour $k > n$ (puisqu'il s'agit d'une suite nulle à partir d'un certain rang).
On pourra écrire $[P]_k$ pour désigner a_k, le nombre devant X^k dans P

Définition - Egalité de polynôme

On dit que les polynômes P et Q sont égaux si $\forall\ n \in \mathbb{N}$, $[P]_n = [Q]_n$

Pour aller plus loin - S.e.v des polynômes de degré $\leqslant n$

On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.
$\mathbb{K}_n[X]$ est un s.e.v. de $\mathbb{K}[X]$, de dimension finie égale à $n+1$.
$(1, X, X^2, \dots, X^n)$ en est une base, appelée base canonique de $\mathbb{K}_n[X]$.

On a les règles de calcul suivantes, qui donne à $\mathbb{K}[X]$, une structure d'espace vectoriel

Théorème - $\mathbb{K}[X]$, comme $\mathbb{K}$-espace vectoriel

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.
$(\mathbb{K}[X],+,.)$ est un $\mathbb{K}$-e.v. de vecteur nul le polynôme 0
Pour $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{m} b_k X^k$ on a

$$P + Q = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k \quad (a_k = 0 \text{ si } k > n,\ b_k = 0 \text{ si } k > m)$$

$$\lambda P = \sum_{k=0}^{n} \lambda a_k X^k$$

Remarque - Linéarité de $P \mapsto [P]_k$

On en déduit que pour tous $\lambda, \mu \in \mathbb{K}$ et $P, Q \in \mathbb{K}[X]$, et pour tout $k \in \mathbb{N}$,
$\big[\lambda P + \mu Q\big]_k = \lambda [P]_k + \mu [Q]_k$.

2.3. $\mathbb{K}[X]$ comme anneau

Théorème - Anneau $\mathbb{K}[X]$

On a noté $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.
$(\mathbb{K}[X],+,\times)$ est un anneau commutatif d'élément neutre pour $\times$ le polynôme $1 = X^0$.
Pour $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{m} b_k X^k$ on a

$$P + Q = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k \quad (a_k = 0 \text{ si } k > n,\ b_k = 0 \text{ si } k > m)$$

$$P \times Q = PQ = \sum_{k=0}^{n+m} c_k X^k \quad \text{avec } c_k = \sum_{\substack{(i,j)\in\mathbb{N}^2\\ i+j=k}} a_i b_j$$

Corollaire - Algèbre $\mathbb{K}[X]$
$(\mathbb{K}[X],+,\times,\cdot)$ est une $\mathbb{K}$-algèbre.

Attention - $\mathbb{K}_n[X]$ n'est pas une algèbre
Ne cherchez pas à réduire $\mathbb{K}[X]$ de manière à avoir une algèbre de dimension finie. $\mathbb{K}_n[X]$ n'est pas stable pour la multiplication (sauf si $n \leqslant 1$).

Savoir faire - Expression formelle
Si P et Q sont deux polynômes (de degré fini, évidemment), alors $P+Q$ et $P\times Q$ sont des polynômes et

$$\forall\, k\in\mathbb{N},\qquad [P+Q]_k=[P]_k+[Q]_k,\qquad [PQ]_k=\sum_{i=0}^{k}[P]_i[Q]_{k-i}=\sum_{i+j=k}[P]_i[Q]_j$$

Cela est indépendant de la valeur de $\deg P$, $\deg Q\ldots$

Pour aller plus loin - Algèbre?
Un $\mathbb{K}$ espace vectoriel $(A,+,\cdot)$ qui vérifie également : $(A,+,\times)$ est un anneau, s'appelle une $\mathbb{K}$-algèbre.
Par exemple $(\mathscr{L}(E),+,\circ,\cdot)$ est une $\mathbb{K}$-algèbre de dimension finie (en tant qu'espace vectoriel de dimension finie) si E est un $\mathbb{K}$ev de dimension finie.

Heuristique - Ce qui compte ce sont les relations algébriques
Beaucoup d'objets mathématiques font partis d'un anneau (avec addition et multiplication des éléments).
Il est alors parfois possible de faire une identification entre cette anneau et les relations associés et l'anneau des polynômes avec les mêmes relations.
On se rend compte que la connaissance sur l'anneau polynômes nous éclaire alors autrement. L'exemple suivant éclaire cette remarque. D'une certaine façon l'anneau des polynômes est l'anneau des relations

Exemple - Calculer A^{100} si $A=\begin{pmatrix}1&2\\1&0\end{pmatrix}$

On calcule les premières valeurs et on remarque que $A^2=\begin{pmatrix}3&2\\1&2\end{pmatrix}=A+2I_2$.

Les puissances de A s'écrivent alors que des polynômes en A : $A^k\in\mathbb{Z}[A]$.
Mais on a mieux : $X^{100}=(X^2-X-2)Q(X)+R(X)$ avec $\deg R<1$ (division euclidienne).
Puis en se plaçant sur l'anneau $\mathbb{R}$: $(-1)^{100}=((-1)^2-(-1)-2)\times Q(-1)+R(-1)=R(-1)$ et $2^{100}=0+R(2)$.
Donc $R=\frac{1}{3}(2^{100}(X+1)-(-1)^{100}(X-2))$ On a alors pour l'anneau $\mathbb{Z}[A]$: $A^{100}=Q(A)\times(A^2-A-2I_2)Q(A)+R(A)=R(A)=\frac{1}{3}\left((2^{100}-(-1)^{100})A+(2^{100}+2(-1)^{100}I_2)\right)$.
Un autre exemple :

Remarque - Formule du binôme
$\mathbb{K}[X]$ étant un anneau commutatif, la formule du binôme est valable pour calculer

$$(P+Q)^m=\sum_{i=0}^{m}\binom{m}{i}P^iQ^{m-i}$$

Remarque - $\mathbb{K}[X]$ anneau euclidien
Comme $\mathbb{Z}$, $\mathbb{K}[X]$ est muni d'une division euclidienne.
Beaucoup de propriétés de l'arithmétique de $\mathbb{Z}$ se transmettent à l'arithmétique de $\mathbb{K}[X]$.
C'est l'enjeu du chapitre 19

2.4. Composée

Définition - Composition polynomiale
Si $P=\sum_{k=0}^{n}a_kX^k$ et $Q\in\mathbb{K}[X]$ (non nul), on définit le polynôme composé

$P\circ Q$ ou $P(Q)$ par :

$$P\circ Q=P(Q)=\sum_{k=0}^{n}a_kQ^k$$

Exemple - Composition
Pour $P=1+X+X^2$ on a

$$P\circ(-X)=P(-X)=1-X+X^2$$

$$P\circ X^2=P(X^2)=1+X^2+X^4$$

Remarque - Notation
On retrouve aussi la notation $P(X)$ pour P.
Exercice
Exprimer le coefficient $[P\circ Q]_k$ en fonction des $[P]_i$ et $[Q]_j$.
On commencera par $k\leqslant 3\ldots$

Correction

Définition - Polynômes pair, impair
$P\in\mathbb{K}[X]$ est dit pair (resp. impair) si $P(-X)=P(X)$ (resp. $P(-X)=-P(X)$).

Exercice
Soit $P\in\mathbb{R}[X]$ un polynôme pair. Montrer qu'il existe $Q\in\mathbb{R}[X]$ tel que $P=Q(X^2)$.

Correction
Notons $P=\sum_{k=0}^{d}a_kX^k$.
On a donc $P(-X)=P(X)=\sum_{k=0}^{d}(-1)^ka_kX^k$, donc $\sum_{k=0}^{d}\left[(-1)^k-1\right]a_kX^k=0$.
Or le polynôme nul a une écriture unique et donc pour tout $k\leqslant d$, $\left[(-1)^k-1\right]a_k=0$.
Mais si k est impair, $(-1)^k-1=-2$ et donc $a_k=0$.
Finalement, $P=\sum_{h=0}^{d/2}a_{2h}X^{2h}$ (et d est nécessairement pair).
On considère alors $Q=\sum_{h=0}^{d/2}a_{2h}X^h\in\mathbb{K}[X]$, on a donc $P(X)=Q(X^2)$.
Notons que la réciproque est vraie, même cela ne nous intéresse pas ici.

2.5. Remarques sur le corps $\mathbb{K}$

Heuristique - $\mathbb{K}$: corps ou anneau?
Pour définir parfaitement $\mathbb{K}[X]$, il faut pouvoir additionner et multiplier les coefficients a_n entre eux.
Pour que ceci se passe bien, il faut fondamentalement que $\mathbb{K}$ soit (au moins) un anneau.
C'est la définition de l'anneau.
Il arrivera que l'on ait besoin, en outre, que chaque élément a_n soit inversible, par exemple pour faire des divisions euclidiennes de polynômes, ou écrire

$$3X\times P=X^3\Rightarrow P=\frac{1}{3}X^2$$

Donc nous avons souvent besoin d'un corps $\mathbb{K}$.

Pour aller plus loin - Anneau $\mathbb{K}[X,Y]$
Si restreindre à une seule indéterminée est important : c'est la base. Mais, souvent, il peut y avoir deux inconnues ou deux références (comme i dans l'exemple plus haut). On peut par exemple considérer les polynômes en $\sqrt{2},\sqrt{3}$ à coefficients dans $\mathbb{Z}$, on le noterait $\mathbb{Z}[\sqrt{2},\sqrt{3}]$.
Il faut donc nécessaire définir une structure adaptée : $\mathbb{K}[X,Y]$.
La méthode classique est de penser $\mathbb{K}[X,Y]=(\mathbb{K}[X])[Y]$. C'est-à-dire qu'il s'agit de polynôme en Y à coefficients dans les polynômes X. On montre que c'est équivalent à faire la construction dans l'autre sens.

Remarque - Quel corps $\mathbb{K}$?
La plupart du temps, on prendra pour corps $\mathbb{R}$ ou $\mathbb{C}$.
Il arrivera, de temps en temps de prendre $\mathbb{Q}$ (si l'on part de l'anneau $\mathbb{Z}$ des entiers), ou moins trivialement : $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (corps des inversibles modulo p).

Remarque - Quel anneau $\mathbb{K}$?
Enfin, pour certains problèmes (*exemple-type : étude des polynômes à coefficients entiers*), on se placera sur $\mathbb{Z}[X]$.
Pour d'autres problèmes (*exemple-type : lemme de factorisation des matrices), on se placera sur $\mathscr{M}_n(\mathbb{K})[X]\simeq\mathscr{M}_n(\mathbb{K}[X])$*).

Remarque - $(\mathbb{K}[X])[Y]$
Pour définir l'ensemble des polynômes de deux variables, on exploite aussi l'anneau $\mathbb{K}[X]$, comme base des coefficients de la variable Y.

$$\mathbb{K}[X,Y] = (\mathbb{K}[X])[Y]$$

On en reparlera plus loin…

3. Degré

3.1. Définition

Définition - Degré d'un polynôme
Soit $P \in \mathbb{K}[X]$, $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$.
On appelle *degré* de P, l'entier n que l'on note $\deg P$, c'est aussi

$$\max\{k \in \mathbb{N} \mid a_k \neq 0\}$$

Par convention, le degré du polynôme nul vaut $-\infty$.
Les scalaires a_k s'appellent les coefficients du polynôme, a_n s'appelle le *coefficient dominant* de P.
On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Définition - Polynôme normalisé ou unitaire
Si $[P]_{\deg P} = 1$, P est dit *normalisé* ou *unitaire.*

Définition - Polynôme constant
Les polynômes de degré nul ou égal à $-\infty$ sont appelés *polynômes constants* (et identifiés aux éléments de $\mathbb{K}$).

Savoir faire - Montrer que $\deg P = k$
Par double inégalité :
- $(\forall\, i \geqslant k+1,\ [P]_i = 0) \Longrightarrow \deg P \leqslant k$
- $(\exists\, k \in \mathbb{N},\ [P]_k \neq 0) \Longrightarrow \deg P \geqslant k$

Définition - Monôme
λX^k est un *monôme.*

3.2. Arithmétique des degrés

Proposition - Arithmétique des degrés
Pour tout polynômes $P, Q \in \mathbb{K}[X]$

$$\forall \lambda \in \mathbb{K}^*, \deg \lambda P = \deg P$$

$$\deg(P+Q) \leqslant \max(\deg P, \deg Q) \text{ avec égalité si } \deg P \neq \deg Q$$

$$\deg PQ = \deg P + \deg Q$$

$$\deg(P \circ Q) = \deg P \times \deg Q \qquad ((P,Q) \neq (0,0))$$

Démonstration
• Les coefficients de λP, sont exactement $(\lambda a_k)_k$, donc si $\lambda \neq 0$,

$$\max\{k \in \mathbb{N} \mid a_k \neq 0\} = \max\{k \in \mathbb{N} \mid \lambda a_k \neq 0\}$$

• Pour tout $k \in \mathbb{N}$, $[P+Q]_k = [P]_k + [Q]_k$ Si $k \geqslant \max(\deg P, \deg Q) + 1$, alors $k \geqslant \deg P + 1$ et $k \geqslant \deg Q + 1$, donc $[P+Q]_k = 0 + 0 = 0$.
Ainsi $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$ Par ailleurs, si $\deg P < \deg Q$, alors $[P+Q]_{\deg Q} = 0 + [Q]_{\deg Q} \neq 0$, donc $\deg(P+Q) \geqslant \deg Q$ • Enfin, on note $d = \deg(P)$ et $g = \deg(Q)$.
Donc $[PQ]_{d+g} = \sum_{h=0}^{d+g} [P]_h [Q]_{c+d-h} = 0 + [P]_d [Q]_g + 0 \neq 0$, donc $\deg(PQ) \geqslant \deg P \times \deg Q$.
Et enfin pour tout $h > 0$,

$$[PQ]_{d+g+h} = \sum_{i=0}^{d+g+h} [P]_i [Q]_{d+g+h-i} = \sum_{i=0}^{d} [P]_i \underbrace{[Q]_{d+g+h-i}}_{=0 \text{ car } d+g+h-i > g} + \sum_{i=d+1}^{d+g+h} \underbrace{[P]_i}_{=0 \text{ car } i > d} b_{d+g+h-i} = 0$$

Ainsi $\deg(PQ) = \deg P + \deg(Q)$.
• Pour tout $k \in \mathbb{N}$, $X^k \circ Q = Q^k = Q \times Q^{k-1}$.
Donc si on note $q_k = \deg Q^k$, on a $q_k = \deg Q + \deg Q^{k-1} = \deg Q + q_{k-1}$.
$q_k = k \deg Q$ (suite arithmétique avec $q_1 = \deg Q$).
Donc ensuite par linéarité : $P \circ Q = \sum_{k=0}^{\deg P} [P]_k (Q^k)$,
donc $\deg P \circ Q \leqslant \max\{\deg Q^k, k \in [\![0, \deg P]\!]\} = \deg Q \times \deg P$.
Et comme les degrés de Q^k sont tous distincts, $\deg(P \circ Q) = \deg Q \times \deg P$. □

Savoir faire - Égalité polynomiale
Par définition, deux polynômes sont égaux si et seulement si ils ont même degré et mêmes coefficients.
On procède donc souvent en deux temps :
1. On étudie les degrés
2. On regarde (ensuite) les coefficients

3.3. Intégrité de $\mathbb{K}[X]$ et éléments inversibles

Comme le dévoile la démonstration : les résultats suivants sont indépendants du corps $\mathbb{K}$ considéré :

Proposition - Anneau intègre (sans diviseur de 0)
$\mathbb{K}[X]$ est un anneau intègre, c'est-à-dire que

$$\forall (P,Q) \in \mathbb{K}[X]^2,\ PQ = 0 \Rightarrow P = 0 \text{ ou } Q = 0.$$

Démonstration
Supposons que $PQ = 0$.

$$\deg(PQ) = \deg P + \deg Q = -\infty \Longrightarrow \deg P = -\infty \text{ ou } \deg Q = -\infty$$

□

Corollaire - Régularité
Soient $(P,Q,R) \in \mathbb{K}[X]^3$, $P \neq 0$. Alors

$$PQ = PR \Rightarrow Q = R.$$

Ce résultat de régularité est vrai même si P n'est pas inversible.

Démonstration
Il suffit de remarquer que $PQ = PR \Rightarrow P(Q-R) = 0$, donc $Q - R = 0$ et $Q = R$. □

Proposition - Eléments inversibles dans $\mathbb{K}[X]$
Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration
Soit $P \in \mathbb{K}[X]$, inversible et Q, son inverse (polynôme).
On a
$$\deg(P \times Q) = \deg(P) + \deg(Q) = \deg(1) = 0$$
Donc, comme $\deg(Q) \geqslant 0$, on a donc $\deg(P) \leqslant 0$.
Ainsi, $P = 0$ (degré égal à $-\infty$) ou P est contant.
Réciproquement, si $P = \lambda (\neq 0)$, alors avec $Q = \frac{1}{\lambda}$, on a $P \times Q = 1$.
Et si $P = 0$, pour tout Q, $P \times Q = 0$, donc P n'est pas inversible.
Finalement l'ensemble des polynômes inversibles est $\mathbb{K}_1[X] \setminus \{0\}$ □

3.4. Valuation

Définition - Valuation d'un polynôme
On appelle valuation de P l'entier $\min\{k \in \mathbb{N} \mid a_k \neq 0\}$.
On pourrait la noter $v_X(P)$.

Exemple - Degré et valuation de $P = 3(X+1)^2 - 3(X-1)$?
$\deg P = 2$ et $v_X(P) = 1$.

Remarque - Elargissement de définition
On retrouve la définition de la valuation p-adique.
Mais ici, on il s'agit de la valuation X-adique
$$v_X(P) = \max\{k \in \mathbb{N} \mid X^k | P \text{ et } X^{k+1} \not| P\}$$

Savoir faire - Montrer que $v_X(P) = k$
Par double inégalité :
— $\left(\forall\ i \leqslant k-1,\ [P]_i = 0\right) \Longrightarrow v_X(P) \geqslant k$
— $\left(\exists\ k \in \mathbb{N},\ [P]_k \neq 0\right) \Longrightarrow v_X(P) \leqslant k$

Exercice
Quelle est la valuation de $P \times Q$?

Correction
$v_X(P \times Q) = v_X(P) + v_X(Q)$

4. Dérivation d'un polynôme

4.1. Définition

Définition - Polynôme dérivé
Soit $P = a_0 + a_1 X + \cdots + a_n X^n = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme non constant. On définit le *polynôme dérivé* de P par
$$P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1} = \sum_{k=0}^{n-1} (k+1) a_k X^k = \sum_{k=1}^{n} k a_k X^{k-1}$$
Si P est constant, on pose $P' = 0$.

Proposition - Degré et dérivation
Soit $P \in \mathbb{K}[X]$. Si $\deg P \geqslant 1$ alors $\deg P' = (\deg P) - 1$.
Et également pour tout $k \in \mathbb{N}$: $[P']_k = (k+1)[P]_{k+1}$.
En particulier : $[P']_{\deg P - 1} = \deg P \times [P]_{\deg P}$

Pour aller plus loin - Définition algébrique
Cette définition, bien que calquée sur la formule de la dérivation de fonctions polynomiales en analyse, est très différente. En particulier, il n'est jamais question ici de passage à la limite. Et surtout, il s'agit bien d'une définition « globale » : sur la forme et non « locale » : en des points…

Démonstration
Il suffit de lire l'écriture de P' □

4.2. Dérivation d'opérations polynomiales

Théorème - Linéarité de la dérivation
Pour $(\lambda, \mu) \in \mathbb{K}^2$ et $(P, Q) \in \mathbb{K}[X]^2$ on a :
$$(\lambda P + \mu Q)' = \lambda P' + \mu Q'$$
$$\left(\sum_{i \in I} \lambda_i P_i\right)' = \sum_{i \in I} \lambda_i P_i'$$
$$(PQ)' = P'Q + PQ'$$
$$(P_1 P_2 \dots P_n)' = \sum_{i=1}^{n} P_i' \prod_{j=1, j \neq i}^{n} P_j \text{ et } (P^n)' = nP'P^{n-1}$$
$$(P \circ Q)' = Q' \times P' \circ Q$$

Démonstration
On notera $P = \sum_{k=0}^{d} a_k X^k$ et $Q = \sum_{h=0}^{g} b_h X^h$.
— Soient $\lambda, \mu \in \mathbb{K}$, (quitte à compléter avec $a_g = 0$ ou $b_d = 0 \dots$), on a
$$\lambda P + \mu Q = \sum_{k=0}^{\max(d,g)} (\lambda a_k + \mu b_k) X^k$$
$$(\lambda P + \mu Q)' = \sum_{k=0}^{\max(d,g)} k(\lambda a_k + \mu b_k) X^{k-1} = \sum_{k=0}^{\max(d,g)} k \lambda a_k X^{k-1} + \sum_{k=0}^{\max(d,g)} k \mu b_k X^{k-1}$$
$$= \lambda P' + \mu Q'$$
— On applique donc la règle de dérivation d'une somme :
$$(PQ)' = \left(\sum_{k=0}^{d+g} \left(\sum_{h=0}^{k} a_h b_{k-h}\right) X^k\right)' = \left(\sum_{k=0}^{d+g} k \left(\sum_{h=0}^{k} a_h b_{k-h}\right) X^{k-1}\right)'$$
Alors que
$$P'Q + PQ' = \left(\sum_{k=0}^{d+g} \left(\sum_{h=0}^{k} (h a_h) b_{k-h}\right) X^{k-1}\right) + \left(\sum_{k=0}^{d+g} \left(\sum_{h=0}^{k} a_h (k-h) b_{k-h}\right) X^{k-1}\right)$$
$$= \left(\sum_{k=0}^{d+g} \left(\sum_{h=0}^{k} (h a_h) b_{k-h} + a_h (k-h) b_{k-h}\right) X^{k-1}\right) = \left(\sum_{k=0}^{d+g} k \left(\sum_{h=0}^{k} a_h b_{k-h}\right) X^{k-1}\right)'$$
Donc
$$(PQ)' = P'Q + PQ'$$
— Il s'agit de démontrer le résultat par récurrence sur n.
Cela est vraie pour $n = 1$ (simple) et $n = 2$ avec la question précédente (et même $n = 0$?).
Soit $n \in \mathbb{N}^*$. Supposons que le résultat soit vraie au rang n.
On a alors d'après la règle d'un produit :
$$(P_1 P_2 \dots P_n P_{n+1})' = (P_1 P_2 \dots P_n)' P_{n+1} + (P_1 P_2 \dots P_n) P_{n+1}'$$
$$= \sum_{i=1}^{n} P_i' \prod_{j=1, j \neq i}^{n} P_j P_{n+1} + (P_1 P_2 \dots P_n) P_{n+1}' = \sum_{i=1}^{n} P_i' \prod_{j=1, j \neq i}^{n+1} P_j + P_{n+1}' \prod_{j=1, j \neq n+1}^{n+1} P_j$$
$$= \sum_{i=1}^{n+1} P_i' \prod_{j=1, j \neq i}^{n+1} P_j$$
La propriété est héréditaire, la récurrence est démontrée.

— Avec $P_1 = P_2 = \cdots = P_n = P$, on a alors

$$(P^n)' = \sum_{i=1}^{n} P' \prod_{j=1, j\neq i}^{n} P = nP^{n-1}P'$$

— On a donc, en exploitant le résultat précédent et LA LINEARITE :

$$(P \circ Q)' = \sum_{k=1}^{n} a_k k Q^{k-1} Q' = Q'P'(Q)$$

□

4.3. Dérivation d'ordre supérieur

Définition - Dérivées successives
Soit $P \in \mathbb{K}[X]$. On définit par récurrence le polynôme dérivé d'ordre k :

$$P^{(0)} = P \text{ et } \forall k \geqslant 0,\ P^{(k+1)} = \left(P^{(k)}\right)'.$$

Par récurrence sur k : $\left(P^{(h)}\right)^{(k)} = P^{(h+k)}$, pour tout h

Théorème - Formule de Leibniz
Soit $(P,Q) \in \mathbb{K}[X]^2$. On a alors :

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$$

En fait, on fait la même démonstration que pour le binôme de Newton (récurrence, décalage de somme, triangle de Pascal). On peut aussi exploiter la formule de Taylor et un produit de polynôme puis identifier…

Démonstration
On note $\mathscr{P}_n$: « $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$ »

— $(PQ)^{(0)} = PQ$
— Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}_n$ est vraie.

$$\begin{aligned}
(PQ)^{(n+1)} &= \left(\sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}\right)' = \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)} Q^{(n-k)} + P^{(k)} Q^{(n-k+1)} \\
&= \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)} Q^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k+1)} \\
&= \sum_{k=0}^{n-1} \binom{n}{k} P^{(k+1)} Q^{(n-k)} + P^{(n+1)} + \sum_{k=1}^{n} \binom{n}{k} P^{(k)} Q^{(n-k+1)} + Q^{(n+1)} \\
&= P^{(n+1)}Q + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) P^{(k)} Q^{(n-k+1)} + PQ^{(n+1)} \\
&= \binom{n+1}{n+1} P^{(n+1)} Q^{(0)} + \sum_{k=1}^{n} \left(\binom{n+1}{k}\right) P^{(k)} Q^{(n-k+1)} + \binom{n+1}{0} P^{(0)} Q^{(n+1)}
\end{aligned}$$

On a donc $\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1}$

□

4.4. Applications

Cas essentiel centré en a

Le résultat suivant nous servira pour la formule de Taylor

Pour aller plus loin - Formule de Taylor
$[P]_i = \dfrac{P^{(i)}(0)}{i!}$. *Donc*

$$\frac{(PQ)^{(k)}(0)}{k!} = [PQ]_k = \sum_{i=0}^{k} [P]_i [Q]_{k-i}$$

$$(PQ)^{(k)}(0) = k! \sum_{i=0}^{k} \frac{P^{(i)}(0) Q^{(k-i)}(0)}{i!(k-i)!}.$$

Ainsi

$$(PQ)^{(k)}(0) = \binom{k}{i} P^{(i)}(0) Q^{(k-i)}(0)$$

Et ceci n'est pas uniquement vrai qu'en 0

Proposition - Dérivation du monôme
Soient $a \in \mathbb{K}$ et $n \in \mathbb{N}$. Alors

$$[(X-a)^n]^{(k)} = \begin{cases} n(n-1)\dots(n-k+1)(X-a)^{n-k} & \text{si } k < n \\ n! & \text{si } k = n \\ 0 & \text{si } k > n \end{cases}$$

Démonstration
On démontre le résultat par récurrence : sur $k!$ (n étant fixé).
Soit $n \in \mathbb{N}$. Notons $\mathscr{Q}_p$: « $[(X-a)^n]^{(k)} = \begin{cases} n(n-1)\dots(n-k+1)(X-a)^{n-k} & \text{si } k < n \\ n! & \text{si } k = n \\ 0 & \text{si } k > n \end{cases}$ »

— $[(X-a)^n]^{(0)} = (X-a)^n$, ce qui correspond.
— Soit $p \in \mathbb{N}$. Supposons que le résultat est vraie au rang p.
On sait que $[(X-a)^n]^{k+1} = \left([(X-a)^n]^k\right)'$ Si $k > n$, $[(X-a)^n]^{k+1} = 0' = 0$. Si $k = n$, $[(X-a)^n]^{k+1} = (n!)' = 0$. Si $k < n$, $[(X-a)^n]^{k+1} = \left(n(n-1)\dots(n-k+1)(X-a)^{n-k}\right)' = n(n-1)\dots(n-k+1)(n-k)(X-a)^{n-k+1}$. Donc $\mathscr{Q}_{n+1}$ est vraie

□

Formule générale

Proposition - Dérivation du polynôme P
Soit $P \in \mathbb{K}[X]$, alors pour tout $k \in \mathbb{N}$ et $j \in \mathbb{N}$:

$$[P^{(k)}]_j = \frac{(j+k)!}{j!} [P]_{j+k}$$

Démonstration
On a vu que pour tout $j \in \mathbb{N}$, $[P']_j = (j+1) \times [P]_{j+1}$.
Fixons $i \in \mathbb{N}$ et posons pour $k \leqslant i$: $a_k = (i-k)! \times [P^{(k)}]_{i-k}$.
On a alors d'après la première remarque : $[P^k]_j = (j+1) \times [P^{k-1}]_{j+1}$ Donc

$$a_k = [P^{(k)}]_{i-k} = (i-k)! \times (i-k+1)[P^{(k-1)}]_{i-k+1} = [(i-(k-1))!][P^{(k-1)}]_{i-(k-1)} = a_{k-1}$$

Donc (a_k) est constante et $a_k = a_0 = i![P^0]_i = i![P]_i$.
Ainsi pour $j = i-k$ (k fixe, changement de variable $i \leftrightarrow j$)

$$[P^{(k)}]_j = \frac{1}{j!} a_k = \frac{(j+k)!}{j!} [P]_{j+k}$$

□

Exercice d'application

Savoir faire - Passer d'une relation entre dérivés de P à une relation entre coefficients

Souvent, on cherche à résoudre une équation différentielle dont l'inconnue est un polynôme P.

1. On précise la notation du degré de P (n)
2. On remplace P, P' par leur expression sommatoire
3. On fait les multiplications prévues dans l'équation (par X, X^2…)
4. On « explose » toutes les sommes, puis on réalise dans chacune le changement de variable de manière à trouver des $\sum_h \alpha_h X^h$.
5. On recolle le tout en une seule somme du type $\sum_{h=a_1}^{a_2} (\alpha_h + \beta_h + \dots) X^h$.
Souvent, il y a des conditions de bords. Dans la somme $(\alpha_h + \beta_h + \dots)$, il ne doit pas y avoir un seul X
6. Par unicité de l'écriture polynomiale, on trouve que pour tout

$h \in [\![0,n]\!]$, $\alpha_h + \beta_h + \cdots = 0$
(n équations à résoudre. Elles sont souvent récurrence : a_{h-2} en fonction de a_h, par exemple...)

Application - $P'' + P' - \lambda X^2 P = 0$ et $X^2 P'' + P' - \lambda P = 0$
Résoudre $P'' + P' - \lambda X^2 P = 0$ (1) et $X^2 P'' + P' - \lambda P = 0$ (2).
Si $n \neq -\infty$ est le degré de $P(\neq 0)$, avec l'équation 1, on trouve que le degré de $Q = P'' + P' - \lambda X^2 P$ vaut exactement $n+2$.
Ce qui est impossible. Seul le cas $P = 0$ est donc envisageable. Et réciproquement : il s'agit bien d'une solution.
Soit n le degré de P, solution de (2), on a alors comme coefficients d'ordre n de Q : $(n(n-1)-\lambda)[P]_n$.
Comme P est solution, nécessairement, ce terme est nul donc $n(n-1) = \lambda$, ce qui nous donne une condition nécessaire sur λ (l'existence d'(au moins) une solution entière naturel de l'équation $x^2 - x - \lambda = 0$).
Ensuite, n étant alors connu, on trouve une relation de récurrence : $(n+1)[P]_{n+1} = (\lambda - n(n-1))[P]_n$...

Exercice
On considère la suite de polynômes définie par récurrence par

$$P_0 = 1, \quad \forall k \in \mathbb{N}, P_{k+1} = (1+X^2)P_k' - (2k+1)XP_k.$$

1. Calculer P_1, P_2, P_3.
2. Déterminer le degré et le coefficient dominant du polynôme P_k.
3. Etudier la parité de P_k.

Correction

1. $P_0' = 0$, donc $P_1 = -1X = -X$ ($k = 0$).
   $P_2 = -(1+X^2) + (2+1)X^2 = 2X^2 - 1$.
   $P_3 = (1+X^2)4X - 5X(2X^2-1) = 6X^3 + 9X$
2. Par récurrence on montre que le terme dominant de P_k est $(-1)^k k! X_k$.
   Cela est vrai pour les premiers polynômes P_0, (P_1, P_2 et P_3).
   Supposons que cela est vraie au rang k.
   le terme dominant de $(1+X^2)P_k'$ est donc $1 \times k(-1)^k k! X^{k+1}$,
   le terme dominant de $-(2k+1)XP_k$ est donc $-(2k+1)(-1)^k k! X^{k+1}$.
   Donc le terme dominant de P_{k+1} est $(-1)^k(k-2k-1)k!X^{k+1} = (-1)^{k+1}(k+1)k!X^{k+1}$
   La récurrence est donc démontrée.
3. On démontre que si P_k est pair (resp. impair), alors P_k' est impair (resp. pair).
   P_0 est pair. On montre alors que P_k a la même parité que k.
   Là aussi par récurrence.

5. Bilan

Synthèse

⇝ On crée un anneau théoriques des opérations algébriques à partir d'éléments d'un corps $\mathbb{K}$ (à ce stade, on peut se placer sur un anneau $\mathbb{K}$, comme $\mathbb{Z}$ - l'inversion des éléments est important pour la factorisation ou division euclidienne).
C'est un anneau des calculs finis.

⇝ On incarne alors les opérations classiques en leur donnant un sens (que) formel.
Par exemple, la dérivation se formalise sans passer par une question de limite. Tous les résultats tombent alors par simple calcul (sans limite).

⇝ Quelques notions sont importantes : additions, multiplications, compositions et aussi degré ou valuation...

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Expression formelle
— Savoir-faire - Montrer que $\deg P = k$
— Savoir-faire - Egalité polynomiale
— Savoir-faire - Montrer que $v_X(P) = k$
— Savoir-faire - Passer d'une relation entre dérivés de P à une relation entre coefficients

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$[P]_k$	Coefficient d'indice k du polynôme P	$[P+Q]_k = [P]_k + [Q]_k$ et $P \times Q]_k = \sum_{i=0}^{k} [P]_i [P]_{k-i}$	
$\deg P$	Degré de P ou $\deg P = \max\{k \in \mathbb{N} \mid [P]_k \neq 0\}$	$\deg(P+Q) \leqslant \max(\deg P, \deg Q)$, $\deg PQ = \deg P + \deg Q$ et $\deg(P \circ Q) = \deg P \times \deg Q$	
$P^{(k)}$	Dérivation k-ième de P	$[P^{(k)}]_j = \frac{(j+k)!}{j!} a_{k+j}$	On retrouve les formules classiques de dérivation

Retour sur les problèmes

99. L'anneau des polynômes est comme l'anneau théoriques des calculs algébriques. Quitte à considérer les polynômes à plusieurs variables
100. Tout passe bien, sauf la division. On en reparlera aux chapitres 20 et 21.
101. Dans le cours : $[P+Q]_k = [P]_k + [Q]_k$ et $P \times Q]_k = \sum_{i=0}^{k} [P]_i [P]_{k-i}$.
    Plus compliqué $[P \circ Q]_k$.
    $$[P \circ Q]_0 = [P]_0 + [P]_1 [Q]_0 + [P]_2 [Q]_0^2 + \ldots$$
    $$[P \circ Q]_1 = [P]_1 [Q]_1 + 2[P]_2 [Q]_0 [Q]_1 + 3[P]_3 [Q]_0^2 [Q]_1 + \ldots$$
    Trouver une formule n'est pas facile...
102. Cela existe très bien. On se débrouille sans notion de convergence (une incarnation simple peut être les nombres p-adiques). On note cet ensemble des séries formelles : $\mathbb{K}[[X]]$. Voir sur wikipedia...
103. Cours.

Chapitre 32

Fonctions polynomiales et racines

Résumé -

Au chapitre précédent nous nous sommes centrés sur le développement, l'opération inverse s'appelle la factorisation.
Ce chapitre se concentre autour d'un résultat simple mais essentiel : si $P(a)=0$, alors P est factorisable par $(X-a)$, déjà entrevu dans le premier chapitre de l'année.
Pour pouvoir écrire cela, il faut d'abord justifier ce que signifie $P(a)$ ou faire $X=a$ (pour $a\in\mathbb{K}$). On définit alors ce qu'est une racine d'un polynôme, une racine d'ordre multiple. On généralise alors les relations de Viète qui lient les coefficients d'un polynôme à ses racines.
Enfin, on se concentre sur le polynôme d'interpolation de Lagrange. Il est la réponse au problème : trouver le polynôme le plus simple (=petit en degré) qui passe par une série de points donnés.
Dans ce chapitre, les résultats d'analyse classique sur $\mathbb{R}$ (théorème des valeurs intermédiaires, théorème de Rolle...) seront fréquemment mobilisés à cause de la « bijection naturelle » entre l'ensemble des polynômes et l'ensemble des fonctions polynomiales.

Sommaire

1. Problèmes 642
2. Fonctions polynomiales et racines 643
2.1. Fonctions polynomiales 643
2.2. Racines d'un polynôme 643
2.3. Nombres maximales de racines et degré de P 644
3. Interpolation de Lagrange 645
3.1. Présentation du problème et polynômes de Lagrange 645
3.2. Interpolation (de Lagrange) 646
4. Racines multiples et formule de Taylor 647
4.1. Formules de Taylor (polynômiale) 647
4.2. Multiplicité d'une racine 648
5. Relations coefficients-racines 649
5.1. Polynôme scindé 649
5.2. Fonctions symétriques élémentaires 649
5.3. Applications 650
6. Théorème fondamental de l'algèbre 652
7. Bilan 652

1. Problèmes

Problème 136 - Egalité de polynômes

Si X est une « variable » qui ne signifie rien, si ce n'est la règle opératoire, que veut dire que deux polynômes sont égaux.
Par exemple X^2-1 et $(X-1)\times(X+1)$ sont-ils égaux? Pourquoi?

Problème 137 - Egalité de polynômes et racines

Si l'on prolonge le problème précédent, à quelle condition deux polynômes P et Q sont égaux, si ils vérifient

$$P(a_k)=Q(a_k)\qquad\forall\ k\in\mathbb{N}_p$$

Est-ce que cela dépend de p (plus il y a de conditions, plus il y a de « chances » (ou nécessité) que $P=Q$)?
Est-ce que cela dépend du corps $\mathbb{K}$ sur lequel on travaille?
(Exemple : X^p-X s'annule en tous les nombres de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ et pourtant ce n'est pas le polynôme nul...)

Problème 138 - Expérience et expression polynomiale

On réalise p expériences qui donne en des points $x_1,\dots x_p$ des valeurs $y_1,\dots y_p$ respectivement.
Est-il possible de donner une expression simple (polynomiale, de degré minimal), unique (?) qui lie y_i à x_i, pour tout $i\in\mathbb{N}_p$?

Problème 139 - Nombre de racines

On a vu en début d'année (pour $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$) ou dans un DS (pour $\mathbb{K}=\frac{\mathbb{Z}}{p\mathbb{Z}}$) qu'un polynôme de degré p ne peut admettre plus de p racines. Est-il possible qu'il en admette exactement p, à tous les coups (ce qui donne un théorème simple)?
On sait que $(X-1)^6$ n'admet qu'une racine : 1. Est-il possible d'élargir la notion de racines pour que le théorème précédent soit juste. Ici, il faudrait dire que 1 est 6 fois racines...

Problème 140 - Construction de $\mathbb{K}[X,Y,Z,\dots]$

On peut rencontrer des opérations polynomiales de plusieurs variables : dans un calcul algébriques, deux nombres peuvent être à étudier en particulier comme variables, les autres étant des paramètres. Avec la formule des « petits Bernoullis » :

$$b^n-a^n=(b-a)\left(\sum_{k=0}^{n-1}b^k a^{n-1-k}\right)$$

Comment construire les polynômes de plusieurs variables Y^n-X^n?
Est-ce que si $\forall\ P\in\mathbb{K}[X,Y]:\forall\ a\in\mathbb{K},P(a,a)=0\Longrightarrow P=(X-Y)Q$?

? Problème 141 - Développement de $\prod_{k=1}^{n}(X-x_k)$

Lorsqu'on développe ce polynôme, on trouve une expression du type $P=\sum_{i=0}^{n} a_i X^i$.
Quel est le lien entre ces nombres a_i et les x_k?
Le développement de petite valeur (et le théorème de Viète) donne le sentiment que pour tout $i\in[\![0,n]\!]$, a_i est une fonction polynomiale en les n variables x_i.
Quelle est cette expression? Que se passe-t-il lorsqu'on inverse dans cette expression x_i avec x_j ? On parle de polynôme symétrique.
Réciproquement, est-ce que tout polynôme symétrique en $\{x_k\}$ est une expression (polynomiale?) des a_i ?

2. Fonctions polynomiales et racines

2.1. Fonctions polynomiales

Définition - Fonctions polynomiales
Soit $P\in\mathbb{K}[X]$, $P=a_0+a_1X+\cdots+a_nX^n$. L'application

$$\begin{array}{rccc}\widetilde{P}: & \mathbb{K} & \to & \mathbb{K}\\ & x & \mapsto & a_0+a_1x+\cdots+a_nx^n\end{array}$$

est appelée *fonction polynomiale associée* à P.

Remarque - De la fonction polynomiale au polynôme?
L'application $\widetilde{P}$ se conçoit bien, mais la réciproque n'est pas forcément évidente a priori.
Etant donnée une fonction, dont on sait qu'elle est polynomiale, pourquoi pourrait-on lui associé comme antécédent un unique polynôme?
Autrement écrit, a-ton nécessairement $\widetilde{P}=\widetilde{Q}\Longrightarrow P=Q$?

Théorème - Correspondance polynôme et fonction polynomiale
Soient $(P,Q)\in\mathbb{K}[X]^2$, $(\lambda,\mu)\in\mathbb{K}^2$. On a

$$\widetilde{PQ}=\widetilde{P}\widetilde{Q}$$
$$\widetilde{\lambda P}=\lambda\widetilde{P}$$
$$\widetilde{P+Q}=\widetilde{P}+\widetilde{Q}$$
$$\widetilde{P\circ Q}=\widetilde{P}\circ\widetilde{Q}$$

De plus si $\mathbb{K}=\mathbb{R}$, on a $\widetilde{P}'=\widetilde{(P')}$.

Démonstration
Il s'agit d'écrire les expressions correspondantes. □

2.2. Racines d'un polynôme

Définition - Racine
Soient $P\in\mathbb{K}[X]$, $a\in\mathbb{K}$.
On dit que a est *racine* de P (ou est un *zéro* de P) si $\widetilde{P}(a)=0$.

Théorème - Racine et division
Soient $P\in\mathbb{K}[X]$, $a\in\mathbb{K}$.
Alors a est racine de P si et seulement il existe $T\in\mathbb{K}[X]$ tel que $P=(X-a)T$.
Dans ce cas on dit que $X-a$ divise P dans $\mathbb{K}[X]$.

Démonstration
Commençons par une remarque calculatoire, en supposant que $P=\sum_{k=0}^{d}a_kX^k$:

$$P-\widetilde{P}(a)=\sum_{k=1}^{d}a_k(X^k-a^k)=\sum_{k=1}^{d}a_k\Big(\sum_{h=0}^{k-1}X^ha^{k-h-1}\Big)(X-a)$$

On note $T=\sum_{k=1}^{d}a_k\big(\sum_{h=0}^{k-1}X^ha^{k-h-1}\big)\in\mathbb{K}[X]$.
Ainsi : a racine de P
si et seulement si $\widetilde{P}(a)=0$ $\quad P=(X-a)T$ □

Proposition - Factorisation
Soient $P\in\mathbb{K}[X]$ et $a_1,a_2,\dots,a_k\in\mathbb{K}$, k racines (distinctes) de P.
Alors $\prod_{i=1}^{k}(X-a_i)$ divise P (i.e. il existe $T\in\mathbb{K}[X]$ tel que $P=T\times\prod_{i=1}^{k}(X-a_i)$.

Démonstration
On procède par récurrence : en considérant, pour tout $h\in[\![1,k]\!]$: $\mathscr{P}_h$: « $\prod_{i=1}^{h}(X-a_i)$ divise P ».

— a_1 est une racine de P, donc $P=(X-a_1)Q_1$. Donc $\mathscr{P}_1$ vraie.
— Soit $h\in[\![1,k-1]\!]$. Supposons que $\mathscr{P}_h$ est vérifiée.
On a donc $P=\prod_{i=1}^{h}(X-a_i)Q_h$. a_{h+1} est par hypothèse une racine de P, donc $\prod_{i=1}^{h}(a_{h+1}-a_i)\widetilde{Q_h}(a_{h+1})=0$.
Or un produit de réel est nul ssi l'un des termes est nul. Ce qui n'est pas le cas des $a_{h+1}-a_i$.
Donc $\widetilde{Q_h}(a_{h+1})=0$, et donc $Q_h=(X-a_{h+1})Q_{h+1}$.
Ainsi $P=\prod_{i=1}^{h+1}(X-a_i)Q_{h+1}$, et donc $\mathscr{P}_{h+1}$ est vraie.

□

2.3. Nombres maximales de racines et degré de P

Corollaire - Nombre maximal de racines
Un polynôme non nul de degré inférieur ou égal à n admet au plus n racines,
ce qui équivaut à :
Un polynôme de degré inférieur ou égal à n qui admet au moins $n+1$ racines est nul.

Démonstration
L'équivalence est simplement due à la contraposition.
Si P est non nul, de degré n admettant k racines.
On a donc $\prod_{i=1}^{k}(X-a_i)$ divise P,
Donc $\deg(\prod_{i=1}^{k}(X-a_i))\leqslant\deg P=n$, i.e. $k=\sum_{i=1}^{k}1\leqslant n$. □

Corollaire - Critère de nullité d'un polynôme
On rappelle que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Soit $P \in \mathbb{K}[X]$ tel que $\forall a \in \mathbb{K}, \widetilde{P}(a) = 0$ alors $P = 0$.

Démonstration
Comme $\mathbb{K}$ est infini, P admet une infinité de racines distinctes, donc plus que son degré. Et donc $P = 0$ □

Attention - Cas de corps non fini…
Ce résultat (ainsi que le suivant) se généralise à $\mathbb{K}$ corps infini mais pas au cas où $\mathbb{K}$ est fini.

Corollaire - Bijection $\mathbb{K}[X]$ et fonction polynomiale
L'application de $\mathbb{K}[X]$ dans l'ensemble des fonctions polynomiales à coefficients dans $\mathbb{K}$ qui à P associe $\widetilde{P}$ est une bijection. On peut donc confondre polynôme et fonction polynomiale et noter $P(a)$ au lieu de $\widetilde{P}(a)$.

Ce corollaire permet de clore la question que nous nous étions posées en début de chapitre.

Démonstration
Le problème n'est pas celui de la surjectivité (par définition des fonctions polynomiales), mais de l'injectivité.
Si P et Q sont telles que pour tout $x \in \mathbb{K}$, $\widetilde{P}(x) = \widetilde{Q}(x)$, alors $\widetilde{P-Q}(x) = 0$.
Donc $P - Q$ est le polynôme nul, i.e. $P = Q$. □

Corollaire - Egalité de FONCTIONS polynomiales
Deux fonctions polynomiales sur $\mathbb{R}$ ou sur $\mathbb{C}$ sont égales si et seulement si elles ont même degré et mêmes coefficients.

Démonstration
Si deux fonctions polynomiales sont égales, alors dans ce cas, les deux polynômes associés sont les mêmes.
Et réciproquement □

Exercice
Soit $(P,Q) \in \mathbb{R}_2[X]^2$ tels que $\widetilde{P}(0) = \widetilde{Q}(0), \widetilde{P}(1) = \widetilde{Q}(1), \widetilde{P}(2) = \widetilde{Q}(2)$. Montrer que $P = Q$.

Correction
$T = P - Q$. T est de degré 2 est admet (au moins) trois racines distinctes : 0, 1 et 2.
Donc $T = 0$ et $P = Q$.

3. Interpolation de Lagrange

3.1. Présentation du problème et polynômes de Lagrange

Heuristique - Problème d'interpolation
Pour toute cette partie, on considère : $x_1, \dots, x_n$ des éléments distincts de $\mathbb{K}$ et $y_1, \dots, y_n \in \mathbb{K}$.
En fait on cherche P le plus simple possible (= de degré minimal) tel que pour tout $i \in \mathbb{N}_n$, $P(x_i) = y_i$.
On appelle un tel problème, un problème d'interpolation. C'est un problème classique en science…

Proposition - Polynômes de Lagrange
Les polynômes définis par

$$L_i = \frac{\prod_{h \neq i} (X - x_h)}{\prod_{h \neq i} (x_i - x_h)}$$

vérifient $\forall (i,j) \in [\![1,n]\!]^2, L_i(x_j) = \delta_i^j$.

Démonstration

$$L_i(x_j) = \frac{\prod_{h \neq i} (x_j - x_h)}{\prod_{h \neq i} (x_i - x_h)}$$

Donc si $j \neq i$, il existe un h tel que $x_j = x_h$ et dans ce cas $L_i(x_j) = 0$.
si $j = i$, alors le produit ne s'annule pas, mais ce réduit : $L_i(x_i) = \frac{\prod_{h \neq i} (x_i - x_h)}{\prod_{h \neq i} (x_i - x_h)} = 1$.
Donc $L_i(x_j) = \delta_{i,j}$.
□

Attention - Dépendance de L_i
Bien que la notation semble faire croire que les L_i ne dépendent que de i (ou $x_i \dots$). Il n'en est rien.
Chaque L_i dépend bien de x_i mais aussi totalement de la famille $(x_1, x_2, \dots x_n)$ donc de chaque x_h.

3.2. Interpolation (de Lagrange)

Théorème - Interpolation selon Lagrange (minimal en degré)
Il existe un unique polynôme P de degré inférieur ou égal à $n-1$ vérifiant :

$$\forall i \in [\![1,n]\!], P(x_i) = y_i.$$

C'est $P = \sum_{i=1}^{n} y_i L_i$.

Démonstration
Concernant l'existence, il suffit de considérer : $P = \sum_{i=1}^{n} y_i L_i$,
comme pour tout $i \in [\![1,n]\!]$, $\deg L_i = n-1$, on a donc $\deg P \leqslant n-1$.
puis $P(x_i) = \sum_{h=1}^{n} y_h L_h(x_i) = \sum_{h=1}^{n} y_h \delta_{h,i} = y_i$.
Concernant l'unicité : si Q vérifie les mêmes propriétés que P,
alors $P - Q$ est de degré $n-1$ et admet n racines distinctes : $x_1, x_2, \dots x_n$,
donc $P = Q$. □

En prenant $y_i = f(x_i)$, on a le corollaire suivant :

Corollaire - Interpolation aux fonctions
Soient $f \in \mathscr{F}(I, \mathbb{R})$ et $x_1, \dots, x_n$ n points distincts de I, alors il existe un unique polynôme P de degré $n-1$ coïncidant avec f en ces n points (polynôme d'interpolation de Lagrange de f).

Corollaire - Interpolation selon Lagrange (général en degré)
Les polynômes $Q \in \mathbb{K}[X]$ tels que $\forall i \in [\![1,n]\!], Q(x_i) = y_i$ sont les polynômes de la forme $\sum_{i=1}^{n} y_i L_i + T$ où $T \in K[X]$ admet $x_1,\dots,x_n$ pour racines (entre autres).

Démonstration
Soit Q qui interpole $(y_1,\dots y_n)$ et $(x_1,\dots x_n)$, sans condition sur les degrés.
Faisons la division euclidienne de Q par $T = \prod_{i=1}^{n}(X-a_i)$.
T est degré n, donc $Q = ST + R$, avec $\deg R \leqslant n-1$.
Puis pour tout $i \in [\![1,n]\!]$, $Q(x_i) = y_i = S(x_i)T(x_i) + R(x_i) = 0 + R(x_i)$.
Comme $\deg R \leqslant n-1$ et R interpole $(y_1,\dots y_n)$ et $(x_1,\dots x_n)$, par unicité : $R = \sum_{i=1}^{n} y_i L_i$.
Finalement : $Q = \sum_{i=1}^{n} y_i L_i + T$, avec T ayant $x_1,\dots,x_n$ pour racines (entre autres). □

4. Racines multiples et formule de Taylor

4.1. Formules de Taylor (polynômiale)

Théorème - Formule de Taylor
Soient $P \in \mathbb{K}[X]$, $\deg P = n$, $a \in \mathbb{K}$. Alors :

$$P = P(a) + P'(a)(X-a) + \cdots + \frac{P^{(n)}(a)}{n!}(X-a)^n = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Démonstration
Notons $T(X) = P(X+a) = \sum_{k=0}^{n} a_k (X+a)^k = \sum_{k=0}^{n} b_k X^k$ Donc $P(X) = T(X-a) = \sum_{k=0}^{n} b_k (X-a)^k$.
Puis $P^{(h)} = \sum_{k=0}^{n} b_k [(X-a)^k]^{(h)} = \sum_{k=h}^{n} b_k \frac{k!}{(k-h)!}(X-a)^{k-h}$.
Et donc en a : $P^{(h)}(a) = h! b_h + \sum_{k=h+1}^{n} b_k \frac{k!}{(k-h)!} \underbrace{(a-a)^{h-k}}_{=0}$.
Ainsi, $b_h = \frac{P^{(h)}}{h!}$ et donc $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$ □

Savoir faire - Division euclidienne et formule de Taylor
La définition de la division euclidienne (et son usage) sera présenté au chapitre suivant… Cet exercice semble un peu trop précoce, mais il est bien en lien avec la formule de Tayor

Exercice
Soient $n > 2$ et $a \in \mathbb{C}$. Déterminer le reste et le quotient dans la division euclidienne de $X^n + 1$ par $(X-a)^3$.

Correction
On applique la formule de Taylor avec $P = X^n + 1$, on a donc :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \underbrace{\left(\sum_{k=3}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-3}\right)}_{=Q}(X-a)^3 + \underbrace{\sum_{k=0}^{2} \frac{P^{(k)}(a)}{k!}(X-a)^k}_{=R}$$

Et comme pour $k \geqslant 1$, $P^{(k)}(a) = \frac{n!}{(n-k)!}a^{n-k}$, et $P^{(0)}(a) = a^n + 1$, on a donc

$$Q = \sum_{k=3}^{n} \binom{n}{k} a^{n-k}(X-a)^{k-3} \text{ et } R = (a^n+1) + n a^{n-1}(X-a) + \frac{n(n-1)}{2}a^{n-2}(X-a)^2 =$$

(On aurait pu aussi exploiter $X^n + 1 = ((X-a)+a)^n + 1 = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}(X-a)^k + 1$).

Pour aller plus loin - Problème LAGRANGE/TAYLOR
Dans l'interpolation de Lagrange, on cherche P minimal (en degré) tel que

$$\forall\ i \in \mathbb{N}_r, \qquad P(x_i) = y_i$$

Dans l'interpolation de Taylor, on cherche P minimal (en degré) tel que

$$\forall\ i \in \mathbb{N}_r, \qquad P^i(x) = y_i$$

*Il arrive, qu'on rencontre des problèmes d'interpolation mixte entre ces deux problèmes (*HERMITE…*)*

4.2. Multiplicité d'une racine

Définition - Racine de multiplicité m
Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $m \in \mathbb{N}^*$. On dit que a est *racine de multiplicité m* (ou d'ordre (de multiplicité) m) de P si $(X-a)^m$ divise P mais $(X-a)^{m+1}$ ne divise pas P.
Par extension, si $P(a) \neq 0$, on dit parfois que a est une racine de multiplicité 0 de P (c'est-à-dire n'est PAS racine de P…).
On note $\mu(a,P)$, l'ordre de multiplicité de a comme racine de P (il peut être nul)

Savoir faire - Exploitation d'une racine d'ordre m
a est racine d'ordre m ssi $P(X) = (X-a)^m Q(X)$, avec $Q(a) \neq 0$

Théorème - Caractérisation des racines multiples
Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $m \in \mathbb{N}^*$. Alors a est racine de multiplicité m de P si et seulement si

$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0 \text{ et } P^{(m)}(a) \neq 0$$

Démonstration
Si a est une racine d'ordre m de P.
Alors $P = (X-a)^m Q(X)$, avec $Q(a) \neq 0$.
La formule de Leibniz donne

$$P^{(k)}(X) = \sum_{h=0}^{k} \binom{k}{h} [(X-a)^m]^{(h)} Q^{(k-h)}(X) = \sum_{h=0}^{\min(k,m)} \frac{k!m!}{h!(k-h)!(m-h)!}(X-a)^{m-h}Q^{(k-h)}(X)$$

Donc

$$P^{(k)}(a) = \begin{cases} 0 & \text{si} \quad k < m \\ \frac{k!}{(k-m)!}Q^{(k-m)}(a) & \text{si} \quad k \geqslant m \end{cases}$$

Ainsi pour $k < m$, $P^{(k)}(a) = 0$ et $P^{(m)}(a) = m!Q(a) \neq 0$ Réciproquement, on suppose que $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.
on applique la formule de Taylor à P de degré $n(> m)$:

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = (X-a)^m Q(X)$$

avec $Q(X) = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}$, donc $Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$. □

Exercice
Déterminer une condition nécessaire et suffisante pour que $(X+1)^{n+1} - X^{n+1} - 1$ ait au moins une racine multiple (c'est-à-dire de multiplicité $\geqslant 2$) dans $\mathbb{C}$.

Correction
On note $T = (X+1)^{n+1} - X^{n+1} - 1$, on a donc $T' = (n+1)\left((X+1)^n - X^n\right)$.
Soit a une racine multiple de T, donc $T(a) = T'(a) = 0$, ainsi $(a+1)^n - a^n = 0$, i.e. $1 + \frac{1}{a} = e^{i\frac{2k\pi}{n}}$.
On a donc $\frac{1}{a} = e^{i\frac{2k\pi}{n}} - 1 = 2ie^{i\frac{k\pi}{n}}\sin\frac{k\pi}{n}$, donc $a = \frac{-ie^{-i\frac{k\pi}{n}}}{2\sin\frac{k\pi}{n}} = \frac{ie^{i\frac{h\pi}{n}}}{2\sin\frac{h\pi}{n}}$, en posant $h = -k$, avec $0 \leqslant h \leqslant n-1$.
Puis, on calcule $T(a)$, (on exploite $(a+1)^n = a^n$),

$$T(a) = (a+1)^{n+1} - a^{n+1} - 1 = a^n((a+1)-1) - 1 = a^{n+1} - 1$$

Pour que $T(a) = 0$, il faut que $a^{n+1} = 1$, donc il faut $|a| = 1$, or $|a| = \frac{1}{2|\sin\frac{h\pi}{n}|}$.
Il faut donc que $\sin\frac{h\pi}{n} = \pm\frac{1}{2}$, donc $\frac{h\pi}{n} \equiv \pm\frac{\pi}{6}[2\pi]$, ou $\frac{h\pi}{n} \equiv \pm\frac{5\pi}{6}[2\pi]$,
on a alors $6h \equiv \pm n[12n]$, ou $6h \equiv \pm 5n[12n]$.
il faut donc que 6 divise n (5 et 6 sont premiers entre eux).
Supposons donc que $n = 6m$. On a alors $h = m$ (car $h \in [\![0, n-1]\!]$), ou $h = 5m$.
On a alors

$$a = \frac{ie^{i\frac{m\pi}{6m}}}{2\sin\frac{m\pi}{6m}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = e^{i\frac{2}{3}\pi} = j \text{ ou } a = \frac{ie^{i\frac{5m\pi}{6m}}}{2\sin\frac{5m\pi}{6m}} = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = e^{-i\frac{2}{3}\pi} = j^2$$

Vérifions que cela fonctionne bien (il suffit d'en vérifier un).
$T(j) = (1+j)^{6m+1} - j^{6m+1} - 1 = -j^2 - j - 1 = -j^2 - j - 1 = 0$ et $T(j^2) = (1+j^2)^{6m+1} - (j^2)^{6m+1} - 1 = -j - j^2 - 1 = 0$
Une condition nécessaire et suffisante : 6 divise n.

5. Relations coefficients-racines

5.1. Polynôme scindé

Nous allons formaliser des résultats vues en début d'année dans l'art de calculer.

Savoir faire - Corps algébriquement clos

Un corps dont tous les polynômes sont nécessairement scindés est appelé un corps algébriquement clos.
Nous en reparlerons lorsque nous aurons vu le théorème fondamental de l'algèbre

Définition - Polynôme scindé

Soit $P \in \mathbb{K}[X]$. On dit que P est scindé sur $\mathbb{K}$ si P s'écrit

$$P = a_n \prod_{i=1}^{n} (X - x_i)$$

où les x_i sont les racines de P dans $\mathbb{K}$ comptées avec leur multiplicité (c'est-à-dire écrites autant de fois que leur multiplicité) et a_n est le coefficient dominant de P.

Remarque - Corps $\mathbb{K}$

Ce résultat dépend du corps $\mathbb{K}$.

5.2. Fonctions symétriques élémentaires

Définition - Fonctions symétriques élémentaires

Soit $P \in \mathbb{K}[X]$ un polynôme scindé sur $\mathbb{K}$ tel que $\deg P = n$.
Soient $x_1, x_2, \dots, x_n$ ses racines comptées avec leur multiplicité. On définit les fonctions symétriques élémentaires des racines :

$$\sigma_1 = x_1 + \cdots + x_n$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + \cdots + x_{n-1}x_n = \sum_{1 \leqslant i < j \leqslant n} x_i x_j$$
$$\vdots$$
$$\sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \dots x_{i_k}$$
$$\vdots$$
$$\sigma_n = x_1 x_2 \dots x_n$$

Savoir faire - Ecrire ces sommes (de Newton)

σ_k correspond à la somme de tous les possibles en prenant exactement k éléments de $\mathbb{N}_n = \{1, 2, \dots n\}$ et en multipliant les nombres x_i indexés par ces k éléments :

$$\sigma_k = \sum_{I_k \subset \binom{\mathbb{N}_n}{k}} \prod_{i \in I_k} x_i$$

Evidemment, même si cela ne se note pas σ_k dépend aussi de n…

Pour aller plus loin - Généralisation

Plus fort :
Tout polynôme symétrique de $\mathbb{K}^n$ dans $\mathbb{K}$ s'exprime à l'aide des fonctions symétriques élémentaires σ_k.

Par exemple (exercice!), si on note $S_p = \sum_{i=1}^{n} x_i^p$, on a :

1. $S_p - \sigma_1 S_{p-1} + \cdots + (-1)^{n-1}\sigma_{n-1}S_{p-n} + (-1)^n \sigma_n S_{p-n} = 0$ *pour* $p \geqslant n$
2. $S_p - \sigma_1 S_{p-1} + \cdots + (-1)^{p-1}\sigma_{p-1}S_1 + (-1)^p \sigma_p \times p = 0$ *pour* $1 \leqslant p \leqslant n-1$

Ce résultat est à la base du théorème de Galois sur les racines des équations polynomiales de degré $\geqslant 5$.

Analyse - Relation de récurrence

Remarquons que si l'on note σ_k^n le terme σ obtenu pour les nombres $x_1, \dots x_n$.
On a donc

$$\begin{aligned} x_n\sigma_{k-1}^{n-1} &= x_n \times \Big(\sum_{1 \leqslant i_1 < i_2 \cdots < i_{k-1} \leqslant n-1} x_{i_1}x_{i_2}\cdots x_{i_{k-1}} \\ &= \sum_{1 \leqslant i_1 < i_2 \cdots < i_{k-1} \leqslant n-1} x_{i_1}x_{i_2}\cdots x_{i_{k-1}}x_n \\ &= \sum_{1 \leqslant i_1 < i_2 \cdots < i_{k-1} \leqslant n-1, i_k = n} x_{i_1}x_{i_2}\cdots x_{i_{k-1}}x_{i_k} \\ &= \sigma_k^n - \sigma_k^{n-1} \end{aligned}$$

Donc $\sigma_k^n = \sigma_k^{n-1} + x_n\sigma_{k-1}^{n-1}$.

Exercice

Ecrire σ_3 et σ_4 pour $n = 5$

Correction

$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 + x_1x_3x_5 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + x_3x_4x_5$.
$\sigma_4 = x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_2x_3x_4x_5$.

Heuristique - Relation coefficients-racines (par récurrence)

Notons $P_n = \lambda(X - x_1)\dots(X - x_n)$, on a donc $P_n = (X - x_n)P_{n-1}$.
Et donc pour tout $k \in \mathbb{N}$

$$[P_n]_k = [P_{n-1}]_{k-1} - x_n[P_{n-1}]_k$$

Cette relation ressemble beaucoup à la relation vue plus haut (avec un changement de signe).
Par ailleurs $[P_n]_n = \lambda$ et $\sigma_0 = 1$ (somme vide).
On montre alors par récurrence (sur n et pour tout k) :

$$\sigma_k^n = (-1)^k \frac{[P_n]_{n-k}}{\lambda} = (-1)^k \frac{[P_n]_{n-k}}{[P_n]_n}$$

Théorème - Relations coefficients-racines

On a les relations suivantes entre les coefficients et les racines (**écrites avec leur multiplicité**) du polynôme scindé P :

$$\forall k \in [\![1, n]\!], \quad \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

Démonstration

Supposons que $P = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 = a_n(X - x_1)(X - x_2)\cdots(X - x_n)$.
Dans le développement de P (écrit initialement sous forme factorisée), on obtient X^p en prenant p termes X dans le produit et en choisissant $n - p$ termes dans l'ensemble $\{-x_i, i \in \mathbb{N}_n\}$.
Il faut considérer tous les cas possibles, en raisonnant sur les indices des x_i et non sur les nombres x_i eux-mêmes. :

$$a_pX^p = a_n \times \left(\sum_{\{i_1, i_2, \dots i_p\} \subset \binom{\mathbb{N}_n}{p}} (-x_{i_1})(-x_{i_2})\dots(-x_{i_p}) \right) X^p$$

ou encore :

$$\sigma_p = \sum_{I_p \subset \binom{\mathbb{N}_n}{p}} \prod_{i \in I_p} x_i = (-1)^p \frac{a_p}{a_n}$$

□

5.3. Applications

Heuristique - Fonctions symétriques générales

Cela permet d'écrire toute expression polynomiale en les racines d'un polynôme, invariante par permutation, en fonction des coefficients du polynôme.
on peut en effet prouver qu'une telle expression s'exprime facilement à l'aide des σ_k.
en particulier $S_k = x_1^k + \cdots x_n^k$ s'exprime à l'aide des coefficients.

Exercice

Déterminer les triplets $(a,b,c) \in \mathbb{C}^3$ tels que

$$\begin{cases} a+b+c &= 1 \\ a^2+b^2+c^2 &= 3 \\ a^3+b^3+c^3 &= 1 \end{cases}$$

Correction

On commence par exprimer les relations en fonctions formes symétriques élémentaires :

$$(a+b+c)^2 = a^2+b^2+c^2+2(ab+ac+bc) \Longrightarrow a^2+b^2+c^2 = \sigma_1^2 - 2\sigma_2$$

$$(a+b+c)^3 = a^3+b^3+c^3+3(ab^2+ac^2+a^2b+a^2c+b^2c+bc^2)+6abc = a^3+b^3+c^3+3(a+b+c)(ab+ac+bc)-3abc$$
$$\Longrightarrow a^3+b^3+c^3 = \sigma_1^3+3\sigma_3-3\sigma_1\sigma_2$$

Il faut résoudre le système

$$\begin{cases} \sigma_1 &= 1 \\ \sigma_1^2-2\sigma_2 &= 3 \\ \sigma_1^3+3\sigma_3-3\sigma_1\sigma_2 &= 1 \end{cases} \Longrightarrow \begin{cases} \sigma_1 &= 1 \\ \sigma_2 &= -1 \\ \sigma_3 &= -1 \end{cases}$$

Ainsi a,b et c sont les racines du polynômes $X^3-X^2-X+1 = (X-1)(X^2-1) = (X+1)(X-1)^2$.
Autrement écrit $S = \{(1,1,-1),(1,-1,1),(-1,1,1)\}$.

Savoir faire - Comment trouver la bonne combinaison en σ_i ?

Voici une méthode, elle n'est pas unique.
Assuré du théorème d'existence (que nous ne démontrons pas), nous pouvons chercher une méthode pour exprimer tout polynôme symétrique.
Soit P un tel polynôme (par exemple $P = x_1^4+x_2^4+x_3^4$).

1. Il faut d'abord trouvé le degré de P,
   si on remplace tous les x_i par X, on obtient un polynôme d'un certain degré n.
   Si ce polynôme possède plusieurs degré, alors on le coupe en addition de polynômes dont les monomes sont tous de même degré.
   Sur notre exemple $n = 4$
2. Connaissant le degré de P, on considère des facteurs à identifier devant le produit des σ_i de degré n.
   Il faut savoir que pour tout i, $\deg(\sigma_i) = i$.
   On a donc sur notre exemple :

   $$P = A\sigma_1^4 + B\sigma_2^2 + C\sigma_1^2\sigma_2 + D\sigma_1\sigma_3$$

   (3 racines, donc pas de σ_4)
3. Il s'agit ensuite de trouver les valeurs des constantes $A,B,C\ldots$.
   On peut prendre des valeurs particulières pour $x_1, x_2 \ldots$.
   Par exemple avec
   — $x_1 = x_2 = 0$ et $x_3 = x$, on a $\sigma_2 = \sigma_3 = 0$ et $\sigma_1 = x$,

   $$P = x^4 = Ax^4 \Longrightarrow A = 1$$

   — $x_1 = x$, $x_2 = -x$, $x_3 = 0$, on a $\sigma_1 = 0$, $\sigma_2 = -x^2$,

   $$P = 2x^4 = Bx^4 \Longrightarrow B = 2$$

   — $x_1 = x$, $x_2 = x$, $x_3 = 0$, on a $\sigma_1 = 2x$, $\sigma_2 = x^2$, $\sigma_3 = 0$

   $$P = 2x^4 = 1(2x)^4 + 2(x^2)^2 + C(2x)^2 \times (x^2) = (16+2+4C)x^4 \Longrightarrow C = -4$$

   — $x_1 = 2x$, $x_2 = -x$, $x_3 = 2x$, on a $\sigma_1 = 3x$, $\sigma_2 = 0$, $\sigma_3 = -4x^3$

   $$P = 33x^4 = 1(3x)^4 + D(3x) \times (-4x^3) = (81-12D)x^4 \Longrightarrow D = 4$$

Donc

$$x_1^4+x_2^4+x_3^4 = \sigma_1^4 + 2\sigma_2^2 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3$$

On peut vérifier les calculs…

Histoire - D'Alembert



Jean Le Rond d'Alembert (1717-1783), est un grand mathématicien, flamboyant, du XVIIIème siècle. Il est néanmoins souvent plus connu pour son travail avec Diderot dans la rédaction de la première encyclopédie…
Sa démonstration du théorème de d'Alembert-Gauss n'a pas résisté aux canons plus exigeants des mathématiciens du XIXième. Il avait montré que toutes racines des polynômes de $\mathbb{C}[X]$ ne pouvait se trouver que dans $\mathbb{C}$ (pas d'extension de corps possible comme pour passer de $\mathbb{R}$ à $\mathbb{C}$).
Quelques années plus tard, Gauss apporta une demi-douzaine de démonstrations différentes de ce théorème…

Exercice

On note x_1, x_2, x_3 les racines de $X^3 - X^2 + 4X + 1$.
Calculer $S = \sum_{i \neq j} x_i^3 x_j$.

Correction

$S = x_1^3x_2 + x_1^3x_3 + x_2^3x_1 + x_2^3x_3 + x_3^3x_1 + x_3^3x_2$.
Il s'agit bien d'une expression symétrique (non élémentaire) de x_1, x_2, x_3.
Notons qu'elle est d'ordre 4,

$$S = A\sigma_1^4 + B\sigma_1^2\sigma_2 + C\sigma_1\sigma_3 + D\sigma_2^2$$

Par exemple avec

— $x_1 = x_2 = 0$ et $x_3 = x$, on a $\sigma_2 = \sigma_3 = 0$ et $\sigma_1 = x$,

$$S = 0 = Ax^4 \Longrightarrow A = 0$$

— $x_1 = x$, $x_2 = -x$, $x_3 = 0$, on a $\sigma_1 = 0$, $\sigma_2 = -x^2$,

$$S = -2x^4 = Dx^4 \Longrightarrow D = -2$$

— $x_1 = x$, $x_2 = x$, $x_3 = 0$, on a $\sigma_1 = 2x$, $\sigma_2 = x^2$, $\sigma_3 = 0$

$$S = 2x^4 = B(4x^2)(x^2) - 2x^4 = (4B-2)x^4 \Longrightarrow B = 1$$

— $x_1 = 2x$, $x_2 = -x$, $x_3 = 2x$, on a $\sigma_1 = 3x$, $\sigma_2 = 0$, $\sigma_3 = -4x^3$

$$S = 12x^4 = -12Cx^4 \Longrightarrow C = -1$$

Donc

$$S = x_1^3x_2 + x_1^3x_3 + x_2^3x_1 + x_2^3x_3 + x_3^3x_1 + x_3^3x_2 = \sigma_1^2\sigma_2 - \sigma_1\sigma_3 - 2\sigma_2^2$$

D'après l'énoncé : $\sigma_1 = 1$, $\sigma_2 = 4$ et $\sigma_3 = -1$, donc

$$S = 1^2 \times 4 - 1 \times (-1) - 2(4)^2 = 4 + 1 - 32 = -27$$

6. Théorème fondamental de l'algèbre

Le théorème suivant est admis :

Théorème - Théorème de d'Alembert-Gauss
Soit $P \in \mathbb{C}[X]$, $\deg P \geqslant 1$. Alors P possède au moins une racine dans $\mathbb{C}$.

Remarque - Démonstration du théorème de d'Alembert-Gauss

Bien que ce théorème soit énoncé dans cette partie de cours, toutes les démonstrations connues exploitent quelques résultats de topologie (comme le TVI par exemple).
Une démonstration consiste à considérer $z \mapsto |P(z)|$ et supposer que $\forall\, z, |P(z)| > 0$.

1. On se place sur un fermé K, il existe z_0 tel que $\inf_{z\in K}|P(z)| = |P(z_0)| > 0$, d'après Weierstrass.
2. Or autour de z_0 ($z_0 + re^{i\theta}$, r petit, $\theta \in [0, 2\pi[$), il y a toujours un z tel que $P(z) < P(z_0)\ldots$
3. On peut prendre $P'(z_0) \in \mathbb{C}$ qui indique la pente de variation, et $\theta = -\arg(P'(z_0))\ldots$

7. Bilan

Synthèse

⇝ En regardant les valeurs prises (incarnation) par un polynôme (calcul formel) dans un corps, on peut trouver une factorisation (formelle) du polynôme.

⇝ Ces factorisations aident à résoudre le problème d'interpolation qu'on retrouve classiquement en science, grâce au polynôme de Lagrange. Mais aussi le théorème d'interpolation des dérivées (en un même point) avec la formule de Taylor.

⇝ Cette dernière formule permet de définir également l'ordre de multiplicité d'une racine, ce qui permet de conclure totalement la factorisation, même par des puissances de polynômes (racines de P de multiplicité $\geqslant 2$).

⇝ Si les polynômes se factorisent totalement (théorème de D'Alembert-Gauss), alors on doit retrouver dans les coefficients d'un polynôme, les traces de ses racines (par développement). Ce sont les formules de Newton qui s'appuie sur une forme de super-symétrie !

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Division euclidienne et formule de Taylor.
— Savoir-faire - Exploitation d'une racine d'ordre m.
— Savoir-faire - Corps algébriquement clos.
— Savoir-faire - Ecrire les sommes (de Newton)
— Savoir-faire - Comment trouver la bonne combinaison en σ_i ?

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\tilde{P}$	Application $\mathbb{K}\to\mathbb{K}$, $x\mapsto P(x)$	$\tilde{P}(a)=0 \iff \exists\, Q$ tq $P=(X-a)Q$	Par abus, on écrit $\tilde{P}=P$
$\mu(a,P)$	(ordre de) multiplicité de a comme racine de P	$\mu(a,P)=k \Leftrightarrow P=(X-a)^k Q$ avec $Q(a)\neq 0$	$k=\min\{h\in\mathbb{N}\mid P^{(h)}(a)\neq 0\}+1$
$L_i(X)=\prod_{j\neq i}\frac{X-x_j}{x_i-x_j}$	Polynômes d'interpolation de LAGRANGE	$L_i(x_j)=\delta_{i,j}$	Il dépend de tous les nombres distincts $x_1,x_2,\dots,x_n$ considérés Il donne une solution particulière au problème d'interpolation. Il faut l'addition aux solutions homogènes.
$T_{a,P}(X)=\sum_{k=0}^{n}\frac{P^{(k)}(a)}{k!}(X-a)^k$	Expression du développement de Taylor de P	$T_{a,P}=P$	Elle lie la potientielle racines en a à $P^{(k)}(a)$
$\sigma_k=\sum_{I\subset\binom{\mathbb{N}_n}{k}}\prod_{i\in I}x_i$	Fonctions symétriques élémentaires de P	$\sigma_k=(-1)^k\frac{[P]_{n-k}}{[P]_n}$ (P scindé)	$x_1,\dots x_n$ sont les racines de P (comptées avec leur multiplicité) La formule se générale à tous les polynômes symétriques en les racines de P

Retour sur les problèmes

104. $P=Q$ si et seulement si $\forall\ k\in\mathbb{N}$, $[P]_k=[Q]_k$.

105. Il suffit qu'il y ait $\max(\deg P,\deg Q)+1$ éléments distincts de $\mathbb{K}$ qui annulent $P-Q$ pour que $P=Q$ en tout élément de $\mathbb{K}$.
Il peut arriver que deux polynômes soient égaux en tout $x\in\mathbb{K}$ ($\mathbb{K}$ fini et de petites dimensions), mais les polynômes sont distincts. Ainsi de $X+1$ et X^2+1 sur $\frac{\mathbb{Z}}{2\mathbb{Z}}[X]$…

106. Voir cours. C'est le polynôme de Lagrange+Homogène :

$$\sum_{k=1}^{p} y_k\prod_{i\neq k}\frac{X-x_i}{x_k-x_i}+Q\prod_{i=1}^{p}(X-x_i)$$

107. Voir cours

108. On a vu au chapitre précédent, dans une remarque, on peut définir (par récurrence) :

$$\mathbb{K}[X_1,X_2\dots X_{n+1}]=(\mathbb{K}[X_1,\dots X_n])[X_{n+1}]$$

à condition d'accepter de se restreindre aux polynômes définis sur un anneau et non un corps.
Dans ce cas la factorisation est plus compliquée…

On pourrait par exemple exploiter les petits Bernoullis. On fixe $a\in\mathbb{R}$.

$$P(X,a)-P(a,a)=\sum_{k=1}^{n}a_k(a)(X^k-a^k)=(X-a)\sum_{k=1}^{n}a_k(a)\sum_{i=0}^{k-1}X^i a^{k-1-i}=(X-a)Q_a(X)$$

où donc Q_a est un polynôme. Mieux : $\forall\ k\in\mathbb{N}$, $[Q_a]_k\in\mathbb{K}[a]$, indépendante de a.
On peut identifier, on note : Q_k tel que $\forall\ a\in\mathbb{K}$, $Q_k(a)=[Q_a]_k$.
On obtient ainsi une factorisation de P par $X-Y$.

109. Voir cours.

Chapitre 33

L'anneau euclidien des polynômes

Résumé -

Bien qu'il s'agisse encore de factorisation de polynôme, ce chapitre est totalement différent du précédent.
En nous concentrant sur la division euclidienne des polynômes, nous voyons que l'ensemble $\mathbb{K}[X]$ ressemble profondément à $\mathbb{Z}$.
Ce chapitre ressemble donc profondément au chapitre d'arithmétique sur $\mathbb{Z}$. On définit le PGCD de deux polynômes avec l'algorithme d'Eucllide adapté, la relation de Bézout, le lemme de Gauss..., puis le PPCM de deux ou plusieurs polynômes.
Les polynômes irréductibles sont les polynômes premiers de $\mathbb{K}[X]$. On retrouve les équivalents aux théorème d'Euclide (décomposition unique en produit de polynômes irréductibles). Dans $\mathbb{C}[X]$, les polynômes irréductibles sont les polynômes de degré $\leqslant 1$ (Théorème de d'Alembert-Gauss). Et dans $\mathbb{R}[X]$, il s'agit des polynômes de degré $\leqslant 1$ ou de degré 2 avec un discriminant $\Delta < 0$.
Toute la théorie des congruences s'exportent de $\mathbb{Z}$ à $\mathbb{K}[X]$... Ce chapitre est aussi pour nous l'occasion de donner quelques vocabulaires sur les anneaux (idéaux...).

Sommaire

1. Problèmes 656
2. Division euclidienne dans $\mathbb{K}[X]$ 657
2.1. Multiples d'un polynômes 657
2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$ . . . 658
2.3. Nature de $\mathbb{K}[X]$ 659
3. Plus Grand Commun Diviseur 660
3.1. Heuristique 660
3.2. Algorithme d'Euclide et coefficients de Bézout 660
3.3. PGCD 661
3.4. Lemme de Gauss et facteurs relativement premiers . 663
3.5. Interprétation avec racines 664
3.6. PGCD de plusieurs polynômes 665
4. Plus Petit Commun Multiple 666
4.1. Caractérisation essentielle 666
4.2. Relation PGCD/PPCM 667
5. Polynômes irréductibles 668
5.1. Décomposition unique en produit d'irréductibles . . 668
5.2. Décomposition dans $\mathbb{C}[X]$ 670
5.3. Décomposition dans $\mathbb{R}[X]$ 671
6. Bilan 673

1. Problèmes

? Problème 142 - Arithmétique

L'anneau $\mathbb{Z}$ n'est pas un corps, comme $\mathbb{K}[X]$.
Néanmoins, nous avons su développer tout un chapitre intéressant sur l'étude de $\mathbb{Z}$ en développant l'arithmétique. Si l'on reprend ce chapitre, on constate qu'à la racine des résultats (PGCD, nombres premiers et congruences...) se trouve la division euclidienne.
Or nous avons également une division euclidienne dans $\mathbb{K}[X]$ (à condition que $\mathbb{K}$ soit un corps).
Quels sont alors les résultats transposables de $\mathbb{Z}$ à $\mathbb{K}[X]$? Qu'est-ce que le PGCD de deux polynômes? Quand est-ce qu'on peut dire qu'un polynôme est un polynôme premier?

? Problème 143 - Fonction arithmétique (multiplicative)

Le chapitre d'arithmétique sur $\mathbb{Z}$ s'est conclue avec les fonctions arithmétiques vérifiant $f(ab) = f(a)+f(b)$ ou $f(ab) = f(a)f(b)$ pour $a \wedge b = 1$.
Existe-t-il des fonctions additives sur les polynômes : $f(PQ) = f(P) + f(Q)$ si $P \wedge Q = 1$? C'est le cas de la fonction degré ou la valuation R-adique.
Existe-t-il des fonctions multiplicatives sur les polynômes : $f(PQ) = f(P)f(Q)$ si $P \wedge Q = 1$?
C'est le cas évidemment de $f_k : P \mapsto P^k$. Peut-on définir un produit de convolution pour créer un groupe de fonction arithmétique?

$$f * g : Q \mapsto \sum_{P|Q,\ P \text{ unitaire}} f(P)g(Q/P)$$

? Problème 144 - Théorèmes de FERMAT

On sait que pour p premier, $n^p \equiv n[P]$.
A-t-on pour P, irréductible : $Q^P \equiv Q[P]$? Mais que peut signifier Q^P?
Et le grand théorème de FERMAT : Existe-t-il des polynômes A, B, C et un entier n tel que $A^n + B^n = C^n$?

? Problème 145 - Corps à p^k éléments

On démontre que concernant les corps finis, ils ne peuvent avoir pour cardinal uniquement des nombres de la forme p^k, avec p premier.
Nous savons déjà fabriqué LE corps à p éléments : il s'agit de $\frac{\mathbb{Z}}{p\mathbb{Z}}$.
Est-il possible de « fabriquer » LE corps à p^k éléments?
La stratégie consiste à se placer sur le corps $\mathbb{Z}/p\mathbb{Z}$, puis l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$, et trouver un polynôme P de degré k irréductible dans cet anneau de polynômes et enfin de considérer l'ensemble quotient $\frac{\mathbb{Z}/p\mathbb{Z}}{(P)}$ (pour la relation d'équivalence $\cdot \equiv \cdot [P]$.
Est-il toujours possible de trouver un tel polynôme P irréductible, à tout degré?
Comment montrer qu'on obtient bien un corps à p^k éléments?

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynômes

Définition - B divise A
Soit $(A,B) \in \mathbb{K}[X]^2$, $B \neq 0$. On dit que B *divise* A dans $\mathbb{K}[X]$ s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.
On dit aussi que A *est divisible* par B, que B est un diviseur de A, ou que A est un *multiple* de B. On note $B|A$.

Définition - Ensemble des multiples
Soit P un polynôme.
L'ensemble des multiples de P est noté $P\mathbb{K}[X]$ ou (P).

Théorème - Polynômes associés
Soient $P,Q \in \mathbb{K}[X]$ deux polynômes non nuls. On a

$$(P|Q \text{ et } Q|P) \Leftrightarrow (\exists \lambda \in \mathbb{K}\setminus\{0\}, Q = \lambda P)$$

On dit alors que P et Q sont des *polynômes associés*.
On a alors $P\mathbb{K}[X] = Q\mathbb{K}[X]$

Démonstration
Comme $P|Q$, il existe R tel que $Q = RP$. Donc $\deg(Q) = \deg R + \deg P$, et ainsi $\deg(P) \leqslant \deg(Q)$.
Puis de même $\deg(Q) \leqslant \deg(P)$. Donc $\deg P = \deg Q$.
On a donc $\deg R = 0$ et donc $R = \lambda$. □

Exercice
Montrer qu'il s'agit d'une relation d'équivalence

Correction
La symétrie est implicitement exploitée dans la définition même.

Théorème - Stabilité par combinaison linéaire
Soient $P,Q \in \mathbb{K}[X], A \in \mathbb{K}[X], A \neq 0$. Soient $\lambda,\mu \in \mathbb{K}$, $(\mu \neq 0)$. Alors

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|\lambda P + \mu Q)$$

En terme de multiple : $P,Q \in A\mathbb{K}[X] \Longleftrightarrow P$ et $(\lambda P + \mu Q) \in A\mathbb{K}[X]$.
On a plus largement encore pour $P,Q,R \in \mathbb{K}[X], A \in \mathbb{K}[X], A \neq 0$ et $\mu \in \mathbb{K}^*$,

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|RP + \mu Q)$$

Démonstration
Supposons que $A|P$ et $A|Q$.
$P = AR_1$, $Q = AR_2$, donc $\lambda P + \mu Q = A(\lambda R_1 + \mu R_2)$ et $A|\lambda P + \mu Q$.
Evidemment, $A|P$.
Réciproquement si $A|P$ et $A|\lambda P + \mu Q$,
alors $P = AR_1$ et $\lambda P + \mu Q = AR_3$, donc $Q = \frac{1}{\mu}(\mu Q + \lambda P) - \frac{\lambda}{\mu}P = A(\frac{1}{\mu}R_3 - \frac{\lambda}{\mu}R_1)$, donc $A|Q$.
On voit que seul l'inversibilité de μ joue un rôle. □

Exercice
Soient $A,B \in \mathbb{R}[X]$.
Montrer que B divise A dans $\mathbb{R}[X]$ si et seulement si B divise A dans $\mathbb{C}[X]$.

Correction
Si B divise A dans $\mathbb{R}[X]$, alors il le divise aussi dans $\mathbb{C}[X]$.
Si $A = RB$, avec $R \in \mathbb{C}[X]$, on a donc $\overline{A} = A = \overline{RB} = \overline{R}B$ (conjuguaison).

Donc $A = \frac{A+\overline{A}}{2} = \frac{R+\overline{R}}{2}B = \mathrm{Re}R \times B$.
Ainsi B divise A dans $\mathbb{R}[X]$.

Exercice
Soit $P \in \mathbb{K}[X]$. Montrer que $P(X) - X$ divise $P(P(X)) - X$.

Correction
Supposons que $P = \sum_{k=0}^{d} a_k X^k$, et on note $T(X) = P(X) - X$ On va d'abord montrer que T divise $P^k - X^k$, pour tout entier k. En effet

$$P^k - X^k = (P-X)\left(\sum_{h=0}^{k-1} P^{k-1-h}X^h\right)$$

Puis par linéarité : T divise $a_k(P^k - X^k) = a_k P^k - a_k X^k$ et $\sum_{k=0}^{n} a_k P^k - \sum_{k=0}^{n} a_k X^k = P(P) - P$.
Enfin : T divise $P(P) - P + T = P(P) - P + P - X = P(P) - X$.
On verra une autre méthode plus loin avec la factorisation par les $X - a$ sur $\mathbb{C}$...

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

Théorème - Existence et unicité de la division euclidienne
Soit $(A,B) \in \mathbb{K}[X]^2$, $B \neq 0$. Alors il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ vérifiant :

$$\begin{aligned} &A = BQ + R \\ &\deg R < \deg B \qquad (\Leftrightarrow R = 0 \text{ ou } 0 \leqslant \deg R < \deg B) \end{aligned}$$

On parle alors de division euclidienne (ou de division suivant les puissances décroissantes) de A par B.

Pour aller plus loin - Division selon les puissances croissantes ?
Lorsqu'on calcule des $DL_n(0)$, on cherche à écrire des puissances croissantes en x. Par exemple lorsqu'on cherche le $DL_3(0)$ de $\frac{x^4+2x^2-x+1}{x^3+x+1}$.
Dans ce cas là, on peut poser la division exactement à l'envers et obtenir :

$$(1-x+2x^2+x^4) = (1+x+x^3)(1-2x+4x^2-5x^3) + 8x^4 - 4x^5 + 5x^6$$

Et donc

$$\frac{x^4+2x^2-x+1}{x^3+x+1} = 1 - 2x + 4x^2 - 5x^3 + O(x^4)$$

Démonstration
Soit $B \in \mathbb{K}[X]$, non nul. On note $d = \deg B$.
On commence par montrer l'existence du couple (Q,R), en raisonnant par récurrence sur $\deg A$.
On constatera que le résultat est vrai si $\deg A = -\infty$, i.e. $A = 0 : A = 0 \times B + 0$.
Pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$: « $\forall\, A \in \mathbb{K}[X]$ avec $\deg A = n$, $\exists\,(Q,R) \in \mathbb{K}[X] \times \mathbb{K}_{d-1}[X]$ tel que $A = BQ + R$ »
— Si $\deg A = 0$.
si $d > 0$, on prend $Q = 0$ et $R = A$.
si $d = 0$, on prend $Q = \frac{A}{B}$ (B non nul) et $R = 0$
Dans tous les cas, $\mathscr{P}_0$ est vraie.
— Soit $n \in \mathbb{N}$. On suppose que $\mathscr{P}_0, \mathscr{P}_1 \dots \mathscr{P}_n$ sont vraies.
Si $\deg A = n+1 < d$, on prend $Q = 0$ et $R = A$ et $\mathscr{P}_{n+1}$ est vraie.
On suppose donc que $n+1 \geqslant d$.
On considère $A = a_{n+1}X^{n+1} + A'$, avec $\deg A' < n+1$ et $a_{n+1} \neq 0$.
On suppose aussi que $[B]_d = b_d \neq 0$. On note $B = b_d X^d + B'$ avec $\deg B' < d$.
Notons $P = \frac{a_{n+1}}{b_d}X^{n+1-d}$.
On a alors $A - PB = (a_{n+1} - \frac{a_{n+1}}{b_d}b_d)X^{n+1} + (A' - \frac{a_{n+1}}{b_d}X^{n+1-d}B')$
$A - PB = A' - \frac{a_{n+1}}{b_d}X^{n+1-d}B'$.
Or $\deg(A') \leqslant n$, $\deg(\frac{a_{n+1}}{b_d}X^{n+1-d}B') = n+1-d+\deg(B') < n+1$.
$\deg(A - PB) \leqslant n$. On appliquer l'une des hypothèses de récurrence à ce $A - PB$.
Donc il existe $Q_1, R \in \mathbb{K}[X]$ avec $\deg R < d$, tel que $A - PB = Q_1 B + R$, donc $A = (Q_1 + P)B + R$.
et ainsi avec $Q = Q_1 + P$, l'hypothèse $\mathscr{P}_{n+1}$ est vérifiée.
Reste à montrer l'unicité.
Si $A = Q_1 B + R_1 = Q_2 B + R_2$, alors $(Q_1 - Q_2)B = R_2 - R_1$.
Or $\deg((Q_1 - Q_2)B) = \deg(Q_1 - Q_2) + \deg B \geqslant \deg B$, si $Q_1 \neq Q_2$.
Alors que $\deg(R_2 - R_1) < \deg B$.
La seule possibilité : $Q_1 - Q_2 = 0$, donc $Q_1 = Q_2$, puis $R_2 - R_1 = 0$ donc $R_1 = R_2$. □

Remarque - Nécessité d'un corps $\mathbb{K}$
Le rôle du corps est assuré par l'existence de b_d^{-1}. Il faut donc au moins que b_d soit inversible (et par récurrence...) pour faire une division euclidienne de A par B.
Cette démonstration nous conduit au savoir-faire :

Savoir faire - Algorithme de division euclidienne

On remarque que cette démonstration (en tout cas la partie concernant l'existence) donne un algorithme pour obtenir Q puis R.

1. On divise le terme de plus haut degré de A par celui de B
   C'est possible car $\mathbb{K}$ est un corps, cela donne un facteur du type $\frac{a_{\deg(A)}}{b_{\deg(B)}}X^{\deg(A)-\deg(B)}$.
   On peut, par habitude, noter ce nombre sous B (dans un tableau $A|B$)
2. Puis on soustrait à A, toute la multiplication de B par ce facteur.
   On peut, par habitude, écrire cette multiplication sous A, ce qui permet de faire la soustraction aisément
3. On obtient un nouveau terme A_1
4. et on recommence la division, jusqu'à ce que $\deg A_n < \deg B$. On a alors $R = A_n$
   Cela se termine bien car la suite $(\deg(A_k))$ est une suite entière strictement décroissante

Exercice

Effectuer la division euclidienne de $A = X^5 + 2X^4 + 3X^2 + X + 4$ par $B = X^2 + 2X + 2$.

Correction

$X^5 + 2X^4 + 3X^2 + X + 4 = (X^3 - 2X + 7)(X^2 + 2X + 2) + (-9X - 10)$

Pour aller plus loin - Méthode de Hörner-Ruffini

Il existe un algorithme, plus ou moins efficace selon l'habitude qu'on en a, pour faire la division euclidienne de deux polynômes.
Voir wikipedia ou le DS 6 de 2016-2017

Proposition - Divisibilité et division euclidienne

On l'équivalence :

$$B|A \iff R = 0$$

où R est le reste de la division euclidienne de A par B.

Démonstration

Si $R = 0$, alors $A = BQ$ et donc $B|A$.
Réciproquement, par unicité de la division euclidienne, on peut identifier dans $A = BQ + 0$, le quotient à Q et le reste à 0. □

2.3. Nature de $\mathbb{K}[X]$

Finalement,

Proposition - Structure de $\mathbb{K}[X]$

On suppose que $\mathbb{K}$ est un corps.
L'ensemble des multiples de P est un idéal principal de $\mathbb{K}[X]$.
$\mathbb{K}[X]$ est un anneau principal.

Exercice

A demontrer

Correction

On notera également :

Définition - Congruence

Soit $P, Q, T \in \mathbb{K}[X]$.
On dit que P est congru à Q modulo T, noté $P \equiv Q[T]$
si $P - Q$ est un multiple de T i.e. $P - Q \in T\mathbb{K}[X]$
ou encore $P = Q + K \times T$ avec $K \in \mathbb{K}[X]$.

Exercice

Montrer que $P \equiv Q[T] \iff P\%T = Q\%T$.

Correction

Il existe $S_1, S_2 \in \mathbb{K}[X]$ tel que $P = TS_1 + (P\%T)$ et $Q = TS_2 + (P\%T)$.
Donc $P - Q = T(S_1 - S_2) + (P\%T - Q\%T)$. Pour des raisons de degré : c'est la division euclidienne de $P - Q$ par T.
On a d'après un théorème précédent :

$$P \equiv Q[T] \Leftrightarrow T \text{ divise } P - Q \Leftrightarrow (P\%T - Q\%T) = 0 \Leftrightarrow P\%T = Q\%T$$

3. Plus Grand Commun Diviseur

3.1. Heuristique

On note momentanément $\mathscr{D}(A)$ l'ensemble des diviseurs de $A \in \mathbb{K}[X]$.

Heuristique - PGCD

Soient A et B deux éléments de $\mathbb{K}[X]$ non nuls. $\mathscr{D}(A) \cap \mathscr{D}(B)$ est une partie non vide (contient 1) de $\mathbb{K}[X]$ dont les éléments sont de degré $\leqslant \max(\deg A, \deg B)$ donc $\{\deg P; P \in \mathscr{D}(A) \cap \mathscr{D}(B)\} (\subset \mathbb{N})$ admet un plus grand élément d.
Tout élément de $\mathscr{D}(A) \cap \mathscr{D}(B)$ de degré d est appelé un *PGCD* (Plus Grand Commun Diviseur) de A et B.
On parlera parfois de « le » PGCD de A et de B, pour désigner le polynôme unitaire de $\mathscr{D}(A) \cap \mathscr{D}(B)$ de degré d. Les autres PGCD lui sont associés.

Ce n'est pas la définition que nous choisirons. Nous reprendrons la caractéristique, plus pratique, vue en arithmétique entière.

3.2. Algorithme d'Euclide et coefficients de Bézout

Lemme - Stabilité des diviseurs et algorithme d'Euclide

Soit $(A, B) \in \mathbb{K}[X]^2$. Si $A = BQ + R$, alors $\mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(B) \cap \mathscr{D}(R)$.

Pour aller plus loin - Anneau euclidien

Un autre exemple d'anneau euclidien (muni d'une division euclidienne) : $\mathbb{Z}[i]$, l'anneau des entiers de Gauss.

Démonstration

On a vu : $P|A$ et $P|B$ ssi $P|B$ et $P|A + B$, on exploite ce résultat.
Soit $P \in \mathscr{D}(A) \cap \mathscr{D}(B)$.
P divise B, donc $P \in \mathscr{D}(B)$.
Puis $A = PA_1$, $B = PB_1$, donc $R = A - BQ = P(A_1 - B_1Q)$,
donc P divise R et $P \in \mathscr{D}(R)$.
Ainsi $P \in \mathscr{D}(B) \cap \mathscr{D}(R)$.
Réciproquement, si $P \in \mathscr{D}(B) \cap \mathscr{D}(R)$.
P divise B, donc $P \in \mathscr{D}(B)$.
Puis $R = PR_1$, $B = PB_1$, donc $A = BQ + R = P(B_1Q + R_1)$,
donc P divise A et $P \in \mathscr{D}(A)$.
Ainsi $P \in \mathscr{D}(A) \cap \mathscr{D}(B)$. □

Définition - Algorithme d'Euclide

On pratique l'algorithme d'Euclide pour les polynômes A et B.
— On commence par poser $R_0 = A$ et $R_1 = B$;
— ensuite, k désignant un entier naturel non nul, tant que $R_{k+1} \neq 0$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1} (on a donc $\deg R_{k+2} < \deg R_{k+1}$).
Comme il n'existe qu'un nombre fini d'entiers naturels entre 0 et $\deg R_0$, il existe $N \in \mathbb{N}^*$ tel que $R_N = 0$.
$\mathscr{D}(R_{N-1}) = \mathscr{D}(A) \cap \mathscr{D}(B)$.

Démonstration
Il existe $N \in \mathbb{N}^*$ tel que $R_N = 0$.
R_{N-1} est alors le dernier reste non nul et on a donc :
$\mathscr{D}(A)\cap\mathscr{D}(B) = \mathscr{D}(R_0)\cap\mathscr{D}(R_1) = \mathscr{D}(R_1)\cap\mathscr{D}(R_2) = \cdots = \mathscr{D}(R_{N-1})\cap\mathscr{D}(R_N) = \mathscr{D}(R_{N-1})\cap\mathscr{D}(0) = \mathscr{D}(R_{N-1})$
□

Analyse - Suites (U_n) et (V_n)

Avec les mêmes notations, on considère les deux suites de polynômes (U_n) et (V_n) définies par la même relation de récurrence :

$$\forall\ n \in \mathbb{N}, \qquad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

avec pour conditions initiales : $U_0 = 1$, $U_1 = 0$ et $V_0 = 0$, $V_1 = 1$.
On a donc $R_0 = A = 1A + 0B = U_0A + V_0B$ et $R_1 = B = 0A + 1B = U_1A + V_1B$.
Puis pour tout $n \in \mathbb{N}$:

$$\begin{aligned} R_{n+2} &= R_n - Q_{n+1}R_{n+1} = (U_nA + V_nB) - Q_{n+1}(U_{n+1}A + V_{n+1}B) \\ &= (U_n - Q_{n+1}U_{n+1})A + (V_n - Q_{n+1}V_{n+1})B \end{aligned}$$

Donc par récurrence, on peut affirmer

Théorème - Couple de Bézout
A partir de l'algorithme d'Euclide, en considérant les suites (U_n) et (V_n) définies par $U_0 = 1$, $U_1 = 0$ et $V_0 = 0$, $V_1 = 1$ et

$$\forall\ n \in \mathbb{N}, \qquad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

On a

$$\forall\ n \in \mathbb{N}, \qquad R_n = U_nA + V_nB$$

En particulier, il existe $U, V \in \mathbb{K}[X]$ tel que $R_{N-1} = UA + VB$

Truc & Astuce pour le calcul - Suites (U_n) et (V_n)

Avec les mêmes notations, on a finalement les deux suites de polynômes (U_n) et (V_n) définies par la même relation de récurrence :

$$\forall\ n \in \mathbb{N}, \qquad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

avec pour conditions initiales : $U_0 = 1$, $U_1 = 0$ et $V_0 = 0$, $V_1 = 1$.
Comme pour le cours d'arithmétique de $\mathbb{Z}$, on peut faire le calcul au fur et à mesure dans un tableau.
Alors, pour tout $n \in \mathbb{N}$, $R_n = U_n \times A + V_n \times B$

Exercice
Pour tout $n \in \mathbb{N}_{N-1}$ que vaut $U_nV_{n+1} - V_nU_{n+1}$?

Correction
On note $A_n = U_nV_{n+1} - V_nU_{n+1}$.
$A_{n+1} = U_{n+1}V_{n+2} - V_{n+1}U_{n+2} = U_{n+1}V_n - Q_{n+1}U_{n+1}V_{n+1} - V_{n+1}U_n + Q_{n+1}U_{n+1}V_{n+1} = -A_n$
Et $A_0 = U_0V_1 - V_0U_1 = 1 \times 1 - 0 \times 0 = 1$ (A_n) est une suite géométrique, de raison (-1), de premier terme 1
et donc $U_nV_{n+1} - V_nU_{n+1} = (-1)^n$.
On en déduira avec le théorème de Bézout que pour tout n, U_n et V_n sont toujours premiers.

3.3. PGCD

Définition - PGCD et couple de Bézout
Soit $(A, B) \in \mathbb{K}[X]^2$, A, B non nuls. Il existe un polynôme D dont les diviseurs sont exactement les diviseurs communs à A et B, c'est-à-dire tel que

$$\forall P \in \mathbb{K}[X], (P|A \text{ et } P|B) \iff P|D.$$

D est un $PGCD$ de A et B et deux polynômes D_1 et D_2 vérifiant ces

hypothèses sont associés.
L'unique polynôme D unitaire vérifiant ces hypothèses est noté $A \wedge B$ (on dit aussi que c'est **le** PGCD de A et B).

Remarque - Relation d'équivalence

$\mathscr{R} : A\mathscr{R}B$ ssi A et B sont PGCD de deux polynômes identiques.
En fait, il s'agit d'une relation d'équivalence, la même que : $\mathscr{R}'$: $A\mathscr{R}'B$ ssi $\exists\ \lambda \in \mathbb{K}$ tel que $A = \lambda B$.
Les classes d'équivalences ont toutes un représentant naturel : un polynôme unitaire.
Avec cette définition, il faut montrer l'existence. La proposition suivante nous donne un exemple.

Proposition - Un PGCD
Le dernier reste non nul obtenu avec l'algorithme d'Euclide est un PGCD de A et B.

Démonstration
On a vu que R_{N-1} est un diviseur de A et B.
Donc si $P|R_{N-1}$, alors $P|A$ et $P|B$.
Et si $P|A$ et $P|B$, alors $P|UA + BV = R_{N-1}$.
On a donc l'équivalence caractéristique et R_{N-1} est un PGCD de A et B. □

Comme $A \wedge B = \lambda R_{N-1}$:

Corollaire - Couple de Bézout
Il existe des polynômes U et V tels que $AU + BV = A \wedge B$.
(U, V) est un couple de Bézout de A et B.

Corollaire - Autre expression du PGCD
D est un PGCD de A et B si et seulement si

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$$

Démonstration
Si D est un PGCD, alors $D = \lambda R_{N-1}$.
Si $P \in A\mathbb{K}[X] + B\mathbb{K}[X]$, alors $\exists\ W, Z \in \mathbb{K}[X]$ tel que $P = WA + ZB$.
Et donc $P = R_{N-1}(WA' + ZB')$ avec $A = A'R_{N-1}$ et $B = B'R_{N-1}$
Et ainsi $P = D\left(\frac{1}{\lambda}(WA' + ZB')\right)$, donc $P \in D\mathbb{K}[X]$
$A\mathbb{K}[X] + B\mathbb{K}[X] \subset D\mathbb{K}[X]$.
Et si $P \in D\mathbb{K}[X] = R_{N-1}\mathbb{K}[X]$, alors $P = (UA + VB)R = URA + VRB$.
Et ainsi $D\mathbb{K}[X] \subset A\mathbb{K}[X] + B\mathbb{K}[X]$.
Réciproquement supposons que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.
On a alors $D \in A\mathbb{K}[X] + B\mathbb{K}[X]$, donc il existe W, Z tels que $D = WA + ZB$.
Et donc si $P|A$ et $P|B$, alors $P|WA + ZB = D$.
On a également $1A + 0B \in D\mathbb{K}[X]$ et donc $D|A$.
Et si $P|D$, alors $P|A$ par transitivité et de même $P|B$. □

Remarque - Elargissement de la définition

On élargit :
- On pose $A \wedge 0 = A$
- Il n'y a pas unicité du couple (U, V) puisque si (U_0, V_0) est un couple de Bezout, alors pour tout $Q \in \mathbb{K}[X]$, $(U_0 + QB, V_0 - QA)$ en est aussi un.
- En pratique, comme avec les entiers, on trouve (U, V) en utilisant l'algorithme d'Euclide et en éliminant les restes successifs.

Exercice
Déterminer $PGCD(A, B)$ ainsi qu'un couple de Bezout lorsque $A = X^3 + X^2 + 2$ et $B = X^2 + 1$.

Correction
On applique donc l'algorithme d'Euclide (division euclidienne successive) :

— $A=(X+1)B+(-X+1)$
— $(X^2+1)=(-X-1)(-X+1)+2$

Donc $2=(X^2+1)-(-X-1)(-X+1)=B+(X+1)(A-(X+1)B)=(X+1)A-(X^2+2X)B$ En divisant par 2 : $A\wedge B=1$ et $(U,V)=(\frac{1}{2}(X+1),\frac{-1}{2}(X^2+2X))$

Le théorème énonce beaucoup de choses, à démontrer…

Définition - Polynômes premiers entre eux
A et B sont dits premiers entre eux si $A\wedge B=1$.

Théorème - Théorème de Bezout
Soient A et B deux polynômes non nuls. Alors

$$A\wedge B=1\Longleftrightarrow\exists(U,V)\in\mathbb{K}[X]^2 \text{ tel que } AU+BV=1.$$

Démonstration
D'après ce qui précède, si $A\wedge B=1$ alors $\exists(U,V)\in\mathbb{K}[X]^2$ tel que $AU+BV=1$
Réciproquement si $AU+BV=1$ alors pour $D\in\mathbb{K}[X]$, $D|A$ et $D|B\Rightarrow D|AU+BV=1$ donc $D\in\mathbb{K}$ et $A\wedge B=1$. □

Exercice
Sans effectuer la division euclidienne, trouver un couple de Bézout pour les polynômes $(1-X)^5$ et $(1+X)^4$.

Correction
$(1+X)+(1-X)=2$, donc $(1+X)\wedge(1-X)=1$. Puis $(8=(5-1)+(4-1)+1)$:

$$2^8=\big((1-X)+(1+X)\big)^8=(1+X)^5\left(\sum_{k=0}^{3}\binom{8}{k}(1-X)^k(1+X)^{3-k}\right)+(1-X)^4\left(\sum_{k=0}^{4}\binom{8}{k}(1+X)^k(1-X)^{4-k}\right)$$

3.4. Lemme de Gauss et facteurs relativement premiers

Théorème - Lemme de Gauss
Soient A,B,C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A\wedge B=1 \text{ et } A|BC)\Rightarrow A|C.$$

Démonstration
Si $A\wedge B=1$ alors $\exists(U,V)\in\mathbb{K}[X]^2$ tel que $AU+BV=1$ d'où $ACU+BCV=C$ et $A|BC\Rightarrow A|BCV\Rightarrow A|C-ACU$.
Or $A|ACU$ d'où $A|C=(C-ACU)+ACU$. □

Proposition - Facteurs relativement premiers
Soient A,B,C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A\wedge B=1 \text{ et } A\wedge C=1)\Rightarrow A\wedge BC=1 \text{ (réciproque vraie)}$$

$$(A\wedge B=1,\ A|C,\ B|C)\Rightarrow AB|C$$

Démonstration
D'après l'identité de Bézout il existe U_1,V_1,U_2,V_2 tels que $AU_1+BV_1=1$ et $AU_2+CV_2=1$,
d'où par produit $A(U_1(AU_2+CV_2))+A(BU_2V_1)+BCV_1V_2=1$,
ce qui peut s'écrire $AU+BCV=1$ avec $(U,V)\in\mathbb{K}[X]^2$, et par Bézout $A\wedge BC=1$.
Pour la seconde implication : $A|C$ donc $C=AQ$; $B|C=AQ$ et $B\wedge A=1$ donc $B|Q$;
$Q=BP$ et $C=ABP$ d'où $AB|C$. □

Corollaire - Bézout avec degré minimal
Soient A,B deux polynômes non constants, premiers entre eux.
Alors il existe un unique couple (U_0,V_0) tel que $AU_0+BV_0=1$ avec $\deg U_0<\deg B$, $\deg V_0<\deg A$.
On a alors $U=U_0+QB$ et $V=V_0-QA$ avec $Q\in\mathbb{K}[X]$

Pour aller plus loin - Résultant
Il existe un objet : le résultant de deux polynômes qui permet de calculer directement (avec un déterminant matriciel) si ces deux polynômes ont un facteur commun. Bien exploiter, on peut aussi en déduire une décomposition de Bézout.

Démonstration
Supposons que $AU+BV=1$.
Pour tout $Q\in\mathbb{K}[X]$, $A(U-BQ)+B(V+AQ)=AU-ABQ+BV+ABQ=1$.
Prenons donc U_0, reste de la division euclidienne de U par B. On a donc $\deg U_0<\deg B$.
Avec Q, la quotient de la division euclidienne : $U=QB+U_0$, donc $U_0=U-QB$.
Notons alors $V_0=V+AQ$, on a donc $AU_0+BV_0=1$, $\deg U_0<\deg B$.
Donc $\deg(AU_0)<\deg A+\deg B$, et donc $\deg(BV_0)<\deg B+\deg A$, ce qui nécessite : $\deg V_0<\deg A$. □

Par récurrence de la proposition : produit des polynômes premiers entre eux :

Corollaire - Facteurs premiers
Soient $A,C,B_1,\dots,B_n$ des polynômes.

$$(\forall i\in[\![1,n]\!],A\wedge B_i=1)\Rightarrow A\wedge\prod_{i=1}^{n}B_i=1$$

$$(\forall(i,j)\in[\![1,n]\!]^2,i\neq j\Rightarrow B_i\wedge B_j=1 \text{ et } \forall i\in[\![1,n]\!],B_i|C)\Rightarrow\prod_{i=1}^{n}B_i\Big|C$$

3.5. Interprétation avec racines

Proposition - Factorisation (division)
Soit $P\in\mathbb{K}[X]$. Si $x_1,\dots,x_p$ sont p racines distinctes de P de multiplicités respectives égales à $m_1,\dots,m_p$, alors $\prod_{i=1}^{p}(X-x_i)^{m_i}$ divise P.

Démonstration
Les polynômes $(X-x_i)^{m_i}$ sont premiers entre eux deux à deux.
En effet, si $T|(X-x_i)^{m_i}$, alors $T=(X-x_i)^{n_i}$ avec $n_i\leqslant m_i$.
Et donc si $T|(X-x_i)^{m_i}$ et $T|(X-x_j)^{m_j}$, alors $T=1$.
Enfin, d'après le corollaire précédent : comme pour tout i $(X-x_i)^{m_i}|P$, alors $\prod_{i=1}^{p}(X-x_i)^{m_i}$ divise P. □

Corollaire - Nombre maximal de racines
Un polynôme non nul de degré n possède au plus n racines comptées avec leur multiplicité (c'est-à-dire comptées autant de fois que leur multiplicité).

Démonstration
On a nécessairement : $\deg\left(\prod_{i=1}^{p}(X-x_i)^{m_i}\right)=\sum_{i=1}^{p}m_i\leqslant\deg(P)=n$. □

Exercice
Trouver les polynômes $P\in\mathbb{R}_7[X]$ tels que $(X+7)\,P(X)=(X-5)\times P(X+2)$

Correction

$(X-5)$ divise P car $(X-5)$ et $(X+7)$ sont premier entre eux.
Ainsi 5 est une racine de P.
Donc avec $a=3$, on a $(-2)P(5)=0=10P(3)$, donc 3 est racine de P.
On continue, ainsi de suite, et $a=1$, $a=-1$, $a=-3$ et $a=-5$ sont également des racines de P.
Donc $P=(X-5)(X-3)(X-1)(X+1)(X+3)(X+5)Q$ avec $\deg Q=1$.
Dans l'expression initiale :

$$(X+7)P(X)=(X-5)(X-3)(X-1)(X+1)(X+3)(X+5)(X+7)Q(X)=(X-5)(X-3)(X-1)(X+1)(X+3)(X+5)(X+7)Q(X+2)$$

Donc $Q=aX+b$, avec $aX+b=aX+(b+2a)$, donc $a=0$.
Les polynômes P cherché sont les $\lambda(X-5)(X-3)(X-1)(X+1)(X+3)(X+5)$.

3.6. PGCD de plusieurs polynômes

La notion de PGCD peut être étendue à un nombre fini de polynômes :

Proposition - PGCD de plusieurs polynômes
Soient $k\in\mathbb{N}^*$, $k\geqslant 2$, et $(A_1,A_2,\dots,A_k)\in\mathbb{K}[X]^k$. Il existe un unique polynôme nul ou unitaire P dont les diviseurs sont exactement les diviseurs communs à tous les A_i, c'est-à-dire tel que

$$\forall T\in\mathbb{K}[X],(\forall i\in[\![1,k]\!],\ T|A_i)\Leftrightarrow T|P$$

En fait, on a $\mathscr{D}(P)=\bigcap_{i=1}^{k}\mathscr{D}(A_i)$.
On l'appelle PGCD de $A_1,A_2,\dots,A_k$ et on le note $A_1\wedge A_2\wedge\dots\wedge A_k$ ou $\bigwedge_{i=1}^{k}A_i$.
On a de plus l'identité de Bézout :

$$\exists(U_1,\dots,U_k)\in\mathbb{K}[X]^k\,|\,P=\sum_{i=1}^{k}U_iA_i.$$

Encore : $A_1\mathbb{K}[X]+A_2\mathbb{K}[X]+\dots+A_k\mathbb{K}[X]$ est l'idéal engendré $P\mathbb{K}[X]$.

Démonstration
On note $\mathscr{A}=\{\sum_{i=1}^{k}U_iA_i,U_i\in\mathbb{K}[X]\}$. Donc pour tout $i\in\mathbb{N}_k$, $A_i\in\mathscr{A}$.
On note $\mathscr{D}_{\mathscr{A}}=\{\deg P,P\in\mathscr{A},P\neq 0\}$.
$\deg(A_1)\in\mathscr{D}_{\mathscr{A}}$, donc $\mathscr{D}_{\mathscr{A}}$ est non vide, inclus dans $\mathbb{N}$.
Il admet un plus petit élément d et il existe $P\in\mathscr{A}$ tel que $d=\deg P$.
Quitte à le diviser par son coefficient dominant, on peut supposer que P est unitaire. On va démontrer que $\mathscr{A}=P\mathbb{K}[X]$.
On a $P\in\mathscr{A}$, puis clairement $P\mathbb{K}[X]\subset\mathscr{A}$ (qui est un idéal).
Réciproquement, soit $B\in\mathscr{A}$.
On pratique la division euclidienne de B par P : $B=QP+R$, donc $R=B-QP\in\mathscr{A}$.
Or $\deg R<\deg P$, donc nécessairement $R=0$, sinon on aurait une contradiction. Et P divise B. Ainsi, $\mathscr{A}=\{\sum_{i=1}^{k}U_iA_i,U_i\in\mathbb{K}[X]\}=P\mathbb{K}[X]$.
Il est donc clair qu'il existe $U_1,\dots U_k$ tels que $P=\sum_{i=1}^{k}U_iA_i$.
Montrons que P vérifie la propriété de divisibilité.
Si, pour tout $i\in\mathbb{N}_k$, $T|A_i$, alors $T|\sum_{i=1}^{k}U_iA_i=P$.
Réciproquement, comme $A_i\in\mathscr{A}$, $P|A_i$ et par transitivité : $T|P|A_i$.
Enfin, montrons l'unicité de P.
Si P_1 vérifie la même propriété alors, comme $P|P$, $P|A_i$ pour tout i; et donc $P|P_1$.
Et de même $P_1|P$. Donc P et P_1 sont associés.
Tous les deux sont unitaires, donc $P=P_1$. □

La proposition suivante permet de justifier la notation associative $\bigwedge_{i=1}^{k}A_i$

Proposition - PGCD par récurrence
Soient $k\in\mathbb{N}^*$, $k\geqslant 2$, et $(A_1,A_2,\dots,A_k)\in\mathbb{K}[X]^k$.
$\bigwedge_{i=1}^{k}A_i=\left(\bigwedge_{i=1}^{k-1}A_i\right)\wedge A_k$

Démonstration
Comme pour les entiers, nous faisons une récurrence sur k.
Notons, pour tout $k\in\mathbb{N}^*$, $k\geqslant 2$:
$\mathscr{P}_k$: « Pour $(A_1,A_2,\dots,A_k)\in(\mathbb{K}[X])^k$, $\exists\,(U_1,\dots,U_k)\in(\mathbb{K}[X])^k\mid\bigwedge_{i=1}^{k}A_i=\sum_{i=1}^{k}U_iA_i$. »
— $\mathscr{P}_2$ est vraie. C'est le théorème de Bézout vu plus haut.
— Soit $k\in\mathbb{N}$, $k\geqslant 2$. Supposons que $\mathscr{P}_k$ est vraie.
Soient $(A_1,A_2,\dots,A_k,A_{k+1})\in\mathbb{Z}^k$.
Notons $\Delta_1=\bigwedge_{i=1}^{k}A_i$ et $\Delta=\bigwedge_{i=1}^{k+1}A_i$.
On a les équivalence, pour tout entier $P\in\mathbb{K}[X]$:

$$P|\Delta_1\text{ et }P|A_{k+1}\Longleftrightarrow\forall\,i\in[\![1,k+1]\!]P|A_i\Longleftrightarrow P|\Delta$$

Donc $\Delta=\Delta_1\wedge A_{k+1}$ (et existe bien…).
D'après l'identité de Bézout, il existe $U,V\in\mathbb{K}[X]$ tel que $\Delta=U\Delta_1+VA_{k+1}$.
Puis on applique $\mathscr{P}_k$, à $(A_1,A_2,\dots,A_k)$: $\Delta_1=U_1A_1+\dots+U_kA_k$.
Finalement $\Delta=\sum_{i=1}^{k+1}U'_iA_i$, avec $U'_{k+1}=V$ et $U'_j=U_j\times U$ pour $j\leqslant k$.
Donc $\mathscr{P}_{n+1}$ est vraie.
Notons qu'on aurait pu commencer à $k=1$, mais le résultat obtenu n'a pas d'intérêt □

Définition - Polynômes premiers entre eux (dans leur ensemble)
Les polynômes $A_1,\dots,A_k$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD vaut 1.

Attention - Polynômes premiers entre eux
Une famille de polynômes premiers entre eux deux à deux est une famille de polynômes premiers entre eux dans leur ensemble.
La réciproque est fausse.
On peut le démontrer avec une décomposition de Bézout

Proposition - Théorème de Bézout
Soient $A_1,\dots,A_k$ des polynômes. Alors

$$\bigwedge_{i=1}^{k}A_i=1\Leftrightarrow\exists(U_1,\dots,U_k)\in\mathbb{K}[X]^k\mid\sum_{i=1}^{k}U_iA_i=1$$

Démonstration
Cela découle de la proposition précédente.
Si $\bigwedge_{i=1}^{k}A_i=1$, alors il existe $(U_1,\dots,U_k)\in\mathbb{K}[X]^k\mid\sum_{i=1}^{k}U_iA_i=1$.
Réciproquement, si il existe $(U_1,\dots,U_k)\in\mathbb{K}[X]^k\mid\sum_{i=1}^{k}U_iA_i=1$
Alors si $\Delta=\bigwedge_{i=1}^{k}A_i$, il divise A_i, pour tout i et donc $\sum_{i=1}^{k}U_iA_i=1$.
Donc $\Delta=1$ □

4. Plus Petit Commun Multiple

4.1. Caractérisation essentielle

Pour aller plus loin - UN/LE PPCM
On devrait parler d'UN PPCM si il s'agit d'un polynôme associé à LE PPCM

Heuristique - PPCM
Soient A et B deux polynômes non nuls.
L'ensemble des multiples communs à A et B est non vide (contient AB) donc l'ensemble des degrés des multiples communs à A et B et non nul, est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément.

Un multiple de A et B de plus petit degré est appelé un $PPCM$ (Plus Petit Commun Multiple) de A et B.

Définition - Caractérisation essentielle du PPCM
Soit $(A,B)\in\mathbb{K}[X]^2$. Il existe un unique polynôme M nul ou unitaire dont les multiples sont exactement les multiples communs à A et B, c'est-à-dire tel que

$$\forall P\in\mathbb{K}[X],\ (A|P \text{ et } B|P)\Leftrightarrow M|P$$

M est appelé **le** $PPCM$ de A et B, noté $A\vee B$.

Démonstration
Soit M, un PPCM de A et de B. Donc $A=MA_1$, $B=MB_1$.
Alors si P est tel que $A|P$ et $B|P$ on a P multiple commun à A et B, donc $\deg(P)\geqslant\deg(M)$.
Faisons la division euclidienne de P par M : $P=MQ+R$ avec $\deg(R)<\deg(M)$.
Or $A|P$, $A|MQ$, donc $A|R=P-MQ$ et de même $B|R$.
Donc R est un multiple de A et de B, mais son degré est plus petit que celui de M.
Par définition de M cela impose $R=0$ et donc M divise P.
Donc les PPCM vérifie la condition : $\forall P\in\mathbb{K}[X]$, $(A|P \text{ et } B|P)\Leftrightarrow M|P$.
Il existe donc bien (au moins) un polynôme qui vérifie la condition.
Supposons qu'il en existe un second : M_1.
Alors comme $A|M$ et $B|M$, on a donc $M_1|M$. Et réciproquement (vu plus haut).
Ainsi, M et M_1 sont associés, et il existe un unique polynôme unitaire vérifiant la condition.
□

Une autre caractérisation essentielle

Corollaire - Autre caractérisation
M est un PPCM de A et B si et seulement si

$$A\mathbb{K}[X]\cap B\mathbb{K}[X]=M\mathbb{K}[X]$$

Démonstration
$P\in A\mathbb{K}[X]\cap B\mathbb{K}[X]\Longleftrightarrow A|P$ et $B|P$.
$P\in M\mathbb{K}[X]\Longleftrightarrow M|P$ Donc
$\big[A|P \text{ et } B|P\Leftrightarrow M|P\big]\Longleftrightarrow\big[P\in A\mathbb{K}[X]\cap B\mathbb{K}[X]\Leftrightarrow P\in M\mathbb{K}[X]\big]$ □

4.2. Relation PGCD/PPCM

Proposition - Relation PGCD et PPCM
Soient $A,B\in\mathbb{K}[X]$ non nuls.
— si $A\wedge B=1$ alors $\exists\lambda\in\mathbb{K}^*\mid AB=\lambda(A\vee B)$.
— dans le cas général, $\exists\lambda\in\mathbb{K}^*\mid AB=\lambda(A\wedge B)\times(A\vee B)$.

Démonstration
Soit P tel que $A|P$ et $B|P$.
Comme $A\wedge B=1$, d'après un corollaire de Gauss : $AB|P$.
Réciproquement, si $AB|P$, alors $A|P$ et $B|P$.
Donc AB est un PPCM de A et B.
Ainsi $A\vee B$ et AB sont associés.
Dans le cas général : $A=(A\wedge B)A'$ et $B=(A\wedge B)B'$
on applique à A' et B', le résultat précédent :
il existe λ tel que $A'B'=\lambda(A'\vee B')$.
On multiplie par $(A\wedge B)^2$:

$$AB=(A\wedge B)A'(A\wedge B)B'=\lambda(A\wedge B)^2(A'\vee B')$$

$$=\lambda(A\wedge B)\times[(A\wedge B)A']\vee[(A\wedge B)B'])=\lambda(A\wedge B)(A\vee B)$$

On a exploité $(QA)\vee(QB)=Q(A\vee B)$.
En effet : $A|P$ et $B|P$ ssi $QA|QP$ et $QB|QP$ □

Pour aller plus loin - Un lien avec les ensembles
Quel est le lien entre cette formule est la suivante?
$card A+card B=card(A\cup B)+card(A\cap B)$.

Heuristique - Décomposition
On peut retenir que si $A=(A\wedge B)A'$, et $B=(A\wedge B)B'$,
alors A' et B' sont premiers entre eux,
et alors $\lambda A\vee B=(A\wedge B)A'B'$.
Et donc : $A\times B=(A\wedge B)A'\times(A\wedge B)B'=(A\wedge B)\times(A\wedge B)A'B'=\lambda(A\wedge B)\times(A\vee B)$

Exercice
Déterminer le PGCD, le PPCM et un couple de Bezout lorsque $A=X^3+3X^2+3X+2$ et $B=X^5+3X^4+2X^3-2X^2-3X+2$.

Correction
On applique l'algorithme d'Euclide :

$$B=X^5+3X^4+2X^3-2X^2-3X+2=(X^2-1)A+(-X^2+4)$$

$$A=X^3+3X^2+3X+2=(-X-3)(-X^2+4)+(7X+14)$$

$$-X^2+4=(-\tfrac{1}{7}X+\tfrac{2}{7})(7X+14)+0$$

Donc $A\wedge B=X+2$ (on prend le dernier reste non nul, unitaire).
Puis comme $A\vee B\times A\wedge B=A\times B=X^9+4X^8+8X^7+11X^6+9X^5+3X^4-7X^3-4X^2-2X+4$.
$A\vee B=(X^7+4X^6+6X^5+3X^4-3X^3-3X^2-X+2)$
(On pour ne pas avoir de trop gros polynôme, on peut voir que :

$$A=(X+2)(X^2+X+1)\qquad B=(X+2)(X^4+X^3-2X+1)$$

$$A\vee B=(X+2)(X^2+X+1)(X^4+X^3-2X+1)=(X^7+4X^6+6X^5+3X^4-3X^3-3X^2-X+2)$$

Enfin un couple de Bézout est $U=\frac{-1}{7}(X^3+3X^2-X-4)$ et $B=\frac{1}{7}(X+3)$ car

$$7X+14=(X+3)B-[(X+3)(X^2-1)-1]A$$

(on peut vérifier)

5. Polynômes irréductibles

5.1. Décomposition unique en produit d'irréductibles

Les polynômes irréductibles jouent ici le même rôle que les nombres premiers dans $\mathbb{Z}$. Les polynômes inversibles sont les polynômes de degré 0 :

Définition - Polynômes irréductibles
$P\in\mathbb{K}[X]$ est dit irréductible si

$$(P=AB,\ A,B\in\mathbb{K}[X])\Rightarrow\deg A=0 \text{ ou } \deg B=0$$

Proposition - Polynôme (de degré 1) irréductible
Quel que soit le corps $\mathbb{K}$ et $\alpha\in\mathbb{K}$, le polynôme $X-\alpha$ est irréductible sur $\mathbb{K}$.

Pour aller plus loin - Polynômes premiers
On dit que p est premier s'il n'est divisible que par 1 et lui-même.
Ici, cette définition ne colle pas bien.
En fait, on a p est premier si $p=ab\Rightarrow a$ ou $b\in\{-1,1\}$.
Et plus généralement : p est premier si $p=ab\Rightarrow a$ ou b inversible

Démonstration
Si $P=AB$ de degré 1, alors $\deg(A)+\deg B=1$ et donc au moins l'un est constant □

Proposition - Polynômes irréductibles et polynômes premiers entre eux
Un polynôme irréductible est premier avec tous les polynômes qu'il ne divise pas.
Un polynôme irréductible divise un produit si et seulement si il divise l'un des facteurs.

Démonstration
Soit P un polynôme irréductible.
Soit A un autre polynôme. Notons $\Delta = P \wedge A$.
Alors $P = \Delta P'$, et donc :
- $\deg\Delta = 0$ et A et P sont premiers
- ou $\deg P' = 0$ et donc $\deg\Delta = \deg P$ et donc $\Delta = \lambda P$.
  Dans ce cas $P|A$.

Soit P un polynôme irréductible. Supposons que $P|P_1 \times P_2$.
Notons $A = P \wedge P_1$, on a donc $P = AP'$ et $P_1 = AP'_1$ avec $P' \wedge P'_1 = 1$.
Et donc $AP'|AP'_1P_2$ et ainsi $P'|P'_1P_2$.
Et alors, d'après le lemme de Gauss : $P'|P_2$, car $P' \wedge P'_1 = 1$.
On a donc $P = AP'$, avec $A|P_1$ et $P'|P_2$. Mais P est irréductible, donc
- $\deg A = 0$ et P' est associé à P et donc P divise P_2
- ou $\deg P' = 0$ et A est associé à P et donc P divise P_1

□

Théorème - Décomposition en produit de facteurs polynomiaux irréductibles
Tout polynôme non constant de $\mathbb{K}[X]$ est le produit d'un scalaire (élément de $\mathbb{K}$) par un produit de polynômes irréductibles unitaires de $\mathbb{K}[X]$.
Cette décomposition est unique à l'ordre des facteurs près.

Démonstration
On démontre d'abord l'existence (récurrence) de la décomposition puis son unicité.
- Posons, pour tout $n \in \mathbb{N}^*$, $\mathscr{H}_n$:« tout polynôme de degré inférieur à n admet une telle décomposition. »
  - $\mathscr{H}_1$ est vraie car $(X-a)$ est irréductible.
  - supposons $\mathscr{H}_n$ vraie pour un certain $n \in \mathbb{N}^*$.
    Soit P un polynôme de degré $n+1$.
    - Si P est irréductible, il suffit de diviser par son coefficient dominant
    - Si P n'est pas irréductible, il existe A et B de degré supérieur ou égal à 1 (chacun),
      tels que $P = A \times B$. Donc $\deg A \leqslant n+1-1 = n$ et $\deg B \leqslant n+1-1 = n$.
      Et on applique $\mathscr{H}_n$ à A et à B.

    La récurrence est démontre, l'existence est assurée.
- Si
$$P = \prod_{i=1}^{r} P_i^{\alpha_i} = \prod_{j=1}^{s} Q_j^{\beta_j}$$
, chacun des P_i et Q_j est irréductible. Alors pour tout i $P_i|P$ d'où il existe j tel que $P_i|Q_j$ (P_i irréductible) soit $P_i = Q_j$ (Q_j irréductible),
  donc en fait on a les mêmes nombres premiers dans les deux décompositions.
  Reste à prouver que les puissances sont les mêmes.
  Supposons pour un i que l'on ait alors $\alpha_i > \beta_i$, en simplifiant par $P_i^{\beta_i}$ on a
$$P_i^{\alpha_i-\beta_i} \prod_{k\neq i} P_k^{\alpha_k} = \prod_{k\neq i} P_k^{\beta_k}$$
  d'où $P_i | \prod_{k\neq i} P_k^{\beta_k}$ ce qui est absurde car P_i irreductible et $P_i \wedge P_k = 1$ pour $k \neq i$. D'où $\alpha_i = \beta_i$.

□

Proposition - Critère de divisibilité par polynômes irréductibles
Soient $A, B \in \mathbb{K}[X]$ non nuls. Si
$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k} \text{ et } B = \mu P_1^{\beta_1} P_2^{\beta_2} \dots P_k^{\beta_k}$$
où les P_i sont irréductibles unitaires distincts deux à deux, $\alpha_i, \beta_i \in \mathbb{N}$ (éventuellement nuls), alors
$$A|B \Leftrightarrow \forall i \in [\![1,k]\!],\ \alpha_i \leqslant \beta_i$$
$$A \wedge B = \prod_{i=1}^{k} P_i^{\min(\alpha_i,\beta_i)}$$

$$A \vee B = \prod_{i=1}^{k} P_i^{\max(\alpha_i,\beta_i)}$$

Démonstration
Si A divise B, alors $P_i^{\alpha_i}$ divise B et donc $\alpha_i \leqslant \beta_i$.

La réciproque est trivial, avec $C = P_1^{\beta_1-\alpha_1} P_2^{\beta_2-\alpha_2} \dots P_k^{\beta_k-\alpha_k}$, on a $A \times C = B$ Supposons que $D|A$, et $D|B$,
alors $D = P_1^{\delta_1} P_2^{\delta_2} \dots P_k^{\delta_k}$, avec $\delta_k \leqslant \alpha_k$.
de même $\delta_k \leqslant \beta_k$. Donc $\delta_k \leqslant \min(\alpha_k, \beta_k)$.
C'est le cas pour $D = a \wedge b$.
Par ailleurs : $\prod_{i=1}^{k} P_i^{\min(\alpha_i,\beta_i)}$ divise A et B, donc divise $a \wedge b$.

On peut donc assimiler : $A \wedge B = \prod_{i=1}^{k} P_i^{\min(\alpha_i,\beta_i)}$ La démonstration pour le PPCM est laissé en exercice.
On peut exploiter $A \wedge B \times A \vee B = A \times B$ et $\min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i) = \alpha_i + \beta_i$ □

5.2. Décomposition dans $\mathbb{C}[X]$

Rappel :

Théorème - Théorème de d'Alembert-Gauss
Soit $P \in \mathbb{C}[X]$, $\deg P \geqslant 1$. Alors P possède au moins une racine dans $\mathbb{C}$.

Corollaire - Décomposition dans $\mathbb{C}$
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration
Soit P irréductibles de $\mathbb{C}$ de degré supérieur à 1.
Il admet au moins une racine α et est donc divisible par $X-\alpha$.
Et donc $P = (X-\alpha)Q$, or P est irreducible, donc $\deg Q = 0$.
Et finalement, P est de degré 1. □

Théorème - $\mathbb{C}$ est algébriquement clos
Tout polynôme non nul P de $\mathbb{C}[X]$ se décompose de manière unique (à une permutation près) sous la forme
$$P = \lambda \prod_{i=1}^{p} (X - x_i)^{m_i}$$
où les $x_i \in \mathbb{C}$ sont distincts et $\sum_{i=1}^{p} m_i = \deg P$.
Tout polynôme non nul de $\mathbb{C}[X]$ est donc scindé sur $\mathbb{C}$ ($\mathbb{C}$ est dit *algébriquement clos*).

Démonstration
On applique le théorème de décomposition en produit de facteurs polynomiaux irréductibles, et ici (sur $\mathbb{C}$) les facteurs irréductibles sont de degré 1, ce qui donne le théorème. □

Savoir faire - Décomposition en produit d'irréductibles de $\mathbb{C}[X]$
Sur $\mathbb{C}[X]$, les polynômes irréductibles sont de degré 1.
Donc décomposer un polynôme P sur $\mathbb{C}[X]$ en produit d'irréductibles est équivalent à chercher toutes les racines de P, en tenant compte de leur ordre de multiplicité.
En règle générale, on choisit, les facteurs, unitaires et on multiplie le produit par λ, le coefficient dominant de P.

En appliquant le critère de divisibilité par des irréductibles :

Corollaire - Critère de divisibilité dans $\mathbb{C}$
Soient $P,Q \in \mathbb{C}[X]$. Alors $P|Q$ dans $\mathbb{C}[X]$ si et seulement si les racines de P sont des racines de Q avec une multiplicité inférieure dans P.

Exercice
Démontrer à nouveau que $P(X)-X$ divise $P(P(X))-X$.
On commencera par faire l'étude dans $\mathbb{C}$, puis dans $\mathbb{K}$.

Correction
Soit $S = P(X)-X$. S est factorisable sur $\mathbb{C}$ en produit de facteurs de degré 1.
Soit a une racine de S, alors $S(a)=0$, donc $P(a)=a$.
Par conséquent, $P(P(a))=P(a)=a$.
Donc a est également une racine de $T = P(P(X))-X$.
Soit k, la multiplicité de a, comme racine de S.
alors $S'(a)=P'(a)-1=0$, donc $P'(a)=1\ldots$ En outre, $T'(a)=P'(a)\times P'(P(a))-1=1\times P'(a)-1=1-1=0$.
On continue ainsi, et on montre que a est alors aussi racine d'ordre (au moins) k de T.
Donc S divise T, dans $\mathbb{C}[X]$.
Et si $S\in\mathbb{R}[X]$, il en est de même de T. On a vu alors que la divisibilité dans $\mathbb{C}$ entraine celle dans $\mathbb{R}$.

5.3. Décomposition dans $\mathbb{R}[X]$

Comme $\mathbb{R}[X]\subset\mathbb{C}[X]$, on sait qu'un polynôme P de $\mathbb{R}[X]$ tel que $\deg P\geqslant 1$ admet dans $\mathbb{C}$ $\deg P$ racines comptées avec leur multiplicité.

Proposition - Conjugaison des racines
Si $z_0\in\mathbb{C}$ est racine de multiplicité m de $P\in\mathbb{R}[X]$,
alors il en est de même de $\overline{z_0}$.

Démonstration
Soit z_0 une racine de P d'ordre m.
Alors $P=(X-z_0)^m Q$.
Et donc $\overline{P}=\overline{(X-z_0)^m Q}=(X-\overline{z_0})^m\overline{Q}$.
Donc $\overline{z_0}$ est une racine d'ordre au moins m.
Si elle est d'ordre $n>m$, on a de la même façon, z_0 est d'ordre au moins n,
ce qui est faux, donc $n=m$. □

Proposition - Si $\deg P$ est impair
Soit $P\in\mathbb{R}[X]$ tel que $\deg P$ soit impair. Alors P a au moins une racine dans $\mathbb{R}$.

Démonstration
On peut exploiter le TVI…, mais ce n'est pas l'esprit ici.
Faisons un raisonnement par l'absurde. Cela signifie que P n'admet que des racines complexes.
Donc pour toute racine z de P, on a $\mathrm{Im}(z)\neq 0$. Notons z_i et n_i ces racines et leur ordre.
Notons $N=\sum_{i|\mathrm{Im}(z_i)>0} n_i$. Alors $\deg P = 2N$, ce qui est faux.
Donc P admet une racine réelle. □

Proposition - Description des irréductibles de $\mathbb{R}[X]$
Les polynômes irréductibles dans $\mathbb{R}[X]$ sont
— les polynômes de degré 1,
— les polynômes de degré 2 à discriminant strictement négatif.

Démonstration
Si z est une racine de $P\in\mathbb{R}[X]$, alors $\overline{z}$ également.
Donc $(X-z)(X-\overline{z})=X^2-2\mathrm{Re}(z)+|z|^2$ divise P.
Or il s'agit d'un polynôme à coefficient réel.
Donc tout polynôme réel P de degré supérieur strictement à 2 est divisible par un polynôme non constant de degré 1 (racine réelle) ou de degré 2 (racine complexes) (ou les deux!).
Evidemment, les polynômes de degré 1 sont irréductibles.
Enfin, parmi les polynômes de degré 2, sont irréductibles ceux n'admettant pas de racines réelles, donc tels que $\Delta<0$. □

Théorème - Factorisation dans $\mathbb{R}[X]$
Tout polynôme non nul de $\mathbb{R}[X]$ se factorise de manière unique (à une permutation près) sous la forme

$$P=\lambda\prod_i (X-\alpha_i)^{m_i}\prod_j (X^2+b_jX+c_j)^{p_j}$$

où les α_i,b_j,c_j sont des réels, m_i,p_j des entiers tels que

$$\sum_i m_i+2\sum_j p_j=\deg P,\qquad \text{et}\qquad b_j^2-4c_j<0.$$

Démonstration
On applique le théorème de factorisation par des irréductibles.
Ici les irréductibles de $\mathbb{R}[X]$ sont décrits par la proposition précédente.
□

Si la factorisation n'est pas évidente, on peut exploiter le savoir-faire suivant :

Savoir faire - Décomposition en produit d'irréductibles de $\mathbb{R}[X]$
On décompose P sur $\mathbb{C}[X]$.
Si α est racine d'ordre m, alors $\overline{\alpha}$ également.
Le polynôme $(X^2-2\mathrm{Re}(\alpha)X+|\alpha|^2)^m$ divise P et est irréductible sur $\mathbb{R}[X]$.

Exercice
Décomposer $2X^4+2$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Correction
$2X^4+2=2(X^4+1)=2(X+e^{i\pi/4})(X+e^{i3\pi/4})(X+e^{-i\pi/4})(X+e^{-3i\pi/4})$ (racine 4ème de l'unité).
Sur $\mathbb{R}[X]$, $2X^4+2=2(X+e^{i\pi/4})(X+e^{-i\pi/4})(X+e^{i3\pi/4})(X+e^{-3i\pi/4})=2(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$

Exercice
Décomposer dans $\mathbb{R}[X]$ le polynôme $X^{2n}-1$.
Que vaut le produit des racines $2n$-ièmes de l'unité ?

Correction
Le produit vaut 1, c'est le terme constant dans le développement de ce $X^{2n}-1$, factorisée sur $\mathbb{C}$.
Et

$$X^{2n}-1=(X-1)\prod_{k=1}^{n-1}(X-e^{ik\pi/n})(X-e^{-ik\pi/n})(X-(-1))=(X-1)(X+1)\prod_{k=1}^{n-1}(X^2-2\cos\left(\frac{k\pi}{n}\right)X+1)$$

Exercice
Soit $z_0,\ldots,z_{n-1}$ les racines n-ièmes de l'unité. Montrer que

$$\prod_{k=0}^{n-1}(z_k^2-2z_k\cos\theta+1)=4\sin^2(\frac{n\theta}{2}).$$

Correction
$(X^2-2\cos\theta+1)=(X-e^{i\theta})(X-e^{-i\theta})$, donc $(z_k^2-2z_k\cos\theta+1)=(z_k-e^{i\theta})(z_k-e^{-i\theta})=$,

$$\prod_{k=0}^{n-1}(z_k^2-2z_k\cos\theta+1)=\prod_{k=0}^{n-1}(e^{i\theta}-z_k)(e^{-i\theta}-z_k)=\prod_{k=0}^{n-1}(e^{i\theta}-z_k)\prod_{k=0}^{n-1}(e^{-i\theta}-z_k)$$
$$=((e^{i\theta})^n-1)((e^{-i\theta})^n-1)=(e^{ni\theta}-1)((e^{-ni\theta}-1)=e^{ni\theta/2}2i\sin\frac{n\theta}{2}e^{-ni\theta/2}2i\sin\frac{-n\theta}{2}$$
$$=-4e^{i0}(-1)\sin^2\frac{n\theta}{2}4\sin^2(\frac{n\theta}{2})$$

6. Bilan

Synthèse

- ⇝ $\mathbb{K}[X]$, comme $\mathbb{Z}$ est muni d'une division euclidienne.
- ⇝ On définit alors l'algorithme d'Euclide pour deux polynômes. Il conduit à la notion de PGCD de ces deux polynômes. Toute la structure est transportée de $\mathbb{Z}$ à $\mathbb{K}[X]$: PGCD, couple de Bézout, lemme de Gauss, PPCM, généralisations… Les méthodes sont identiques.
  On peut exploiter en outre : les racines, la dérivations et le changement d'origine !
- ⇝ Les nombres premiers deviennent les polynômes irréductibles. Le théorème d'Euclide d'écriture comme produit unique d'irréductibles (unitaires) est toujours vraie.
  Une description complète des irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$ est possible et assez simple.
- ⇝ On termine par une extension hors-programme de la notion de congruence.
  Et plus largement de la notion d'anneau euclidien (factoriel…) et d'idéaux…

Savoir-faire et Truc & Astuce du chapitre

- — Savoir-faire - Algorithme de la division euclidienne
- — Truc & Astuce pour le calcul - Suites (U_n) et (V_n)
- — Savoir-faire - Décomposition en produit d'irréductibles de $\mathbb{C}[X]$
- — Savoir-faire - Décomposition en produit d'irréductibles de $\mathbb{R}[X]$

Notations

	Propriétés	*Remarques*
es diviseurs de A		
es multiples de A		
et B (généralisable)	$(A)+(B)=(A\wedge B)$	Défini à une constante multiplicative près
et B (généralisable)	$(A)\cap(B)=(A\vee B)$	Défini à une constante multiplicative près

Retour sur les problèmes

110. C'est le but de ce cours.

111. Considérons $f\star g : P\mapsto \sum_{D|P,\,D\text{ unitaire}} f(D)g(P/D)$.
On a toujours, pour $P\wedge Q=1$, $D|PQ\iff D=D_1D_2$ avec $D_1|P$, $D_2|P$.
Dans ce cas $\Phi : D\mapsto(D_1,D_2):=(D\wedge P, D\wedge Q)$ établit une bijection $\mathscr{D}(PQ)$ sur $\mathscr{D}(P)\times\mathscr{D}(Q)$.
Supposons que f et g soient multiplicative. Alors on a, pour $P\wedge Q=1$:

$$f\star g(PQ)=\sum_{D|PQ\text{ unitaire}} f(D)g(PQ/D)=\sum_{D_1|P,D_2|Q,\text{ unitaires}} f(D_1D_2)g(PQ/D_1D_2)$$

$$=\sum_{D_1|P,D_2|Q,\text{ unitaires}} f(D_1)f(D_2)g(P/D_1)g(Q/D_2)=f(P)\times g(Q)$$

L'élément neutre est $f : 1\mapsto 1$ et $f : P\mapsto 0$ si $P\neq 1$.
Tout est pareil ! avec une fonction de Möbius….
La question est : que peut nous apprendre alors un tel outil ?

112. Concernant le grand théorème de Fermat, on parle ici du théorème de Liouville.
Supposons que $P^n+Q^n+R^n=0$ avec $P,Q,R\in\mathbb{C}[X]$ (avec $n\geqslant 3$).

(a) On commence par montrer qu'il suffit d'étudier le cas P,Q,R premiers entre eux deux à deux
(sinon, si $D|P$ et $D|Q$, alors $D|R$, et on peut simplifier)

(b) On dérive $\frac{P^n}{R^n}+\frac{Q^n}{R^n}=-1$(qu'on ne peut pas faire avec les entiers) :

$$P^{n-1}(PR'-RP')=-Q^{n-1}(QR'-RQ')$$

(c) Si P et R ne sont pas associés, alors $PR'-R'P\neq 0$.
Puis $Q\wedge P=1$, donc $Q^{n-1}|PR'-R'P$ et de même $P^{n-1}|QR'-R'Q$.
On ne peut avoir $\deg R>\max(\deg P,\deg Q)$, donc au moins un des $\deg P$ ou $\deg Q$ est le maximum de $\{\deg P,\deg Q,\deg R\}$.
Supposons que $p=\deg P=\max(\deg Q,\deg R)$.
Par division $P^{n-1}|QR'-RQ'$, alors $\deg P^{n-1}=(n-1)p\leqslant\deg Q+\deg R-1<2\deg P$.
Contradiction, puisque $n\geqslant 3$, donc $n-1\geqslant 2$ (sauf si $\deg P=0$…)

113. Classiquement, on noteF_p, le corps $\left(\frac{\mathbb{Z}}{p\mathbb{Z}},+,\times\right)$. On se place donc sur $F_p[X]$, les polynômes à coefficients dans F_p.
Si P est un polynôme irréductible de $F_p[X]$, et de degré n,
alors $\frac{F_p[X]}{(P)}$, l'ensemble des classes d'équivalences pour la relation $\cdot\equiv\cdot[P]$
et un corps. On exploite le théorème de Bézout.
Cet ensemble possède comme ensemble de représentant $\{Q\in F_p[X]\mid\deg Q<n\}$, de cardinal p^n.
Existe-t-il un tel polynôme irréductible ? Oui !
Comment en trouver ? On exploite le lemme suivant :
Pour tout $r\in\mathbb{N}$, sur F_p, le polynôme $R=X^{p^r}-X$ est égal au produit de tous les polynômes unitaires irréductibles de degré divisant r.
Cela donne la minoration :

$$\text{Nbre de polynôme de degré } n \text{ irréductible}\geqslant\frac{p^n-p^{\lfloor n/2\rfloor+1}}{n}$$

Et précisément, P de degré n est irreductible sur F_p ssi :
— $P|X^{p^n}-X$
— $\forall\, q\in\mathscr{P}$ tel que $q|n$, $P\wedge X^{p^{n/q}}-X=1$
(… Voir Wikipedia ou le cours de Demazure p.220)

Chapitre 34

Le corps des fractions de l'anneau intègre des polynômes

Résumé -

Nous avons vu au chapitre précédent un lien fort entre $\mathbb{Z}$ et $\mathbb{K}[X]$. Ces deux anneaux intègres présentent un autre problème en commun : ce ne sont pas des corps, c'est-à-dire que la plupart de leurs éléments ne sont pas inversibles.
Pour éviter ce problème pour $\mathbb{Z}$, nous avons construit $\mathbb{Q}$, corps des fractions rationnelles grâce à la relation d'équivalence $(p_1,q_1)\mathscr{R}(p_2,q_2)$ ssi $q_1\times p_2 = q_2\times p_1$.
Nous exploitons le même principe ici pour construire $\mathbb{K}(X)$, le corps des fractions rationnelles.
Nous nous concentrons alors sur la décomposition en éléments simples de toutes fractions, cela est souvent bien pratique lorsque l'on rencontre des fonctions rationnelles (à intégrer par exemple...).

Sommaire

1. Problèmes 676
2. $\mathbb{K}(X)$, corps des fractions de $\mathbb{K}[X]$ anneau intègre 676
2.1. Construction de $\mathbb{K}(X)$ 676
2.2. Représentant irréductible. Degré et pôle 677
2.3. Fonction rationnelle 678
2.4. Dérivation 678
3. Décomposition en éléments simples des fractions rationnelles 679
3.1. Partie entière 679
3.2. Principe de décomposition sur un corps $\mathbb{K}$ 679
3.3. Application de la décomposition sur le corps $\mathbb{C}$ . . . 682
3.4. Application de la décomposition sur le corps $\mathbb{R}$ . . . 682
4. Bilan 683

1. Problèmes

Problème 146 - $Z\to\mathbb{Q}$ et $\mathbb{K}[X]\to$??

Si l'on conduit le même processus de construction qui permet de passer de $\mathbb{Z}$ à $\mathbb{Q}$ (afin d'obtenir un corps) à partir de $\mathbb{K}[X]$, qu'obtient-on?
Quel est ce processus déjà?

Problème 147 - Intégration de fractions

Depuis le début d'année, on a rencontré des (fonctions) fractions rationnelles essentiellement dans le cours du calcul d'intégrales.
La stratégie consistait alors à réduire le plus possible la complexité du numérateur, et de factoriser le dénominateur afin d'obtenir une décomposition en éléments simples. Nous avons pratiqué cette méthode dans des cas simples, sans en voir la théorie.
Est-il toujours possible de décomposer toute fraction rationnelle en éléments simples? Et qu'est-ce que cela peut signifier?
En réinvestissant la théorie, est-il possible de trouver un algorithme de décomposition (qui marcherait à tous les coups)?
Quelle conséquence pour les intégrations de fractions rationnelles.

Problème 148 - Paramétrage rationnel du cercle

Une paramétrisation naturelle du cercle est donné par le couple $(\cos t,\sin t)$. Mais les fonctions cos et sin sont transcendantes.
Considérons le cercle d'équation $x^2+y^2=1$ et la droite d'équation $y=a(x+1)$, de pente a et qui passe par $A(-1,0)$.
L'intersection de ces deux courbes donne les points $M(x,y)$ tels que $1=x^2+y^2=x^2+a^2(x+1)^2$.
Or on sait que $(-1,0)$ est toujours une solution de cette intersection, on peut donc factoriser l'équation par $x+1$:

$$x^2+a^2(x+1)^2=1\iff(x+1)[(x-1)+a^2(x+1)]=0\iff(x-1)=0 \text{ ou } x=\frac{1-a^2}{1+a^2}$$

Comme $a(x+1)=a(\frac{1-a^2}{1+a^2}+1)=\frac{2a}{1+a^2}$ On trouve donc un nouveau paramétrage **rationnel** du cercle : $(\frac{1-a^2}{1+a^2},\frac{2a}{1+a^2})$.
Ce résultat vous rappelle-t-il quelque chose?
Comment exploiter cette paramétrisation pour trouver tous les triplets entiers pythagoriciens ($x^2+y^2=z^2$)?
Est-ce que la méthode s'adapte à autre chose que le cercle trigonométrique (cubique)? Qu'en faire?

2. $\mathbb{K}(X)$, corps des fractions de $\mathbb{K}[X]$ anneau intègre

2.1. Construction de $\mathbb{K}(X)$

Heuristique - Ensemble quotient

On crée l'ensemble $\mathbb{K}(X)$ à l'image de l'ensemble $\mathbb{Q}$.
$\mathbb{Z}$ était un anneau intègre mais pas un corps, l'ensemble $\mathbb{Q}$ est le plus petit corps contenant

, $\mathbb{Z}$. De même on va créer un corps contenant $\mathbb{K}[X]$.

Définition - Fractions rationnelles (par classe d'équivalence)
La relation binaire définie sur $\mathbb{K}[X]\times(\mathbb{K}[X]\setminus\{0\})$ par

$$(A_1,B_1)\mathscr{R}(A_2,B_2)\Leftrightarrow A_1B_2=A_2B_1$$

est une relation d'équivalence.
On note $K(X)$ l'ensemble des classes d'équivalence pour cette relation, un élément F de $\mathbb{K}(X)$ est écrit sous la forme $F=\dfrac{A}{B}$ (ou $F(X)=\dfrac{A(X)}{B(X)}$) où $(A,B)\in\mathbb{K}[X]\times(\mathbb{K}[X]\setminus\{0\})$.
On a donc $\dfrac{A_1}{B_1}=\dfrac{A_2}{B_2}\Leftrightarrow A_1B_2=A_2B_1$
F s'appelle une fraction rationnelle.

Proposition - Corps des fractions rationnelles
Muni des lois internes + et × définies par

$$\frac{A_1}{B_1}+\frac{A_2}{B_2}=\frac{A_1B_2+B_1A_2}{B_1B_2},\quad \frac{A_1}{B_1}\times\frac{A_2}{B_2}=\frac{A_1A_2}{B_1B_2}$$

$(\mathbb{K}(X),+,\times)$ est un corps contenant $\mathbb{K}[X]$ (on identifie B à $\dfrac{B}{1}$).

Démonstration
Il suffit d'écrire une à une les propriétés à vérifier… □

2.2. Représentant irréductible. Degré et pôle

Définition - Représentant irréductible
Soit $F=\dfrac{A}{B}$ et $D=A\wedge B$.
On a donc $A=DP$ et $B=DQ$ avec $P\wedge Q=1$, et alors $F=\dfrac{P}{Q}$.
On dit que $\dfrac{P}{Q}$ est un représentant irréductible de F.

Définition - Degré
Soit $F\in\mathbb{K}(X)$.
L'élément de $\mathbb{Z}\cup\{-\infty\}$, $\deg A-\deg B$, est indépendant du choix du représentant $\dfrac{A}{B}$ de F.
On l'appelle degré de la fraction rationnelle F, noté $\deg F$.

Il faut démontrer l'indépendance par représentant.

Démonstration
Soit $F=\dfrac{A_1}{B_1}=\dfrac{A_2}{B_2}$.
- Si $F=0$ alors $A_1=A_2=0$ et $\deg A_1-\deg B_1=\deg A_2-\deg B_2=-\infty$.
- Si $F\neq 0$, alors $A_1\neq 0$ et $A_2\neq 0$. On a $A_1B_2=A_2B_1$ donc $\deg A_1+\deg B_2=\deg A_2+\deg B_1$ d'où $\deg A_1-\deg B_1=\deg A_2-\deg B_2$.

□

Proposition - Extension des propriétés sur les degrés
On a les propriétés suivantes :

$$\deg(F_1+F_2)\leqslant\max(\deg F_1,\deg F_2)$$
$$\deg F_1F_2=\deg F_1+\deg F_2$$
$$\deg F=-\infty\Leftrightarrow F=0$$

Démonstration
On suppose que $F_1=\frac{A_1}{B_1}$ et $F_2=\frac{A_2}{B_2}$

$\deg(F_1F_2)=\deg\frac{A_1A_2}{B_1B_2}=\deg(A_1A_2-\deg(B_1B_2)=\deg(A_1)+\deg(A_2)-\deg(B_1)-\deg(B_2)=\deg F_1+\deg F_2$

Et ainsi de suite □

Définition - Racines et pôles
Soit $F\in\mathbb{K}(X)$, $\dfrac{P}{Q}$ un représentant irréductible de F. Soit $a\in\mathbb{K}$. On dit que a est une racine (ou un zéro) de F si $P(a)=0$ (a racine de P) et que a est un pôle de F si $Q(a)=0$ (a racine de Q).
La multiplicité d'une racine (resp. d'un pôle) de F est sa multiplicité en tant que racine de P (resp. de Q).

Remarque - a pôle et racine de F?
L'ensemble des racines et l'ensemble des pôles sont disjoints. (pourquoi?)

Exemple - Racines et les pôles de $\dfrac{X^3+X^2+X-3}{X^2-X}$
Quels sont les racines et les pôles de $\dfrac{X^3+X^2+X-3}{X^2-X}$?
$X^3+X^2+X-3=(X-1)(X^2+2X+3)=(X-1)(X+1+i\sqrt{2})(X+1-i\sqrt{2})$.
$X^2-X=X(X-1)$. Deux racines : $-1-i\sqrt{2}$ et $-1+i\sqrt{2}$ et un pôle 0.

2.3. Fonction rationnelle

Définition - Fonction rationnelle
Soit $F\in\mathbb{K}(X)$, $\dfrac{P}{Q}$ un représentant irréductible de F. On note Δ_F l'ensemble des pôles de F et on définit alors la fonction rationnelle associée à F par

$$\begin{array}{rccc}\widetilde{F}: & \mathbb{K}\setminus\Delta_F & \to & \mathbb{K}\\ & x & \mapsto & \dfrac{\widetilde{P}(x)}{\widetilde{Q}(x)}\end{array}$$

Remarque - Egalité des fonctions
Lorsque $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$ (ou plus généralement un corps infini) on a $\widetilde{F_1}=\widetilde{F_2}$ si et seulement si $F_1=F_2$.

2.4. Dérivation

Définition - Dérivée
Soit $F\in\mathbb{K}(X)$. La fraction rationnelle $\dfrac{A'B-AB'}{B^2}$ est indépendante du représentant choisi $\dfrac{A}{B}$ de F. On l'appelle dérivée de la fraction rationnelle F, notée F'.
Les propriétés vis à vis de la somme, du produit, ou du produit par un élément de $\mathbb{K}$ sont les propriétés usuelles.

Il faut démontrer l'indépendance du résultat en rapport au représentant.

Démonstration
Soit $F = \frac{A}{B} = \frac{A_1}{B_1}$. On a alors $AB_1 = A_1B$ donc en dérivant $A'B_1 + AB_1' = A_1'B + A_1B'$. En multipliant par BB_1, en utilisant $AB_1 = A_1B$ et en regroupant les termes on obtient $(A_1B_1' - A_1'B_1)B^2 = (AB' - A'B)B_1^2$ d'où $\frac{A_1B_1' - A_1'B_1}{B_1^2} = \frac{AB' - A'B}{B^2}$.
□

Remarque - Dérivation et fonction rationnelle
Lorsque $\mathbb{K} = \mathbb{R}$ les fonctions rationnelles $\widetilde{F}'$ et $\widetilde{F'}$ coincident.

3. Décomposition en éléments simples des fractions rationnelles

3.1. Partie entière

Proposition - partie entière
Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$ avec $P \wedge Q = 1$.
Alors il existe un unique couple $(E, \widehat{F}) \in \mathbb{K}[X] \times \mathbb{K}(X)$ tel que

$$F = E + \widehat{F} \text{ et } \deg \widehat{F} < 0.$$

E est appelée partie entière de la fraction F.

Démonstration
Si $\widehat{F} = \frac{A}{B}$ (irréductible), avec $\deg \widehat{F} < 0$, donc $\deg A - \deg B < 0$, i.e. $\deg A < \deg B$.
On a donc $F = \frac{P}{Q} = E + \frac{A}{B}$, donc $\frac{P}{Q} = \frac{EB + A}{B}$.
Par irréductibilité, Q et B sont associés et donc on trouve : $P = EQ + A$, avec $\deg A < \deg Q$.
Finalement, il s'agit de la division euclidienne de P par Q : E est le quotient et A le reste.
La décomposition est unique. □

Savoir faire - Comment obtenir la partie entière?
Si $\deg F < 0$ alors $E = 0$,
sinon on effectue la division euclidienne de P par Q :
$P = EQ + R$ et $F = \frac{P}{Q} = E + \frac{R}{Q}$.

3.2. Principe de décomposition sur un corps $\mathbb{K}$

Théorème - Décomposition en éléments simples sur $\mathbb{K}$
Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$ une fraction irréductible. Q se décompose en produit de polynômes irréductibles

$$Q = \lambda Q_1^{k_1} \dots Q_p^{k_p} = \lambda \prod_{j=1}^{p} Q_j^{k_j}.$$

Alors F s'écrit de manière unique, E étant la partie entière,

$$F = E + \sum_{j=1}^{p} \left(\frac{P_{1j}}{Q_j} + \frac{P_{2j}}{Q_j^2} + \dots + \frac{P_{k_j j}}{Q_j^{k_j}} \right)$$

où $P_{ij} \in \mathbb{K}[X], \deg P_{ij} < \deg Q_j$.
Cette décomposition s'appelle la **décomposition en éléments simples** sur

$\mathbb{K}$ (ou dans $\mathbb{K}(X)$) de la fraction F.
Si $Q_j = X - a_j$, $a_j \in \mathbb{K}$, $\left(\frac{P_{1j}}{Q_j} + \frac{P_{2j}}{Q_j^2} + \dots + \frac{P_{k_j j}}{Q_j^{k_j}} \right)$ s'appelle la **partie polaire** de F relative (ou associée) au polynôme Q_j (ou au pôle a_j si $Q_j = X - a_j$).

Heuristique - Principe de démonstration
On exploite une formule de Bézout généralisée pour démontrer l'existence (par récurrence sur p).
Puis avec la formule de Taylor, on simplifie les fractions.

Pour aller plus loin - A quoi cela peut servir?
Une application déjà vue de la décomposition en éléments simples concerne le calcul de primitive/intégrale d'une fraction rationnelle.
Une autre application peut se faire pour les série génératrice rationnelle (avec des séries géométriques) ou bien le calcul de DL_n. Par exemple, avec $\frac{X^3}{(X-1)^3(X-2)^2} = \dots = \frac{1}{(X-1)^3} + \frac{5}{(X-1)^2} + \frac{12}{(X-1)} + \frac{8}{(X-2)^2} - \frac{12}{X-2}$*, on peut affirmer :*
$\frac{x^3}{(x-1)^3(x-2)^2} \underset{x \to 1}{=} \frac{1}{(x-1)^3} + \frac{5}{(x-1)^2} + \frac{12}{x-1} + 20$

Démonstration
Ce résultat se démontre en plusieurs étapes, en voici les grandes lignes :
— Tout d'abord l'existence.
Première étape : on montre par récurrence sur p que F s'écrit sous la forme

$$F = E + \sum_{i=1}^{p} \frac{B_i}{Q_i^{k_i}} \text{ avec } \deg B_i < \deg Q_i^{k_i}.$$

Si $p = 1$ on a le résultat d'après la proposition précédente.
Supposons le résultat vrai à un rang $p - 1 \geqslant 1$.
Au rang p, on a $Q_p^{k_p} \wedge (Q_1^{k_1} \dots Q_{p-1}^{k_{p-1}}) = 1$
donc $\exists (U, V) \in \mathbb{K}[X]$ tel que $UQ_p^{k_p} + VQ_1^{k_1} \dots Q_{p-1}^{k_{p-1}} = 1$ avec $\deg V < \deg Q_p^{k_p}$
et donc $PUQ_p^{k_p} + PVQ_1^{k_1} \dots Q_{p-1}^{k_{p-1}} = P$. On a alors

$$F = \frac{PU}{Q_1^{k_1} \dots Q_{p-1}^{k_{p-1}}} + \frac{PV}{Q_p^{k_p}}$$

Par division euclidienne $PV = A_p Q_p^{k_p} + B_p$ avec $\deg B_p < \deg Q_p^{k_p}$, d'où :

$$F = A_p + \frac{B_p}{Q_p^{k_p}} + \frac{PU}{Q_1^{k_1} \dots Q_{p-1}^{k_{p-1}}}$$

D'après l'hypothèse de récurrence au rang $p - 1$, on obtient

$$F = A_p + E_{p-1} + \sum_{i=1}^{p} \frac{B_i}{Q_i^{k_i}} \text{ avec } \deg B_i < \deg Q_i^{k_i}.$$

Comme $\deg \left(\sum_{i=1}^{p} \frac{B_i}{Q_i^{k_i}} \right) < 0$, d'après la proposition précédente (unicité), $A_p + E_{p-1}$ est la partie entière E.
Seconde étape : on montre que pour $B \in K[X], Q \in \mathbb{K}[X] \setminus \mathbb{K}$ et $k \in \mathbb{N}$, il existe $V_0, V_1, \dots V_k \in \mathbb{K}[X]$ vérifiant

$$B = V_0 + V_1 Q + \dots + V_k Q^k \text{ avec } \deg V_i < \deg Q.$$

Sur $\mathbb{C}[X]$, si Q est irréductible, il est de la forme $X - a$ et il s'agit donc de la formule de Taylor.
Plus généralement (et donc sur $\mathbb{R}[X]$ en particulier) on montre ce résultat par récurrence sur $\deg B$ en utilisant la division euclidienne.
(En fait il s'agit d'une sorte de décomposition dans la base Q, comme en informatique en début d'année)
En appliquant la première étape, puis la seconde à $B = B_i, Q = Q_i$ et $k = k_i$, on obtient l'existence voulue.

— Pour l'unicité, il s'agit en fait de démontrer l'unicité à chacune des étapes, d'abord pour les B_i, puis pour les V_j. (travail sur les degrés et la divisibilité).
□

Proposition - Pôles simples
Si a est un pôle simple de $F = \frac{P}{Q}$ ($\deg F < 0$), pour trouver la partie polaire $\frac{\lambda}{X - a}$, on peut utiliser $\lambda = \frac{P(a)}{\widehat{Q}(a)} = \frac{P(a)}{Q'(a)}$ où $\widehat{Q}$ est telle que $Q = (X - a)\widehat{Q}$.

Ce second résultat (avec Q', facile à obtenir car polynôme) évite même la factorisation de Q

Démonstration
Si $P = EQ + \overline{P}$, et a un pôle de F, alors $P(a) = E(a)Q(a) + \overline{P}(a) = \overline{P}(a)$.
On peut donc suppose que $\deg F < 0$ comme $\frac{\overline{P}}{Q}$ car $F(a) = \frac{P(a)}{Q(a)} = \frac{\overline{P}(a)}{Q(a)}$.
$F = \frac{P}{Q} = \frac{P}{\widehat{Q}\times(X-a)} = \frac{\lambda}{X-a} + \frac{R}{\widehat{Q}}$.
Donc en multipliant par $(X-a)$: $(X-a)F = \frac{P}{\widehat{Q}} = \lambda + \frac{R\times(X-a)}{\widehat{Q}}$.
Et comme a est un pôle simple (donc $Q'(a) \neq 0$), on a en $X = a$: $\frac{P(a)}{\widehat{Q}(a)} = \lambda + 0$.
Par ailleurs, d'après la règle du produit : $Q' = (X-a)\widehat{Q}' + \widehat{Q}$ et donc en substituant a à X : $Q'(a) = 0 + \widehat{Q}(a) = \lambda$. □

Savoir faire - Obtenir la partie polaire - cas pôle simple

Si a est un pôle simple de $F = \frac{P}{Q}$, la partie polaire $\frac{\lambda}{X-a}$ s'obtient avec

$\lambda = \frac{P(a)}{Q'(a)}$

Savoir faire - Obtenir la partie polaire - cas d'un pôle multiple

En isolant la partie polaire relative au pôle a de multiplicité m, on a, pour $Q = (X-a)^m\widehat{Q}$,

$$F = \sum_{k=1}^{m} \frac{\lambda_k}{(X-a)^k} + \frac{P_1}{\widehat{Q}}.$$

• En multipliant cette égalité par $(X-a)^m$ et en substituant a à X on trouve λ_m.

• On retranche ensuite $\frac{\lambda_m}{(X-a)^m}$ à F, on obtient donc après simplification une fraction dont a est pôle de multiplicité $m-1$ et on recommence.
Cette méthode est en pratique applicable si m est petit.
D'autres possibilités une fois λ_m obtenu :
• On multiplie par X puis on prend la limite en $+\infty$ de la fonction rationnelle obtenue : cela permet généralement d'obtenir λ_1.
• Si $m \geqslant 3$, on a donc obtenu λ_m et λ_1. Si l'on veut éviter les soustractions successives, on substitue des valeurs particulières simples à X autres que le pôle (0,...)

Cela marche aussi pour $m = 1$.
Exercice

Décomposer en éléments simples la fraction $F = \frac{1}{X^2(X-1)^3}$.

Correction
Les pôles sont 0 d'ordre 2 et 1 d'ordre 3.
Donc $F = \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X-1} + \frac{d}{(X-1)^2} + \frac{e}{(X-1)^3}$
On a $b = \frac{1}{(0-1)^3} = -1$ et $e = \frac{1}{1^2} = 1$
Donc $\frac{a}{X} + \frac{c}{X-1} + \frac{d}{(X-1)^2} = F - \frac{-1}{X^2} - \frac{1}{(X-1)^3} = \frac{X^3-4X^2+3X}{X^2(X-1)^3} = \frac{X-3}{X(X-1)^2}$
On vérifie qu'il y a bien une simplification par X et par $X-1$.
Donc $a = \frac{-3}{(0-1)^2} = -3$ et $d = \frac{1-3}{1} = -2$.
Donc $F = \frac{-3}{X} + \frac{-1}{X^2} + \frac{c}{X-1} + \frac{-2}{(X-1)^2} + \frac{1}{(X-1)^3}$.
On peut appliquer la même méthode, ou prendre une valeur en un point, par exemple en -1 :
$F(-1) = \frac{1}{-8} = 3 - 1 - \frac{c}{2} - \frac{1}{2} - \frac{1}{8}$, donc $c = 3$.
Ainsi $F = \frac{-3}{X} + \frac{-1}{X^2} + \frac{3}{X-1} + \frac{-2}{(X-1)^2} + \frac{1}{(X-1)^3}$

3.3. Application de la décomposition sur le corps $\mathbb{C}$

Sur $\mathbb{C}$, on applique le théorème « Décomposition en éléments simples sur $\mathbb{K}$ », les facteurs irréductibles sont des polynômes de degré 1.

Théorème - Décomposition en éléments simples sur $\mathbb{C}$
Soit $F = \frac{P}{Q} \in \mathbb{C}(X)$ une fraction irréductible. Q se décompose en produit de polynômes irréductibles $Q = \lambda\prod_{j=1}^{p}(X-\alpha_j)^{k_j}$.
Alors F s'écrit de manière unique, E étant la partie entière et $A_{ij} \in \mathbb{C}$,

$$F = E + \sum_{j=1}^{p}\left(\frac{A_{1j}}{X-\alpha_j} + \frac{A_{2j}}{(X-\alpha_j)^2} + \cdots + \frac{A_{k_jj}}{(X-\alpha_j)^{k_j}}\right)$$

Théorème - Lemme de Gauss-Lucas
Si $P = \lambda\prod_{j=1}^{p}(X-\alpha_j)^{k_j}$ alors $\frac{P'}{P} = \sum_{j=1}^{p}\frac{k_j}{X-\alpha_j}$.

Démonstration
Un simple calcul :

$$P' = \lambda\sum_{j=1}^{p}\left(k_j(X-\alpha_j)^{k_j-1}\prod_{i=1,i\neq j}^{p}(X-\alpha_i)^{k_i}\right) = \sum_{j=1}^{p}\left(k_j\frac{P}{X-\alpha_j}\right)$$

Donc

$$\frac{P'}{P} = \sum_{j=1}^{p}\frac{k_j}{X-\alpha_j}$$

□

Pour aller plus loin - Localisation des racines de P'
Le théorème de Rolle appliqué à $\tilde{P}$ permet d'affirmer qu'entre deux racines de P, se trouve une racine de P'. Et si les racines de P sont dans $\mathbb{C}$?
Le théorème de Gauss-Lucas permet d'affirmer que si $P'(\beta) = 0$, alors (en prenant la partie conjuguée) : $\sum_{j=1}^{p}\frac{k_j}{|\beta-\alpha_j|^2}(\beta-\alpha_j) = 0$.
Donc en notant $\lambda_j = \frac{k_j}{|\beta-\alpha_j|^2}$ et $N = \sum_{j=1}^{p}\lambda_j$, on a $\beta = \frac{1}{N}\sum_{j=1}^{p}\lambda_j\alpha_j$.
Par conséquent : β est dans l'enveloppe convexe des racines (α_j)

3.4. Application de la décomposition sur le corps $\mathbb{R}$

Sur $\mathbb{R}$, on applique le théorème « Décomposition en éléments simples sur $\mathbb{K}$ », les facteurs irréductibles sont des polynômes de degré 1 ou 2 avec $\Delta < 0$.

Théorème - Décomposition en éléments simples sur $\mathbb{R}$
Soit $F = \frac{P}{Q} \in \mathbb{R}(X)$ une fraction irréductible. Q se décompose en produit de polynômes irréductibles

$$Q = \lambda\prod_{j=1}^{p'}(X-\alpha_j)^{k'_j}\prod_{j=1}^{p''}(X^2+\delta_jX+\gamma_j)^{k''_j}.$$

Alors F s'écrit de manière unique, E étant la partie entière,

$$F = E + \sum_{j=1}^{p'}\left(\frac{A_{1j}}{X-\alpha_j} + \frac{A_{2j}}{(X-\alpha_j)^2} + \cdots + \frac{A_{k'_jj}}{(X-\alpha_j)^{k'_j}}\right) + \sum_{j=1}^{p''}\left(\frac{B_{1j}X+C_{1j}}{X^2+\delta_jX+\gamma_j} + \cdots + \frac{B_{k''_jj}X+C_{k''_jj}}{(X^2+\delta_jX+\gamma_j)^{k''_j}}\right)$$

tous les coefficients A, B, C étant des réels.
La première somme est formée d'éléments simples de première espèce, la seconde d'éléments simples de deuxième espèce.

Savoir faire - Décomposition en élément simples de deuxième espèce

On peut
- décomposer dans $\mathbb{C}(X)$ et regrouper les pôles conjugués : cela marche bien quand la multiplicité est 1 ;
- procéder par identification ;
- quand il ne reste qu'un ou deux coefficients à calculer, on utilise des valeurs particulières : $0, 1, -1, +\infty, -\infty$;
- utiliser une éventuelle parité et l'unicité de la décomposition.

4. Bilan

Synthèse

⇝ Exactement de la même manière que $\mathbb{Q}$ étend $\mathbb{Z}$ en intégrant les inversible, on construit le corps des fractions rationnelles $\mathbb{K}(X)$ à partir de l'anneau intègre $\mathbb{K}[X]$.

⇝ On étend alors la notion de degré et de derivée ; on définit les fractions irréductibles ; on définit aussi les pôles (et racines) des fractions rationnelles.

⇝ Un savoir-faire nous mobilise tout particulièrement : l'algorithme de décomposition en éléments simples de $\frac{A}{B}$.
D'abord l'écriture (existence) : on commence par faire la division euclidienne de A par B ; puis on factorise le dénominateurs B en produit de puissance d'irréductibles ; on trouve enfin les numérateurs (de degré minimal) qu'il faut associé à chacun.
Puis la recherche des coefficients exacts des polynômes (différents savoir-faire à combiner)

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Comment obtenir la partie entière ?
- Savoir-faire - Obtenir la partie polaire - cas pôle simple
- Savoir-faire - Obtenir la partie polaire - cas pôle multiple
- Savoir-faire - Décomposition en éléments simples de deuxième espèce

Notations

	Propriétés	*Remarques*
fraction rationnelle à partir de tègre $\mathbb{K}[X]$	$\frac{\mathbb{K}[X]}{\mathscr{R}}$ avec $(A,B)\mathscr{R}(C,D)$ ssi $AD=BC$	Ce sont les classes d'équivalence pour la relation des fractions

Retour sur les problèmes

114. Cours

115. Oui, on se restreint d'abord aux irréductibles avec la décomposition en éléments simples sur les dénominateurs.

116. Supposons que $x^2+y^2=z^2$. On a donc $a\in\mathbb{Q}$ tel que $\frac{x}{z}=\frac{1-a^2}{1+a^2}$ et $\frac{2a}{1+a^2}$.
Si on note $a=\frac{p}{q}$ on trouve en multipliant tout par q^2 :
$x=q^2-p^2$, $y=2pq$ et $z=q^2+p^2$.
C'est exactement toutes les solutions possibles de triplets pythagoriciens premiers entre eux (on peut aussi multiplier par λ). On peut l'adapter au cubique et obtenir une nouvelle loi de groupe… (https://webmath.univ-rennes1.fr/master/master2/textes/legeay.pdf)

Huitième partie

Probabilités

Chapitre 35

Probabilités sur un univers fini

Résumé -

Depuis quelques siècles, le mathématiciens se proposent "d'éclairer de leurs lumières" les problèmes liés à des événements aléatoires, dus au hasard. Pour ce faire ils ont développé un type de calcul : le calcul de probabilité.

On associe au mot hasard une racine arabe : az-zahr qui signifie le dé. Il est apparu en français pour signifier tout d'abord un jeu de dés, puis plus généralement un événement non prévisible et par extension le mode d'apparition de ce type d'événement.

L'objet de la théorie mathématique des probabilités est l'analyse mathématique puis la synthèse calculatoire des phénomènes dans lesquels le hasard intervient, semble-t-il....

Dans ce premier chapitre, nous posons de manière satisfaisante la modélisation acceptable de toute expérience aléatoire : il s'agit d'abord de définir un espace de probabilité. Une fois cela fait, nous reprenons une notion très importante du cours de l'année dernière : le conditionnement en probabilités (et la notion d'événements indépendants qui en découle).

Sommaire

1. Problème 688
2. Vocabulaire des expériences aléatoires 689
2.1. Modélisation en probabilité 689
2.2. Expérience aléatoire 689
2.3. Evénements 690
3. Espaces probabilisés finis 691
3.1. Définitions 691
3.2. Propriétés 692
3.3. Suite (dé)croissante d'événements 693
3.4. Exemples de probabilité 694
3.5. Loi uniforme et simulation avec Python 696
4. Conditionnement et indépendance 697
4.1. Conditionnement 697
4.2. Indépendance en probabilité 704
5. Bilan 707

1. Problème

Problème 149 - Structure mathématique

Le hasard (ou les phénomènes contingent) peuvent-ils s'interpréter au mieux avec une modélisation mathématique?
Les probabilités peuvent-elles se mesurer, se calculer (s'additionner...)?
De quel objet mathématiques sont-elles tout proche?
Et les événements associés, quelle est la structure de l'ensemble des événements? De quel objet mathématiques sont-ils tout proche?

Problème 150 - Quelle définition pour la probabilité d'un événement

Pendant quelques siècles, les mathématiciens comprenaient les probabilités de deux façons :
- les fréquentialistes : la probabilité d'un événement est égal à la proportion de réalisation de cet événement lorsqu'on réalise un grand nombre de fois cette expérience.
- les subjectivistes : la probabilité d'un événement se calcul à partir des symétries du problèmes et de raisonnements subjectifs a priori.

Aujourd'hui, en mathématiques, le débat est tranché. Comment?
Si les deux approches ont co-existé c'est qu'il y a certainement un lien assez profond entre les deux. Lequel et sous quelle forme mathématique?

Problème 151 - Informatique

Peut-on simuler informatiquement le hasard ou un pseudo-hasard qui y ressemble beaucoup?
Si oui, comment ces simulations peuvent nous aider à mieux comprendre les lois de probabilités et à vérifier les calculs effectués (qui sont souvent des calculs sur des « grands nombres »)?

Problème 152 - Incompatibilité des événements

Des événements qui ne peuvent se réaliser en même temps sont dits incompatibles.
Que peut-on dire de leur probabilité de réalisation?

Problème 153 - Indépendance des événements

Et des événements indépendants? Qu'est-ce que cela veut dire?
La définition de l'indépendance d'événements est-elle d'abord mathématique ou phénoménologique?

Problème 154 - Deux événements en relation

Si l'on sait que deux événements E_1 et E_2 sont dépendant mutuellement l'un de l'autre, il est possible de trouver une relation entre ces deux dépendances $E_1 \Rightarrow E_2$ et $E_2 \Rightarrow E_1$, en fonction de E_1 et E_2. On peut donc passer d'un calcul d'une probabilité à l'autre.
Si on ajoute une temporalité entre les deux, cela donne une formule pour remonter le temps : la formule de Bayes. Que nous apprend-elle?

Concrètement : Si un test médical donne avec 99% le bon diagnostic et qu'il m'annonce que je suis malade. Quelle est la probabilité que je sois véritablement malade? (Ai-je toutes les informations?)

2. Vocabulaire des expériences aléatoires

Heuristique - Sur quelques définitions...

Dans cette partie, nous commençons par quelques définitions qui ne sont pas très « mathématiques ». Elles donnent plus un principe d'application qu'un cadre formalisé qui nous permettra de faire des démonstrations.

2.1. Modélisation en probabilité

Le "modèle" est un concept clé en mathématiques de l'aléatoire et de manière générale en science même si ce concept a mis du temps à se dégager. On rappelle néanmoins :

Définition - Modèle mathématique

Un modèle est une interprétation abstraite, simplifiée et idéalisée d'un objet du monde réel ou d'une description de la réalité.

Heuristique - Modélisation en probabilité

Pour obtenir un modèle pseudo-concret associé à une situation réelle, il est d'abord nécessaire (**sans quoi, on ne peut pas faire grand chose**) de recenser toutes les résultats possibles de l'expérience que l'on observe → *définition de l'univers.*
L'étape supplémentaire consiste donc à **associer** *(si possible)* **à chacune des situations possibles un nombre qui mesure la possibilité de réalisation**→ *définition de la tribu d'événements sur l'univers.*
Ces nombres (il y a plusieurs situations possibles) sont associés en une **fonction** de probabilité, elle prend ces valeurs dans un ensemble $\mathscr{A}$ qui peut être celui des sous ensembles de Ω. Pour comprendre les propriétés essentielles vérifiées par $\mathscr{A}$, il faut voir celles que l'on souhaite associer à $\mathbf{P}$.→ *définition (enfin) de la probabilité.*

2.2. Expérience aléatoire

La définition suivante n'est pas très « mathématique ». C'est plus un principe d'application qu'un cadre formalisé qui nous permettra de faire des démonstrations :

Définition - Expérience aléatoire

On appelle **expérience aléatoire** toute expérience dont le résultat dépend du **hasard** :
• lancer de dé, tirage d'une carte, jeu de pile ou face,
• observation du nombre d'appels dans un central téléphonique pendant une durée fixée,
• observation de la durée de vie d'un individu anonyme d'une population, tirage d'un nombre au hasard entre 0 et 1...
A une telle expérience on associe l'ensemble de tous les résultats observables, noté Ω et appelé **univers** (ou univers des possibles).

Exemple - Univers possible

Ω peut être un ensemble :

- *fini*, c'est par exemple le cas lorsque l'expérience aléatoire consiste à jeter deux dés à six faces, numérotées de 1 à 6 ; on a alors

$$\Omega = \{1,2,3,4,5,6\}^2 = \{(1,1),\dots,(2,4),\dots\}$$

si un résultat correspond au couple : résultat du dé 1, résultat du dé 2.
C'est l'expérience aléatoire simulée par `random.randint(1,7,2)` du module `numpy.random` de `Python`.
Si on prend pour résultat de l'expérience, la somme des deux nombres obtenus :

$$\Omega' = \{2,3,4,\dots,11,12\}$$

- *dénombrable*, c'est par exemple le cas lorsque l'expérience aléatoire consiste à observer le nombre d'appels transitant par une antenne relai en 10 minutes ; on a alors

$$\Omega = \mathbb{N}$$

(potentiellement infini dénombrable).
- *infini non dénombrable*, c'est par exemple le cas lorsque l'expérience aléatoire consiste à tirer au hasard un nombre réel entre 0 et 1 (en pointant un compas de pointe infiniment fine sur une règle graduée de 0 à 1 par exemple) ; on a alors

$$\Omega = [0,1]$$

C'est l'expérience aléatoire simulée par `random.rand(1)` du module `numpy.random` de `Python`.
Mais ce n'est pas l'expérience aléatoire vraiment réalisée car la pointe du compas n'est pas ici infiniment fine.

2.3. Evénements

Comparaison événements/ensembles

Définition - Issue et événement aléatoire

Un élément de Ω est usuellement noté ω et appelé **issue**.
Un **événement aléatoire** A est représenté par l'ensemble des résultats ω qui le réalisent. C'est donc une partie de Ω. On a donc $\omega \in A$ et $A \subset \Omega$.
Le singleton $\{\omega\}$ est appelé événement élémentaire.

Exemple - « Tirer » au hasard

- On jette deux dés à six faces, numérotées de 1 à 6 ; on considère A l'événement "obtenir une somme égale à 10", alors
$A = \{(4,6),(5,5),(6,4)\}$
- On observe le nombre d'appels transitant par une antenne relai pendant 10 minutes, on considère A l'événement "plus de 10^4 appels transitent par l'antenne" et B "aucun appel ne transite par l'antenne", alors

$$A = [\![10^4,\infty[\![\text{ ou } [\![10^{-4},\infty[\![\qquad B = \emptyset$$

- On tire au hasard un nombre réel entre 0 et 1 ; on considère A l'événement "obtenir un nombre strictement inférieur à 0.5" et B l'événement "obtenir un entier", alors

$$A = [0,0.5[\qquad B = \{0,1\}$$

Définition - Vocabulaire probabiliste

On utilise le vocabulaire probabiliste suivant pour les événements :

notation	terminologie probabiliste
$\emptyset$	**événement impossible**
Ω	**événement certain**
$\overline{A}$	**événement contraire** de A
singleton $\{\omega\}$	**événement élémentaire**
$A \cup B$	**événement** A **ou** B
$A \cap B$	**événement** A **et** B
$A \cap B = \emptyset$	A et B sont **incompatibles**
$A \subset B$	A **implique** B

Système complet d'événements - Partition de Ω

Définition - Système complet d'événements
On appelle **système complet d'événements** toute famille finie ou dénombrable $(A_i)_{i\in I}$ d'événements deux à deux incompatibles, tels que $\bigcup_{i\in I} A_i = \Omega$.
Dans le cas où Ω est fini, un système complet d'événement est une famille finie $(A_1, A_2, \dots, A_n)$ d'événements deux à deux incompatibles tels que $\bigcup_{i=1}^{n} A_i = \Omega$.

Exemple - Trivial
si $A \in \mathscr{P}(\Omega)$, $(A, \overline{A})$ forme un système complet d'événements.

Remarque - Partition
Si l'on impose que tous les événements soient non vides, alors un système complet d'événements est une partition finie ou dénombrable de Ω.

3. Espaces probabilisés finis

On considère désormais uniquement le cas où Ω est un ensemble fini.

3.1. Définitions

Définition - Probabilité sur un univers fini
Soit Ω un univers fini.
On appelle **probabilité** sur Ω toute application $\mathbf{P} : \mathscr{P}(\Omega) \to [0,1]$ telle que

(i) $\mathbf{P}(\Omega) = 1$

(ii) Pour tout couple (A, B) d'événements incompatibles, $\mathbf{P}(A \uplus B) = \mathbf{P}(A) + \mathbf{P}(B)$

On appelle **espace probabilisé fini** tout couple $(\Omega, \mathbf{P})$ où $\mathbf{P}$ est une probabilité sur un univers fini Ω.

Pour aller plus loin - Espace probabilisé fini/espace probabilisable/espace de probabilité
Il ne s'agit pas de la définition généralement admise d'un espace de probabilisé (ou de probabilité).
Dans le cas non fini, il faut également ajouter une tribu de Ω.
Une tribu τ de Ω est un ensemble de parties de Ω contenant la partie vide, stable par réunion (et intersection) dénombrable et par passage au complémentaire.
La mesure de probabilité $\mathbf{P}$ est alors définie sur τ.
Finalement, dans le cas fini, on prend par principe $\tau = \mathscr{P}(\Omega)$ et on n'en parle plus…

Attention - Addition et réunion
Notons bien que l'on réunit les événements (et **on ne les additionne pas**)
En revanche, on additionne les probabilités des événements (incompatibles) (et **on ne les réunit pas**)

Définition - Evénements négligeable, presque sûr
Un événement A est dit **négligeable** si $\mathbf{P}(A) = 0$.
Un événement A est dit **presque sûr** (p.s.) si $\mathbf{P}(A) = 1$.
Une propriété $\mathscr{P}$ est dite **presque sûre** (ou **vraie presque sûrement**) si la probabilité qu'elle se réalise vaut 1.

Pour aller plus loin - Cas discret
La démonstration reste identique dans le cas de Ω non fini mais dénombrable comme on le voit en seconde année.
Le résultat reste vrai dans des cadre plus large encore…

Pour aller plus loin - Crible de Poincaré
Comme en dénombrement, on a une formule plus général dans le cas des événements non disjoints :

$$P(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{k=1}^{n} (-1)^{k+1} \Big(\sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} P(A_{i_1} \cap \cdots \cap A_{i_k}) \Big)$$

Savoir faire - Une bonne habitude à prendre de suite
Lorsque l'on écrit $\mathbf{P}(A)$, surtout on ne *dit* pas *« P de A »* mais bien *« la probabilité de l'événement A »* ou beaucoup mieux : *« la probabilité que l'on ait obtenu un as »*.
On notera en effet : qu'il y a toujours un verbe dans une proposition relative dans ce cas là et donc qu'il manque un verbe dans la proposition principale. La dernière expression proposée invite naturellement à dire ensuite *« vaut »* ou *« est égale à »* ; ce que n'invite pas à faire *« P de A »*

3.2. Propriétés

Proposition - Premières propriétés
Soit $(\Omega, \mathbf{P})$ un espace probabilisé fini. Alors

1. $\mathbf{P}(\overline{A}) = 1 - \mathbf{P}(A)$
2. $\mathbf{P}(\emptyset) = 0$
3. $\mathbf{P}(A \cup B) = \mathbf{P}(A) + \mathbf{P}(B) - \mathbf{P}(A \cap B)$
4. $A \subset B \Rightarrow (\mathbf{P}(A) \leqslant \mathbf{P}(B)$ et $\mathbf{P}(B \setminus A) = \mathbf{P}(B \cap \overline{A}) = \mathbf{P}(B) - \mathbf{P}(A)$
5. Si $A_1, \cdots, A_n$ sont n événements deux à deux incompatibles alors $\mathbf{P}(\bigcup_{k=1}^{n} A_k) = \sum_{k=1}^{n} \mathbf{P}(A_k)$.
6. Si $(A_i)_{1\leqslant i\leqslant n}$ est un système complet d'événements alors $\sum_{i=1}^{n} \mathbf{P}(A_i) = 1$.
7. Plus généralement si $A_1, \cdots, A_n$ sont n événements alors $\mathbf{P}(\bigcup_{k=1}^{n} A_k) \leqslant \sum_{k=1}^{n} \mathbf{P}(A_k)$.

Remarque - Précision pour 4.
Si $A \not\subseteq B$), on n'a pas $\mathbf{P}(B \setminus A) = \mathbf{P}(B) - \mathbf{P}(A)$.

Démonstration

1. Comme $\overline{A} \cap A = \emptyset$, $\mathbf{P}(A) + \mathbf{P}(\overline{A}) = \mathbf{P}(A \cup \overline{A})$.
   Et comme $A \cup \overline{A} = \Omega$ et $\mathbf{P}(\Omega) = 1$, on a le résultat attendu.
2. Comme $\emptyset = \overline{\Omega}$, alors d'après la règle précédente : $\mathbf{P}(\emptyset) = 1 - \mathbf{P}(\Omega) = 1 - 1 = 0$.
3. Nous ne savons rien de A et B ici.
   On note $A' = A \setminus (A \cap B) = A \cap \overline{B}$.
   Ainsi, $A = A \cup (A \cap B)$ et $A' \cap (A \cap B) = \emptyset$, donc $\mathbf{P}(A) = \mathbf{P}(A') + \mathbf{P}(A \cap B)$.
   Enfin, comme $B \cap A' = \emptyset$ (sinon, $A' \cap (A \cap B) \not\emptyset$), on a
   $$\mathbf{P}(A \cup B) = \mathbf{P}(A' \cup B) = \mathbf{P}(A') + \mathbf{P}(B) = \mathbf{P}(A) - \mathbf{P}(A \cap B) + \mathbf{P}(B)$$
4. Si $A \subset B$, alors il existe C tel que $A \cup C = B$ et $A \cap C = \emptyset$, donc $\mathbf{P}(B) = \mathbf{P}(A) + \mathbf{P}(C) \geqslant \mathbf{P}(A)$.
   et plus précisément donc, $\mathbf{P}(C) = \mathbf{P}(B \setminus A) = \mathbf{P}(B) - \mathbf{P}(A)$
5. On applique par récurrence le résultat donné un peu plus haut.
6. Supposons que $(A_i)_{1\leqslant i\leqslant n}$ est un système complet d'événements.
   Alors les A_i sont disjoints deux à deux, $\mathbf{P}(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} \mathbf{P}(A_i)$.
   Et comme dans ce cas, $\bigcup_{i=1}^{n} A_i = \Omega$, on retrouve le résultat annoncé.
7. On procède par récurrence. Elle est plus subtile, on va la faire.
   On note $\mathscr{P}_n$ le résultat à démontrer et qui dépend de n.
   On a vu que $\mathscr{P}_1$ et $\mathscr{P}_2$ sont vraies.
   Soit n, supposons que $\mathscr{P}_n$ est vraie.
   Soient $A_1, \cdots, A_n, A_{n+1}$, $n+1$ événements et $B = \bigcup_{i=1}^{n} A_i$. Alors
   $$\mathbf{P}(\bigcup_{k=1}^{n+1} A_k) = \mathbf{P}(B \cup A_{n+1}) \leqslant \mathbf{P}(B) + \mathbf{P}(A_{n+1}) \leqslant \sum_{k=1}^{n} \mathbf{P}(A_k) + \mathbf{P}(A_{n+1})$$
   d'après $\mathscr{P}_n$. Et donc $\mathscr{P}_{n+1}$ est vérifiée.

□

Proposition - Détermination d'une probabilité
Soit Ω un univers fini. Tout événement A est fini et est donc le réunion finie des événements élémentaires le constituant, par conséquent :

$$\mathbf{P}(A) = \sum_{\omega\in A} \mathbf{P}(\{\omega\})$$

Si $\Omega = \{\omega_1, \omega_2, \cdots, \omega_n\}$ alors l'application $\tilde{\mathbf{P}} : \Omega \to [0,1]$, $\omega_i \mapsto p_i$ définit une probabilité $\mathbf{P} : A \mapsto \sum_{\omega\in A} \tilde{\mathbf{P}}(\omega)$ sur Ω
si et seulement si

$$\forall i \in [\![1,n]\!], p_i \geqslant 0 \text{ et } \sum_{i=1}^{n} p_i = 1.$$

Démonstration
Notons d'abord que si $A = \{\omega_{i_1} \dots \omega_{i_p}\}$ et $B = \{\omega_{j_1} \dots \omega_{j_q}\}$ sont incompatibles,
alors $\mathbf{P}(A) = \sum_{h=1}^{p} p_{i_h}$, $\mathbf{P}(B) = \sum_{k=1}^{q} p_{j_q}$
et $\mathbf{P}(A\cup B) = \mathbf{P}(\{\omega_{i_1} \dots \omega_{i_p}, \omega_{j_1} \dots \omega_{j_q}\}$ donc $\mathbf{P}(A\cup B) = \sum_{h=1}^{p} p_{i_h} + \sum_{k=1}^{q} p_{j_q} = \mathbf{P}(A) + \mathbf{P}(B)$.
Ensuite, $\mathbf{P}$ est une probabilité sur Ω
si et seulement si $\mathbf{P}(\Omega) = 1$ et pour (A,B) incompatibles, $\mathbf{P}(A\cup B) = \mathbf{P}(A) + \mathbf{P}(B)$
Or $\mathbf{P}(\Omega) = \sum_{\omega\in\Omega} \mathbf{P}(\{\omega\}) = \sum_{i=1}^{n} p_i$.
□

3.3. Suite (dé)croissante d'événements

Ici, on souligne quelques manipulations ordinaires chez les probabilistes :

Evénements/Ensemble

Proposition - Réunion/intersection d'événements
Soit $(A_i)_{i\in I}$ une famille d'événements.

$$\bigcap_{i\in I} A_i = \{\omega\in\Omega \mid \forall\, i\in I, \omega\in A_i\} = [\forall\, i\in I, \omega\in A_i]$$

$$\bigcup_{i\in I} A_i = \{\omega\in\Omega \mid \exists\, i\in I, \omega\in A_i\} = [\exists\, i\in I, \omega\in A_i]$$

On remplace parfois des « il existe » par des « réunions » (et parfois, on agit dans l'autre sens).

(Dé)Croissance

Définition - Suites (dé)croissantes d'événements
On dit que $(A_i)_{i\in\mathbb{N}}$ est une suite croissante (respectivement décroissante) d'événements,
si pour tout $i\in\mathbb{N}$, $A_i \subset A_{i+1}$ ou $A_i \Rightarrow A_{i+1}$ (resp. $A_{i+1}\subset A_i$, $A_{i+1}\Rightarrow A_i$).

Exemple - $E_n = \bigcup_{i=1}^{n} A_i$, $F_n = \bigcap_{i=1}^{n} A_i$
$E_{n+1} = \bigcup_{i=1}^{n+1} A_i = E_n \cup A_{n+1}$, donc $E_n \subset E_{n+1}$.
(E_n) est une suite croissante d'événements.
$F_{n+1} = \bigcap_{i=1}^{n+1} A_i = F_n \cap A_{n+1}$, donc $F_{n+1}\subset F_n$.
(F_n) est une suite décroissante d'événements.

Pour aller plus loin - Théorème de la limite croissante (P)
Si (A_n) est une suite croissante d'événements. Notons $A = \{\omega\in\Omega \mid \exists\, n\in\mathbb{N} \text{ tel que } \omega\in A_n\}$. Nécessairement, pour tout $n\in\mathbb{N}$, $A_n\subset A$. En fait, on a $A = \lim(A_n)$. On écrira : $\mathbf{P}(A) = \lim \mathbf{P}(A_n) = \mathbf{P}(\lim(A_n))$, avec interversion! Ce sera le théorème de la limite croissante pour les probabilités. Il existe le théorème de limite décroissante.

Savoir faire - Suite croissante d'événements et convergence
Si $(A_i)_{i\in\mathbb{N}}\nearrow$, alors on note $B_i = A_{i+1}\setminus A_i$.
Et, $A_{i+1} = A_i \cup B_i$, réunion disjointe, donc $\mathbf{P}(A_{i+1}) = \mathbf{P}(A_i) - \mathbf{P}(B_i)$.
Et ainsi : $\mathbf{P}(B_i) = \mathbf{P}(A_{i+1}) - \mathbf{P}(A_i)$ et par télescopage :

$$\sum_{i=0}^{n-1} \mathbf{P}(B_i) = \mathbf{P}(A_n) - \mathbf{P}(A_0)$$

On passe alors à la « limite monotone ».
De même, pour $(A_i)_{i\in\mathbb{N}}\searrow$, avec $C_i = A_i\setminus A_{i+1}$:

$$\sum_{i=0}^{n-1} \mathbf{P}(C_i) = \mathbf{P}(A_0) - \mathbf{P}(A_n)$$

Pour aller plus loin - Convergence de variables aléatoires
Nous verrons plus loin (au chapitre suivant) comment exploiter ces résultats pour étudier la convergence de suites d'événements, de variables aléatoires plus précisément.

3.4. Exemples de probabilité

Définition - Probabilité uniforme sur un univers fini
On appelle **probabilité uniforme** sur Ω, univers fini, la probabilité telle que tous les événements élémentaires soient équiprobables.
Nécessairement

$$\forall\omega\in\Omega, \mathbf{P}(\{\omega\}) = \frac{1}{\text{Card}\,(\Omega)} \text{ et } \mathbf{P}(A) = \frac{\text{Card}\,(A)}{\text{Card}\,(\Omega)} = \frac{\text{« nb de cas favorables »}}{\text{« nb total de cas »}}$$

on dit aussi qu'on est sous **hypothèse d'équiprobabilité**.

Attention - D'autres probabilités
On peut, bien évidemment définir d'autres probabilités que la probabilité uniforme sur un univers fini.

Exercice
On lance trois dés honnêtes. Calculer :
1. la probabilité d'obtenir au moins un as.
2. la probabilité d'obtenir au moins deux faces identiques.
3. la probabilité que la somme des chiffres soit paire.
4. la probabilité que la somme des chiffres obtenus soit paire et que l'on ait au moins deux faces identiques.

Correction
Nous choisirons la probabilité uniforme définie sur $\Omega = [\![1,6]\!]^3$.
On considère bien des listes, car même si les dés n'étaient pas différentiable pour le joueur, ils restent néanmoins trois dès différents.
$\text{Card}\,(\Omega) = 6^3 = 216$

1. On note A, l'événement : « obtenir au moins un as ».
   On raisonne de manière ensembliste et donc il s'agit de calculer le cardinal de ce sous-ensemble de Ω.
   On raisonne avec le complémentaire : la probabilité de n'avoir aucun as est $5^3 = 125$.
   Donc $\mathbf{P}(A) = 1 - \frac{125}{216} = \frac{91}{216}$
2. On note B, l'événement : « obtenir au moins deux faces identiques ».
   L'événement contraire (ensemble complémentaire) consiste à obtenir une liste de 3 éléments différents. Il y a donc $A_6^3 = 6\times5\times4 = 120$ tirages avec trois nombres différents.
   Donc $\mathbf{P}(B) = 1 - \frac{120}{216} = \frac{96}{216} = \frac{4}{9}$
3. On note C, l'événement : « la somme des chiffres est paire ».
   Il y a plusieurs façons de faire. Une consiste à noter $\Phi : L = (a,b,c) \mapsto L'(7-a, 7-b, 7-c)$.
   On note que Φ est une bijection de Ω sur lui-même (c'est une involution : $\Phi^2 = \text{id}$).
   Par ailleurs
   $(a,b,c)\in C \iff a+b+c$ pair $\iff (7-a)+(7-b)+(7-c) = 21-(a+b+c)$ impair $\iff \Phi(a,b,c)\notin C$
   Donc $\Phi(C) = \overline{C}$, et donc $\text{Card}\,(C) = \text{Card}\,(\overline{C})$ et comme $C\cup\overline{C} = \Omega$, $\mathbf{P}(C) = \frac{1}{2}$

4. On note D : « la somme des chiffres obtenus est paire et au moins deux faces sont identiques. ».
   Si deux faces sont identiques, alors nécessairement leur somme est paire, et donc pour que D soit réalisée, il faut que la dernière face soit paire.
   Pour procéder au dénombrement, nous allons procéder par disjonction de cas :
   — les trois faces sont identiques ; il y a trois situations possibles : $(2,2,2)$, $(4,4,4)$ et $(6,6,6)$.
   — la troisième face est distincte des deux autres, celles-ci sont paires ; il y a $\binom{2}{3}\times 3\times 2 = 18$ cas.
   — la troisième face est distincte des deux autres, celles-ci sont impaires ; il y a $\binom{2}{3}\times 3\times 3 = 27$ cas.
   La probabilité de D est donc $\mathbf{P}(D) = \dfrac{3+18+27}{216} = \dfrac{2}{9}$

Exemple - Probabilité non uniforme

Nous allons ici juste nous baser sur la modélisation pseudo-concrète d'un lancer de deux dés.
On considère deux dés parfaitement équilibré. On peut donc associer au tirage de chacun de ces deux dés une probabilité uniforme.
Notons A_k, l'événement "obtenir k avec un dé". Alors $\mathbf{P}_u(A_k) = \dfrac{1}{6}$ pour tout $k \in \mathbb{N}_6$.
Si l'on additionne les résultats des deux dés, on obtient des valeurs qui varient entre 2 et 12.
Notons B_h, l'événement "obtenir h avec deux dés".
Si l'on considère ou **modélise** que les événements b_h suivent **la loi uniforme à éventualités équiprobables**, alors cela donne $\mathbf{P}_u(B_h) = \dfrac{1}{11}$, pour tout $h \in [\![2,12]\!]$, car $\left|[\![2,12]\!]\right| = 11$.
Or on constate expérimentalement, que ce n'est pas une bonne modélisation.
En réalité, les deux dés étant indépendants et différents, l'on peut convenir que l'ensemble à considérer n'est pas $[\![2,12]\!]$, mais $\{(a,b), a,b \in \mathbb{N}_6\}$. Cet ensemble possède : $6^2 = 36$ couples possibles. Parmi ceux-ci
— un est associé à 2 : $(1,1)$
— deux sont associés à 3 : $(1,2)$ et $(2,1)$
— trois sont associés à 4 : $(1,3)$, $(2,2)$ et $(3,1)$
— quatre sont associés à 5 : $(1,4)$, $(2,3)$, $(3,2)$ et $(4,1)$
…
— un est associé à 12 : $(6,6)$
Dans ce cas, $\Omega = \{(a,b), a,b \in \mathbb{N}_6\}$ et $\mathrm{Card}\Omega = 36$ et $B_h = \{(a,b) \mid a+b = h, a,b \in \mathbb{N}_6\}$,

$$\mathrm{Card}B_h = \begin{cases} |\{(1,h-1),(2,h-2),\dots(h-1,1)\}| & = (h-1)-1+1 \quad \text{si} \quad h-1 \leqslant 6, \\ & = h-1 \qquad\qquad\qquad\quad (i.e.\ h \leqslant 7) \\ |\{(h-6,6),(h-5,5),\dots(6,h-6)\}| & = 6-(h-6)+1 \quad \text{si} \quad h-6 \geqslant 1, \\ & = 13-h \qquad\qquad\qquad\quad (i.e.\ h \geqslant 7) \end{cases}$$

Ce bon modèle conduit donc au second modèle suivant : $(\Omega', \mathscr{P}(\Omega'), \mathbf{P}_{u'})$
où $\Omega' = \{B_2, B_3, B_4, B_5, B_6, B_7, B_8, B_9, B_{10}, B_{11}, B_{12}\}$ et

$$\forall\, h \in [\![2,12]\!] \qquad \mathbf{P}_{u'}(B_h) = \begin{cases} = \dfrac{h-1}{36} & \text{si} \quad h \leqslant 7 \\ = \dfrac{13-h}{36} & \text{si} \quad h \geqslant 7 \end{cases}$$

$\mathbf{P}_{u'}(B_2) = \frac{1}{36}$, $\mathbf{P}_{u'}(B_3) = \frac{1}{18}$, $\mathbf{P}_{u'}(B_4) = \frac{1}{12}$, $\mathbf{P}_{u'}(B_5) = \frac{1}{9}$, $\mathbf{P}_{u'}(B_6) = \frac{5}{36}$, $\mathbf{P}_{u'}(B_7) = \frac{1}{6}$
$\mathbf{P}_{u'}(B_8) = \frac{5}{36}$, $\mathbf{P}_{u'}(B_9) = \frac{1}{9}$, $\mathbf{P}_{u'}(B_{10}) = \frac{1}{12}$, $\mathbf{P}_{u'}(B_{11}) = \frac{1}{18}$, $\mathbf{P}_{u'}(B_{12}) = \frac{1}{36}$.
La loi de probabilité ainsi définie n'est pas uniforme à éventualité équiprobable, mais on montre sans difficulté qu'elle vérifie les axiomes précédents (car elle dérive d'une loi uniforme…) :

1. $\mathbf{P}_{u'}(\Omega) = 1$
2. $\forall\, A$ et B, deux événements incompatibles (disjoints) : $\mathbf{P}_{u'}(A \cup B) = \mathbf{P}_{u'}(A) + \mathbf{P}_{u'}(B)$

Exercice
On lance un dé à six faces numérotées de 1 à 6. Définir une probabilité sur Ω telle que le 6 ait une chance sur deux de sortir (exemple de dé pipé…avec un peu de plomb d'un côté, ça doit pouvoir se faire !)

Correction
On peut prendre $\mathbf{P}(\{6\}) = \frac{1}{2}$ et $\mathbf{P}(\{1\}) = \mathbf{P}(\{2\}) = \mathbf{P}(\{3\}) = \mathbf{P}(\{4\}) = \mathbf{P}(\{(\}) = \frac{1}{10}$.
Il s'agit bien d'une probabilité $\mathbf{P}$ définie que $\Omega = \{1,2,3,4,5,6\}$ avec $\sum_{\omega} \mathbf{P}(\{\omega\}) = 1$

Pour aller plus loin - Avec variables aléatoires
Nous verrons lorsque nous aurons défini les variables aléatoires que la meilleure façon (=plus naturelle) de présenter cette situation est d'exploiter les variables aléatoires.
On note X_k, le résultat du dé k. $X_k \hookrightarrow \mathscr{U}([\![1,6]\!])$.
Et ici, on s'intéresse à $S = X_1 + X_2$.
On trouve alors $S(\Omega) = [\![2,12]\!]$ et $\mathbf{P}(S=h) = \sum_{i=1}^{h-1} \mathbf{P}(X_1 = i)\mathbf{P}(X_2 = h-i)$.
On peut effectuer ce(s) calcul(s)… ou bien penser que cela ressemble au produit de Cauchy et donc considérer le polynôme $P_S = P_{X_1} \times P_{X_2}$, ou $[P_Y]_k = \mathbf{P}(Y=k)$.

Application - Jeu de « Passe-Dix »

On lance trois dés parfaitement équilibrés.
Montrer que la probabilité pour que la somme des points amenés dépasse dix est égale à la probabilité pour que cette somme ne dépasse pas dix.
Ce que nous savons de symétrique repose sur le dé. Nous allons donc considérer l'univers Ω comme le triplet des points amenés donnés par les trois dés (différenciés).
$\mathrm{Card}\Omega = 6^3 = 216$.
Notons E_1 l'événement :"Avoir un total supérieur à 10".
Alors $E_1 = \{(a,b,c) \in \mathbb{N}_6^3 \mid a+b+c \geqslant 11\}$
De même avec E_2 l'événement :"Avoir un total inférieur à 10".
Alors $E_2 = \{(a,b,c) \in \mathbb{N}_6^3 \mid a+b+c \leqslant 10\}$
Notons $\varphi : \Omega \to \Omega$, $(a,b,c) \mapsto (7-a, 7-b, 7-c)$.
Alors $(a,b,c) \in E_1 \Leftrightarrow a+b+c \geqslant 11 \Leftrightarrow 21-(a+b+c) \leqslant 21-11 = 10$
$\Leftrightarrow (7-a)+(7-b)+(7-c) \leqslant 21-11 = 10 \Leftrightarrow \varphi(a,b,c) \in E_2$.
Donc φ établit une bijection de E_1 sur E_2, donc $\mathrm{Card}E_1 = \mathrm{Card}E_2$.
Et finalement, en divisant par $\mathrm{Card}\Omega$, on a $\mathbf{P}_{u'}(E_1) = \mathbf{P}_{u'}(E_2)$

Savoir faire - Exercice de probabilités (1). Choix du modèle

Dans ces premiers exercices de probabilité, il faut avec précision définir le modèle étudié

1. la définition de Ω est très importante. Il faut coller au plus près de la réalisation de l'expérience ; Ω est l'ensemble des réalisations possibles. Vous pouvez commencer par vous demander quelle est la meilleure façon de décrire ces solutions.
   Comment décrire une solution ? Cette description permet-elle de décrire toutes les solutions, et réussit-elle à faire la différence entre deux solutions différentes ?
2. en ce qui concerne la tribu, il s'agit souvent de prendre $\mathscr{P}(\Omega)$.
3. en ce qui concerne le choix de la probabilité, dans cette première catégorie d'exercices, il s'agira souvent de prendre la probabilité uniforme.
   On peut penser à l'exercice du lancer de deux dés…

Exercice
Le chevalier de Méré (personnage historique de la cour de Louis XIV) avance deux règles :
— *« il est avantageux de parier sur l'apparition d'au moins un six en lançant un dé quatre fois de suite »*
— *« il est avantageux de parier sur l'apparition d'au moins un double-six en lançant deux dés vingt-quatre fois de suite »*
Que pensez-vous de ces règles ?

Correction
La première règle est juste, la probabilité de gain vaut $p_1 = 1 - \left(\frac{5}{6}\right)^4 \approx 0,517747$.
La première règle est fausse, la probabilité de gain vaut $p_2 = 1 - \left(\frac{35}{36}\right)^{24} \approx 0,491404$.

3.5. Loi uniforme et simulation avec Python

Avec Python, la seule mesure de probabilité définie sur un ensemble fini est la mesure uniforme.

Informatique - Rappel des commandes en python

Il faut importer la bibliothèque random. Puis la commande `randint(1,n)` tire « au hasard », en suivant une loi uniforme, un nombre entre 1 et n.
Parfois on a besoin de `random` qui tire un nombre aléatoire entre 0 et 1.
Voyons le programme du tirage de deux dés.

Informatique - Simulation du lancer de dés

```
def deux-dés:
   """ résultat du lancer de 2 dés"""
   a:=randint(1,6)+randint(1,6)
   return(a)
```

Attention - Quelle différence?

Comparer les deux commandes suivantes :

`a:=randint(1,6)+randint(1,6)` et `a:=2*randint(1,6)`

Le second tire un seul nombre entre 1 et 6 et le multiplie par deux. Ainsi, on simule ici un tirage uniforme dont les résultats possibles sont $2,4,6,8,10$ et 12.

Analyse - Etude et résultat du programme

Après 1 000 simulations de ce programme, on a obtenu les résultats suivants :

résultat	2	3	4	5	6	7	8	9	10	11	12
quantité	29	53	85	107	140	167	144	113	87	61	14
proportion	0,029	0,053	0,085	0,107	0,140	0,167	0,144	0,113	0,087	0,061	0,014
probabilité	0,027	0,055	0,083	0,111	0,138	0,166	0,138	0,111	0,083	0,055	0,027

Remarque - Différence entre résultat fréquentielle et probabilité a priori

On remarque la différence entre la modélisation, le résultat exact d'**une** expérience et la limite lorsque l'on réalise une infinité de simulations.

Exercice

Programmer en Python deux programmes pour simuler les jeux du chevalier de Méré.
Effectuer 20 simulations de 1000 parties de chacun des jeux.
Que pensez-vous du résultat ?

Correction

```
from random import *

def Meree1(a):
   """Simulations de a lancers de 4 dés"""
   succes=0.0
   for k in range(a):
      d1=randint(1,6)
      d2=randint(1,6)
      d3=randint(1,6)
      d4=randint(1,6)
      if (d1-6)*(d2-6)*(d3-6)*(d4-6)==0:
   succes=succes+1
   return(succes/a)

def Meree2(a):
   """Simulations de a lancers de 24*2 dés"""
   succes=0.0
   for k in range(a):
      succ=0
      for i in range(24):
         d=randint(1,6)+randint(1,6)
         if d==12 :
            succ=1
      if succ==1 :
   succes=succes+1
   return(succes/a)
```

Sur une simulation (avec $n = 10000$), on a trouvé pour Meree1 : $0,509$ et pour Meree2 : $0,4965$.

4. Conditionnement et indépendance

4.1. Conditionnement

Probabilité conditionnelle

Heuristique - Principe du conditionnement

Le but de ce paragraphe est d'expliquer comment tenir compte d'informations déjà connues, mais également de voir comment retrouver des résultats relatifs au "passé".
Par exemple, si on lance deux dés parfaits et que l'on note :
A : « la somme des points obtenus est au moins égale à 10 »,
B : « le premier dé amène un 3 »,
C : « le premier dé amène un 6 ».
Une fois le premier lancer effectué, si B est réalisé, on a des informations sur la réalisation de A... mais également si C est réalisé.
De même, une tierce personne arrivant après l'expérience, à laquelle on dit avoir obtenu une somme égale à 11 peut dire si B a été réalisé.

Définition - Probabilité conditionnelle sachant l'événement A

Soit $(\Omega, \mathbf{P})$ un espace probabilisé fini et B un événement de probabilité non nulle. Soit A un événement quelconque.
On appelle **probabilité de A sachant B** le nombre $\mathbf{P}_B(A) = \dfrac{\mathbf{P}(A\cap B)}{\mathbf{P}(B)}$, également noté $\mathbf{P}(A|B)$.
Alors l'application $\mathbf{P}_B$ est bien une probabilité définie sur Ω.
On a donc $\mathbf{P}(A\cap B) = \mathbf{P}(A)\times \mathbf{P}_A(B)$, valable même si $\mathbf{P}(A) = 0$.

Avec cette définition, il y a un résultat à démontrer : il s'agit bien d'une probabilité

Démonstration

$\mathbf{P}_A(\Omega) = \dfrac{\mathbf{P}(A\cap\Omega)}{\mathbf{P}(A)} = \dfrac{\mathbf{P}(A)}{\mathbf{P}(A)} = 1$.
Si B_1 et B_2 sont incompatibles :

$$\mathbf{P}_A(B_1\cup B_2) = \frac{\mathbf{P}((B_1\cup B_2)\cap A)}{\mathbf{P}(A)} = \frac{\mathbf{P}((B_1\cap A)\cup(B_2\cap A))}{\mathbf{P}(A)}$$

Or $(A\cap B_1)\cap(A\cap B_2) = A\cap B_1\cap B_2 = \emptyset$, donc comme $\mathbf{P}$ est un e mesure de probabilité :

$$\mathbf{P}_A(B_1\cup B_2) = \frac{\mathbf{P}(B_1\cap A)+\mathbf{P}(B_2\cap A)}{\mathbf{P}(A)} = \mathbf{P}_A(B_1)+\mathbf{P}_A(B_2)$$

□

Remarque - Du sens de cette formule

L'application $\mathbf{P}_B$ est bien une probabilité.
Mais pourquoi l'appeler « probabilité conditionnelle à l'événement B » ou encore « probabilité sachant B »?
Si l'on sait que B s'est réalisé, on peut imaginer que l'univers est passé de Ω à B, *par cette information.*
En outre, la réalisation de A correspond alors au cas de réalisation de A et de B.
En terme de cardinal (cas fini), on cherche :

$$\frac{\mathrm{card}(A\cap B)}{\mathrm{card}(B)} = \frac{\frac{\mathrm{card}(A\cap B)}{\mathrm{card}(\Omega)}}{\frac{\mathrm{card}(B)}{\mathrm{card}(\Omega)}} = \frac{\mathbf{P}(A\cap B)}{\mathbf{P}(B)} = \mathbf{P}_B(A)$$

C'est un peu comme une projection de Ω sur B.

Exercice

Considérons une famille dont nous savons qu'elle a deux enfants et supposons que les quatre répartitions possibles, dans l'ordre de naissance, FF, FG, GF, GG sont équiprobables.

1. Quelle est la probabilité que les deux enfants soient des garçons sachant que le cadet est un garçon ?
2. Quelle est la probabilité que les deux enfants soient des garçons sachant qu'il y a au moins un garçon ?
3. Quelle est la probabilité qu'Etienne soit l'ainé de sa fratrie ?

Correction

On note G_i, l'événement « l'enfant i est un garçon ».

1. Deux méthodes :
$$\mathbf{P}_{G_2}(GG) = \frac{\mathbf{P}(GG \cap G_2)}{\mathbf{P}(G_2)} = \frac{\frac{1}{4}}{\frac{2}{4}} = \frac{1}{2}$$
ou bien
$$\mathbf{P}_{G_2}(GG) = \frac{\text{Card}(\{GG\})}{\text{Card}(\{GG, FG\})}$$
.
2. Deux méthodes :
$$\mathbf{P}_{G_1 \cup G_2}(GG) = \frac{\mathbf{P}(GG \cap (G_1 \cup G_2))}{\mathbf{P}(G_1 \cup G_2)} = \frac{\mathbf{P}(GG \cap (G_1 \cup G_2))}{1 - \mathbf{P}(FF)} = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}$$
ou bien
$$\mathbf{P}_{G_1 \cup G_2}(GG) = \frac{\text{Card}(\{GG\})}{\text{Card}(\{GG, FG, GF\})}$$
.

Remarque - Utilisation fréquente

Si $\mathbf{P}(B) \neq 0$, on a
$$\mathbf{P}(A \cap B) = \mathbf{P}_B(A)\mathbf{P}(B) = \mathbf{P}(A|B)\mathbf{P}(B)$$
On reviendra sur cette relation plus bas (formule de Bayes).

Attention - Grosse faute, classique

Il est très important de bien faire la différence entre $\mathbf{P}(A \cap B)$ et $\mathbf{P}_A(B)$.
- $\mathbf{P}(A \cap B)$ est la probabilité d'avoir A et B (partant de rien de réalisé).
- $\mathbf{P}_A(B) = \mathbf{P}(B|A)$ est la probabilité d'avoir B , sachant que A est réalisé

Savoir faire - Suivre un certain formalisme

Dans ce genre d'exercice, la démarche est toujours identique :

1. Présenter les événements importants.
   Ne pas en donner une liste trop grande (on exploitera les notations de complémentaires).
   On fera attention à donner des noms significatifs à ces événements.
2. Exprimer la(les) relation(s) vérifiées par les probabilités connues et à trouver
3. Présenter le modèle « naturelle » donnant les probabilités des événements selon l'énoncé (probabilité uniforme bien choisie, justifiée mais sans excès)

Insistons, il s'agit bien **de définir des événements** A_1 et **pas des probabilités** p_1. On cherche alors $\mathbf{P}(A_1)\dots$

Exercice

Soient $\mathscr{U}_1$ et $\mathscr{U}_2$ deux urnes contenant chacune 2 boules noires et 3 boules blanches. On tire au hasard une boule de l'urne $\mathscr{U}_1$, on note sa couleur et on la met dans $\mathscr{U}_2$. On tire alors au hasard une boule de $\mathscr{U}_2$. Quelle est la probabilité d'obtenir deux fois une boule noire ?

Correction

On note N_i, l'événement « obtenir une boule noire au tirage i ». On cherche donc $\mathbf{P}(N_1 \cap N_2)$.
On supposera un tirage suivant une loi uniforme selon la répartition :
$$\mathbf{P}(N_1 \cap N_2) = \mathbf{P}(N_1) \times \mathbf{P}(N_2|N_1) = \frac{2}{2+3} \times \frac{3}{6} = \frac{1}{5}$$

Formule des probabilités composées

Proposition - Formule des probabilités composées

Soit $(A_i)_{1 \leqslant i \leqslant n}$ une famille d'événements tels que $\mathbf{P}(A_1 \cap \dots \cap A_{n-1}) \neq 0$ alors
$$\mathbf{P}\left(\bigcap_{i=1}^{n} A_i\right) = \mathbf{P}(A_1)\mathbf{P}_{A_1}(A_2)\mathbf{P}_{A_1 \cap A_2}(A_3)\cdots\mathbf{P}_{A_1 \cap \dots \cap A_{n-1}}(A_n)$$

Pour aller plus loin - Moins loin

C'est la fameuse multiplication des branches du lycée

Démonstration

Il s'agit évidemment ici de faire une démonstration par récurrence.

Soit $\forall\, n \in \mathbb{N}^*$, $\mathscr{P}_n$: "$\forall\, (A_i)_{1 \leqslant i \leqslant n}$ telle que $\mathbf{P}(\cap_{i=1}^{n-1} A_i) \neq 0$ alors $\mathbf{P}\left(\cap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} \mathbf{P}_{\cap_{j<1} A_j}(A_i)$".

1. $\mathscr{P}_1$: $\forall\, A \in \Omega$, non négligeable, $\mathbf{P}(A) = \mathbf{P}(A)$.
   Donc $\mathscr{P}_1$ est vraie.
2. Soit $n \in \mathbb{N}^*$ tel que $\mathscr{P}_n$ est vraie.
   Soit $(A_i)_{1 \leqslant i \leqslant n+1}$ une famille d'événement telle que $\mathbf{P}(\cap_{i=1}^{n} A_i) \neq 0$.
   Notons $B = \cap_{i=0}^{n} A_i$: $\mathbf{P}(B \cap A_{n+1}) = \mathbf{P}(B) \times \mathbf{P}_B(A_{n+1})$ (formule de Bayes).
   Mais on peut appliquer à l'événement B le résultat $\mathscr{P}_n$, car $\mathbf{P}(\cap_{i=1}^{n-1} A_i) \neq 0$ (puisque $\mathbf{P}(\cap_{i=1}^{n} A_i) \neq 0$).
   Ainsi $\mathbf{P}(B \cap A_{n+1}) = \left(\prod_{i=1}^{n} \mathbf{P}_{\cap_{j<1} A_j}(A_i)\right) \times \mathbf{P}_B(A_{n+1})$
   en remplaçant B par sa valeur : $\mathbf{P}(\cap_{i=1}^{n+1} A_i)) = \prod_{i=1}^{n+1} \mathbf{P}_{\cap_{j<1} A_j}(A_i)$
   Par conséquent $\mathscr{P}_{n+1}$ est vérifiée, i.e. $\forall\, n \in \mathbb{N}^*$, $\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1}$

On a ainsi montré le résultat par récurrence, pour tout entier. □

Exercice

Une urne contient 4 boules blanches, 3 boules noires. On tire une à une et sans remise 3 boules de l'urne. Quelle est la probabilité d'avoir, dans cet ordre, deux blanches puis une noire ?

Correction

On note B_i, l'événement « avoir une boule blanche au tirage i ».
On cherche
$$\mathbf{P}(B_1 \cap B_2 \cap \overline{B_3}) = \mathbf{P}(B_1)\mathbf{P}_{B_1}(B_2)\mathbf{P}_{B_1 \cap B_2}(\overline{B_3}) = \frac{4}{7} \times \frac{3}{6} \times \frac{3}{5} = \frac{6}{35}$$

Exercice

Une urne contient 10 boules blanches et 10 boules noires.
On effectue une suite de tirage de boules de l'urne, on note sa couleur, puis :
— on l'a remet si elle est noire
— on la garde si elle est blanche
Calculer la probabilité p_n qu'au cours des n premiers tirages, on est retiré une et une seule boule blanche.
Quelle est la limité de p_n ? Donner un équivalent de (p_n).

Correction

Notons B_i l'événement le i^e tirage est celui d'une boule blanche et N_i, l'événement contraire.
Guidé par la question, notons E_k l'événement : parmi les n tirage, seul le k^e a donné une boule blanche.
Autrement dit : $E_k = N_1 \cap N_2 \cap \dots N_{k-1} \cap B_k \cap N_k \cap \dots \cap N_n$.
On cherche en fait $p_n = \sum_{k=1}^{n} \mathbf{P}(E_k)$, car les événements sont indépendants.
Or d'après la formule de probabilités composées :
$$\mathbf{P}(E_k) = \mathbf{P}(N_1) \times \mathbf{P}_{N_1}(N_2) \times \dots \mathbf{P}_{N_1 \cap \dots \cap N_{k-1}}(B_k) \times \dots \mathbf{P}_{N_1 \cap N_2 \cap \dots N_{k-1} \cap B_k \cap N_{k+1} \cap \dots N_{n-1}}(N_n)$$
Enfin choisissons notre modélisation : nous considérons qu'à chaque tirage élémentaire, nous avons une loi uniforme : $\frac{\text{Nombre de cas favorables}}{\text{Nombre total de cas}}$.

1. $\mathbf{P}(N_1) = \frac{10}{20} = \frac{1}{2}$, $\mathbf{P}_{N_1}(N_2) = \frac{10}{20} = \frac{1}{2}$, puisque la boule noire a été remise . . .
   $\mathbf{P}_{N_1 \cap \dots \cap N_{k-2}}(N_{k-1}) = \frac{10}{20} = \frac{1}{2}$, pour les mêmes raisons.
2. $\mathbf{P}_{N_1 \cap \dots \cap N_{k-1}}(B_k) = \frac{1}{2}$, il y a toujours autant de boules blanches (10), que de noires (10).
3. $\mathbf{P}_{N_1 \cap N_2 \cap \dots N_{k-1} \cap B_k}(N_{k+1}) = \dots = \mathbf{P}_{N_1 \cap N_2 \cap \dots N_{k-1} \cap B_k \cap N_{k+1} \cap \dots N_{n-1}}(N_n) = \frac{10}{19}$,
   car il y a une boule blanche de retirée après le k^e tirage.

Et ainsi $\mathbf{P}(E_k) = \left(\frac{1}{2}\right)^k \left(\frac{10}{19}\right)^{n-k} = \left(\frac{10}{19}\right)^n \left(\frac{19}{20}\right)^k$, puis
$$p_n = \sum_{k=1}^{n} \left(\frac{10}{19}\right)^n \left(\frac{19}{20}\right)^k = \left(\frac{10}{19}\right)^n \times \frac{19}{20} \times \frac{1 - \left(\frac{19}{20}\right)^n}{1 - \frac{19}{20}} = 19\left(\frac{10}{19}\right)^n \left(1 - \left(\frac{19}{20}\right)^{n+1}\right).$$
Donc comme $0 < \frac{10}{19} < 1$ et $0 < \frac{19}{20} < 1$, $\lim_n(p_n) = 0$. Et $p_n \sim 19\left(\frac{10}{19}\right)^n$

Formule des probabilités totales

Proposition - Formule des probabilités totales
Soit $(A_i)_{1\leqslant i\leqslant n}$ un système complet d'événements, tous de probabilité non nulle. Alors, pour tout événement B on a

$$\mathbf{P}(B)=\sum_{i=1}^{n}\mathbf{P}(A_i)\mathbf{P}_{A_i}(B)$$

En particulier si $\mathbf{P}(A)\neq 0,1$, $\mathbf{P}(B)=\mathbf{P}(A)\mathbf{P}_A(B)+\mathbf{P}(\overline{A})\mathbf{P}_{\overline{A}}(B)$.

Démonstration
Soit $(\Omega,\mathbf{P})$ un espace probabilité fini.
Soient $(A_i)_{i\in I}$ un système complet d'événements tel que
$\forall\ i\in I,\ \mathbf{P}(A_i)>0\ \forall\ i\in I,\ \mathbf{P}(B\cap A_i)=\mathbf{P}(A_i)\times\mathbf{P}_{A_1}(B)$
(A_i) est un système complet d'événements, donc : $\forall\ i,j\in I,\ A_i\cap A_j=\emptyset$ et $\sum_{i\in I}\mathbf{P}(A_i)=1$.
Et $\left(B\cap A_i\right)_{i\in I}$ est une suite (finie ou non) d'événements incompatibles 2 à 2.
La σ-additivité de $\mathbf{P}$ donne alors : $\mathbf{P}\left(\bigcup_{i\in I}(B\cap A_i)\right)=\sum_{i\in I}\mathbf{P}(B\cap A_i)$.
Or on peut factoriser : $\bigcup_{i\in I}(B\cap A_i)=B\cap(\bigcup_{i\in I}A_i)=B\cap\Omega=B$.
Ainsi $\mathbf{P}(B)=\sum_{i\in I}\mathbf{P}(A_i)\times\mathbf{P}_{A_i}(B)=\sum_{i\in I}\mathbf{P}(B\cap A_i))$ □

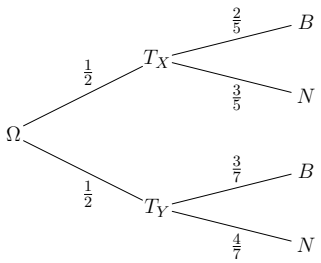
Exercice
Soit n un entier non nul. Une urne $\mathscr{U}$ contient des jetons numérotés : 1 jeton numéroté 1, 2 jetons numérotés 2, ..., n jetons numérotés n. On dispose de n urnes numérotées de 1 à n ; l'urne i contient i boules blanches et $n-i$ noires. On tire un jeton dans $\mathscr{U}$, s'il est numéroté i, on prélève une boule dans l'urne i.
Quelle est la probabilité que la boule prélevée soit blanche ?

Correction
On note A_k, l'événement « le jeton tiré de $\mathscr{U}$ est numéroté k ».
On pourrait prendre une variable aléatoire qui indique le numéro tiré. On note B, l'événement « la boule tirée est blanche ».
La famille $(A_1,A_2,\dots A_n)$ forme un système complet d'événement. Donc

$$\mathbf{P}(B)=\sum_{i=1}^{n}\mathbf{P}(A_i)\mathbf{P}_{A_i}(B)=\sum_{i=1}^{n}\frac{2i}{n(n+1)}\frac{i}{n}=\frac{2}{n^2(n+1)}\sum_{i=1}^{n}i^2=\frac{2n+1}{3n}$$

Attention - Ne pas oublier...
... de préciser (et de démontrer, si nécessaire) que nous sommes en présence d'un système complet d'événements

Savoir faire - Botanique (1)
L'exercice nous montre que cette formule s'applique **à chaque fois que des événements sont liés**. C'est à dire à chaque fois que vous avez envie de faire un arbre…



La somme des probabilités de chaque branche, partant d'une même racine vaut 1.
Le nombre figurant sur chaque branche correspond à la probabilité de l'événement situé à droite de la branche, sachant l'événement situé à gauche.
Attention à ne pas sommer abusivement les probabilités associées aux branches de l'arbre.

Formule de Bayes

Proposition - Formules de Bayes
Soit B, événement de probabilité non nulle.

1. Si A est un événement de probabilité non nulle, alors
$$\mathbf{P}_B(A)=\frac{\mathbf{P}_A(B)\mathbf{P}(A)}{\mathbf{P}(B)}=\frac{\mathbf{P}(B|A)\mathbf{P}(A)}{\mathbf{P}(B)}$$
2. Si $(A_i)_{1\leqslant i\leqslant n}$ est un système complet d'événements, tous de probabilité non nulle. Alors, pour tout j on a
$$\mathbf{P}_B(A_j)=\frac{\mathbf{P}(A_j)\mathbf{P}_{A_j}(B)}{\sum_{i=1}^{n}\mathbf{P}(A_i)\mathbf{P}_{A_i}(B)}=\frac{\mathbf{P}(B|A_j)\mathbf{P}(A_j)}{\sum_{i=1}^{n}\mathbf{P}(B|A_i)\mathbf{P}(A_i)}$$

Démonstration
Il s'agit de réécrire la définition des probabilités conditionnelles de deux façons. □

Savoir faire - Botanique (2)
L'exercice nous montre que cette formule s'applique à chaque fois que vous avez envie de faire un arbre… et que la question posée remonte la chronologie naturelle de l'arbre.
Il s'agit de calculer la probabilité d'un premier événement, sachant que c'est le deuxième qui est en fait réalisé…

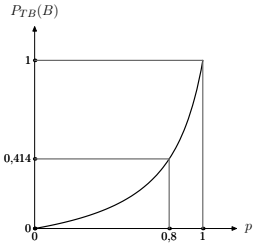
Exemple - QCM
Dans un questionnaire à choix multiples, les candidats doivent choisir parmi m réponses. Chaque candidat est soit complètement ignorant et choisit alors ses réponses au hasard, soit omniscient et connaît alors les bonnes réponses.
Si la proportion des candidats omniscients est p, quelle est la probabilité que parmi les personnes ayant trouvé la bonne réponse à une question, le candidat est agi au hasard ?

1. *Etudier au niveau des événements (ensemble)*
   (a) *Définition des événements élémentaires, selon l'énoncé*
   Notons I, l'événement être ignorant et O, l'événement contraire.
   Notons C, l'événement avoir tout juste et F, l'événement contraire.
   (b) *Annoncer ce que l'on cherche (événement)*
   On nous demande de trouver $\mathbf{P}_C(I)$.
2. *Faire l'étude des probabilités (numérique)*
   (a) *Expliciter les probabilités connues*
   On sait par hypothèse que $\mathbf{P}(I)=1-p$ et $\mathbf{P}(O)=p$ puis $\mathbf{P}_O(C)=1$ et $\mathbf{P}_I(C)=\frac{1}{m}$, puisqu'il choisit au hasard une réponse parmi les m possibles.
   I et O sont contraires donc que $\mathbf{P}_C(I)+\mathbf{P}_C(O)=1$,

(b) *Travailler numériquement les formules du calcul de probabilité pour obtenir ce que l'on cherche*
La formule des probabilités totales donne : $\mathbf{P}(C) = \mathbf{P}(I)\mathbf{P}_I(C) + \mathbf{P}(O)\mathbf{P}_O(C)$.
Donc $\mathbf{P}(C) = (1-p)\dfrac{1}{m} + p \times 1 = \dfrac{1+(m-1)p}{m}$.
Puis avec la formule de Bayes : $\mathbf{P}_C(I) = \dfrac{\mathbf{P}_I(C)\mathbf{P}(I)}{\mathbf{P}(C)} = \dfrac{\frac{1-p}{m}}{\frac{1+(m-1)p}{m}} = \dfrac{1-p}{1-p+mp}$

Exercice
Un taxi est impliqué dans un carambolage de nuit. Deux compagnies de taxi, les Rouges et les Bleus, opèrent en ville. Nous savons que 85% des taxis en ville sont Rouge et 15% sont Bleus.
1. Quelle est la probabilité que le taxi impliqué dans l'accident soit un Bleu ?
Quelques heures plus tard nous apprenons qu'un témoin a identifié le taxi responsable comme Bleu. Le tribunal a testé la fiabilité des témoignages dans ce type de circonstances (accident de nuit) et en a conclu que les témoins identifient correctement les couleurs avec une probabilité p et se trompent avec une probabilité $1-p$.
Nous définissons les événements :
— B est l'événement :"Le taxi est bleu", son complémentaire est R.
— TB est l'événement :"Le témoignage a affirmé que le taxi est bleu", son complémentaire est TR.
2. Quelle est la probabilité pour que le taxi impliqué dans l'accident soit un Bleu ?
On étudiera les situations : $p = 0$, $p = 1$ et $p = 0,8$ et on pourra tracer $\mathbf{P}_{TB}(B)$ en fonction de p.
3. Que se passe-t-il si n témoins indépendants affirment qu'il s'agit d'un taxi bleu ?

Correction
Soit $(\Omega, \mathscr{A})$ un espace probabilisable adapté. ...
1. Ce que l'on sait : $p_1 = \mathbf{P}(B) = 0,15$ et $\mathbf{P}(R) = 0,85$.
2. Et ce que l'on cherche c'est $p_2 = \mathbf{P}_{TB}(B) = \dfrac{\mathbf{P}(TB \cap B)}{\mathbf{P}(TB)} = \dfrac{\mathbf{P}(TB \cap B)}{\mathbf{P}(TB \cap B) + \mathbf{P}(TB \cap R)}$.
Donc $p_2 = \dfrac{\mathbf{P}_B(TB)\mathbf{P}(B)}{\mathbf{P}_B(TB)\mathbf{P}(B) + \mathbf{P}_R(TB)\mathbf{P}(R)}$.
Or $\mathbf{P}_B(TB) = p$ c'est la probabilité que le témoignage soit juste.
Or $\mathbf{P}_R(TB) = 1-p$ c'est la probabilité que le témoignage soit faux.
Ainsi $p_2 = \dfrac{p \times 0,15}{p \times 0,15 + (1-p) \times 0,85} = \dfrac{0,15p}{0,85 - 0,7p} = \dfrac{3p}{17 - 14p}$
Pour $p = 0$: $p_2 = 0$, pour $p = 1$: $p_2 = 1$, pour $p = 0,8$: $p_2 = \dfrac{12}{29} \approx 0,414$



3. On a alors $\mathbf{P}_{TB_n}(B) = \dfrac{3p^n}{17(1-p)^n + 3p^n} = \dfrac{1}{1 + \frac{17}{3}(\frac{1-p}{p})^n}$.
Si $\frac{1-p}{p} < 1 \Leftrightarrow p > \dfrac{1}{2}$ alors $\mathbf{P}_{TB_n}(B) \to 1$.
Si $\frac{1-p}{p} = 1 \Leftrightarrow p = \dfrac{1}{2}$ alors $\mathbf{P}_{TB_n}(B) = \dfrac{3}{20} = 0.15$. (le témoignage ne sert à rien)
Si $\frac{1-p}{p} > 1 \Leftrightarrow p < \dfrac{1}{2}$ alors $\mathbf{P}_{TB_n}(B) \to 0$.
Le résultat semble très logique !

Exercice
Une usine possède trois ateliers de production de poupées : A, B et C.
L'atelier A est responsable de 60% de la production de poupées de l'usine, B de 25% et C de 15%.
Le technicien qualité de l'entreprise estime que
— A la sortie de A, il y a 1 poupée barbue sur 1000.
— A la sortie de B, il y a 50 poupées barbues sur 1000.
— A la sortie de C, il y a 10 poupées barbues sur 1000.

1. Calculer la probabilité qu'une poupée prise au hasard dans les stocks de l'usine soit barbue ?
2. Manque de bol !, le technicien qualité est tombé sur une poupée barbue. Calculer la probabilité que celle-ci soit issue de l'usine A. De même pour l'usine B. De même pour l'usine C.

Correction
Soit a l'événement "la poupée est issue de l'usine A".
Soit b l'événement "la poupée est issue de l'usine B".
Soit c l'événement "la poupée est issue de l'usine C".
Soit $barbe$ l'événement la poupée est barbue.
1. (a,b,c) est un système complet d'événements, donc $\mathbf{P}(barbe) = \mathbf{P}(a)\mathbf{P}_a(barbe) + \mathbf{P}(b)\mathbf{P}_b(barbe) + \mathbf{P}(c)\mathbf{P}_c(barbe)$
Modélisons que la loi de probabilité suit la répartition statistique. Donc d'après les hypothèses du problème : $\mathbf{P}(a) = 0,6$, $\mathbf{P}(b) = 0,25$ et $\mathbf{P}(c) = 0,15$.
Et aussi : $\mathbf{P}_a(barbe) = 0,001$, $\mathbf{P}_b(barbe) = 0,05$ et $\mathbf{P}_c(barbe) = 0,01$.
Finalement $\mathbf{P}(barbe) = 0,0006 + 0,0125 + 0,0015 = 0,0146$,
la probabilité que la poupée soit barbue est $1,46\%$

2. On cherche ici $\mathbf{P}_{barbe}(a)$, $\mathbf{P}_{barbe}(b)$ et $\mathbf{P}_{barbe}(c)$.
$\mathbf{P}_{barbe}(a) = \dfrac{\mathbf{P}(a) \times \mathbf{P}_a(barbe)}{\mathbf{P}(barbe)} = \dfrac{0,0006}{0,0146} \approx 4,1\%$
$\mathbf{P}_{barbe}(b) = \dfrac{\mathbf{P}(b) \times \mathbf{P}_b(barbe)}{\mathbf{P}(barbe)} = \dfrac{0,0125}{0,0146} \approx 85,6\%$
$\mathbf{P}_{barbe}(c) = \dfrac{\mathbf{P}(c) \times \mathbf{P}_c(barbe)}{\mathbf{P}(barbe)} = \dfrac{0,0015}{0,0146} \approx 10,3\%$
On vérifie que la somme est bien égale à 1.

Attention - $\mathbf{P}_a(barbe)$
Notons que dans cet exercice (*et dans la plupart*), ce qui nous intéresse en réalité c'est d'exploiter cette formule des probabilités totales. Et dans ces cas, la probabilité conditionnelle ne s'obtient pas par un calcul forcé du genre $\mathbf{P}_a(barbe) = \frac{\mathbf{P}(barbe)}{\mathbf{P}(a)}$, mais **il est donné dans les hypothèses de l'énoncé**!

4.2. Indépendance en probabilité

Indépendance(s) en probabilité

Définition - Indépendance (en probabilité)
Deux événements d'un espace probabilisé fini (Ω, P) sont dits **P**-indépendants (ou indépendants en probabilité) si $\mathbf{P}(A \cap B) = \mathbf{P}(A)\mathbf{P}(B)$.
Si le contexte est clair, on parle d'indépendance sans préciser la probabilité **P** considérée.

Ce nouveau point de vue a peut-être pas plus de sens

Proposition - Autre point de vue
Si $\mathbf{P}(A) \neq 0$, A et B sont indépendants (pour **P**) si et seulement si $\mathbf{P}_A(B) = \mathbf{P}(B)$.

Démonstration
Il suffit d'écrire la formule □

Attention - Dépendance des événements, a priori selon la probabilité considérée

Cette notion dépend de la probabilité considérée sur $(\Omega, \mathscr{A})$.

Exemple - Illustration de la remarque précédente

On considère l'expérience du lancer de dé à 6 faces, donc $\Omega = \mathbb{N}_6 = [\![1;6]\!]$.
On considère les deux événements A : " obtenir 4 ou 5" et B : " obtenir 5 ou 6".
Donc l'événement $A \cap B$ est " obtenir 5".
Ces deux événements sont-ils indépendants ? Cela dépendant de la mesure de probabilité.
Considérons $\mathbf{P}_1$, la probabilité uniforme.

Alors $\mathbf{P}_1(A) = \frac{|A|}{|\Omega|} = \frac{1}{3}$, de même $\mathbf{P}_1(B) = \frac{1}{3}$ et $\mathbf{P}_1(A \cap B) = \frac{1}{6}$.

$\mathbf{P}_1(A) \times \mathbf{P}_1(B) = \frac{1}{9} \neq \mathbf{P}_1(A \cap B)$: A et B ne sont pas indépendants pour $\mathbf{P}_1$.

Considérons $\mathbf{P}_2$, la probabilité "dé truqué" suivante :

$\mathbf{P}_2(\{6\}) = \frac{1}{3}$, $\mathbf{P}_2(\{5\}) = \mathbf{P}_2(\{4\}) = \frac{1}{6}$ et $\mathbf{P}_2(\{3\}) = \mathbf{P}_2(\{2\}) = \mathbf{P}_2(\{1\}) = \frac{1}{9}$.

Alors $\mathbf{P}_2(A) = \mathbf{P}_2(\{4\}) + \mathbf{P}_2(\{5\}) = \frac{1}{3}$, de même $\mathbf{P}_2(B) = \frac{1}{6} + \frac{1}{3} = \frac{1}{2}$ et $\mathbf{P}_1(A \cap B) = \mathbf{P}_2(\{5\}) = \frac{1}{6}$.

d'où $\mathbf{P}_1(A) \times \mathbf{P}_1(B) = \frac{1}{3} \times \frac{1}{2} = \mathbf{P}_1(A \cap B)$: A et B sont indépendants pour $\mathbf{P}_2$.

On vérifie qu'il s'agit bien d'une mesure de probabilité : $3 \times \frac{1}{9} + 2 \times \frac{1}{6} + \frac{1}{3} = \frac{3}{3} = 1$

Attention - Ne pas confondre incompatibles et indépendants

On fera bien attention à ne pas confondre :

— *A et B sont incompatibles* :
cette notion ne dépend pas de la probabilité : $A \cap B = \emptyset$.
cela sert pour calculer $\mathbf{P}(A \cup B)$
(on parle aussi d'événements disjoints avec une vision ensembliste).

— *A et B sont indépendants* :
cette notion dépend de la probabilité : $\mathbf{P}(A \cap B) = \mathbf{P}(A) \times \mathbf{P}(B)$.
cela sert pour calculer $\mathbf{P}(A \cap B)$

En fait deux événements (non négligeables) incompatibles ne peuvent pas être indépendants.
Si l'un se réalise, alors l'autre ne peut pas se réaliser…

Définition - Cas de plus de 2 événements

Soit $(\Omega, \mathbf{P})$ un espace de probabilité fini

1. n événements $A_1, \dots, A_n$ sont dits deux à deux indépendants si
$$\forall i, j \in [\![1, n]\!],\ i \neq j,\ \mathbf{P}(A_i \cap A_j) = \mathbf{P}(A_i)\mathbf{P}(A_j).$$
2. n événements $A_1, \dots, A_n$ sont dits mutuellement indépendants si
$$\forall J \subset [\![1, n]\!],\ \mathbf{P}\left(\bigcap_{j \in J} A_j\right) = \prod_{j \in J} \mathbf{P}(A_j)$$

Proposition - Equivalence des complémentaires

A, B sont indépendants $\Rightarrow$ $A, \overline{B}$ sont indépendants, $\overline{A}, \overline{B}$ sont indépendants.
Plus généralement :
Soient $A_1, A_2, \dots, A_n$ des événements mutuellement indépendants.
Posons pour tout $i \leqslant n$, $B_i = A_i$ ou $\overline{A_i}$.
Alors $B_1, B_2, \dots, B_n$ sont mutuellement indépendants.

Pour aller plus loin - Avec le crible

Notons $A = \bigcap_{i \in I} A_i$ *et* $B = \bigcap_{j \in J} \overline{A_j}$, *donc* $\overline{B} = \bigcup_{j \in J} A_j$.
$(B, \overline{B})$ *est un système complet d'événements :*
$\mathbf{P}(A) = \mathbf{P}(A \cap B) + \mathbf{P}(A \cap \overline{B})$.

$$\mathbf{P}(A \cap B) = \mathbf{P}(A) - \mathbf{P}(A \cap \overline{B}) = \mathbf{P}(A) - \mathbf{P}(A \cap (\bigcup_{j \in J} A_j))$$

On applique alors la méthode du crible :

$$\mathbf{P}(A \cap B) = \sum_{k=0}^{|J|} (-1)^k \sum_{K \in \binom{J}{k}} \mathbf{P}(A \bigcap \cap_{k \in K} A_k)$$

$$\mathbf{P}(A \cap B) = \sum_{k=0}^{|J|} (-1)^k \sum_{K \in \binom{J}{k}} \mathbf{P}(A) \times \prod \mathbf{P}(A_k)$$

Démonstration

• Commençons par le cas de deux événements.
Comme $A = (A \cap B) \cup (A \cap \overline{B})$ et que cette réunion est disjointe :

$$\mathbf{P}(A \cap \overline{B}) = \mathbf{P}(A) - \mathbf{P}(A \cap B) = \mathbf{P}(A)[1 - \mathbf{P}(B)]$$

car $\mathbf{P}(A \cap B) = \mathbf{P}(A)\mathbf{P}(B)$, puisque A et B sont indépendants. Et donc :

$$\mathbf{P}(A \cap \overline{B}) = \mathbf{P}(A)\mathbf{P}(\overline{B})$$

Et en appliquant la même implication à $\overline{B}, A$, indépendants, on trouve $\overline{B}, \overline{A}$ indépendants.
• Généralisons à k événements.
Soit $n \in \mathbb{N}$ fixé.
Posons, pour tout $p \in \{0, 1, \dots n\}$, $\mathscr{P}_p$: « $\forall\ J \subset \mathbb{N}_n$ et $\text{card}(J) = p$, $\forall\ I \subset \mathbb{N}_n \setminus J$, $(A_i, B_j)_{i \in I, j \in J}$ sont mutuellement indépendants. »

— Le cas $\mathscr{P}_0$ est vraie par hypothèse.

— Soit $p < n$. Supposons que $\mathscr{P}_p$ est vraie.
Soit $J \subset \mathbb{N}_n$ et $\text{card}(J) = p + 1$.
Soient $A_1, A_2, \dots, A_n$ des événements mutuellement indépendants.
Notons, enfin, $j_1 = \min J$ (j_1 existe bien car $\text{card}(J) = p + 1 \geqslant 1$) et $J' = J \setminus \{j_1\}$.
Soit $I \in \mathbb{N}_n \setminus J$.

$$\left(\cap_{i \in I} A_i\right) \bigcap \left(\cap_{j \in J'} \overline{A_j}\right) = \left(\cap_{i \in I} A_i \bigcap \cap_{j \in J'} \overline{A_j} \cap \overline{A_{j_1}}\right) \bigcup \left(\cap_{i \in I} A_i \bigcap \cap_{j \in J} \overline{A_j} \cap A_{j_1}\right)$$

Cette réunion est disjointe :

$$\mathbf{P}\left(\cap_{i \in I} A_i \bigcap \cap_{j \in J} \overline{A_j}\right) = \mathbf{P}\left(\cap_{i \in I} A_i \bigcap \cap_{j \in J'} \overline{A_j}\right) - \mathbf{P}\left(\cap_{i \in I \cup \{j_1\}} A_i \bigcap \cap_{j \in J'} \overline{A_j}\right) = \prod_{i \in I} \mathbf{P}(A_i) \prod_{j \in J'} \mathbf{P}(\overline{A_j}) - \prod_{i \in I \cup \{j_1\}} \mathbf{P}(A_i) \prod_{j \in J'} \mathbf{P}(\overline{A_j})$$

d'après $\mathscr{P}_k$ (appliqué deux fois).

$$\mathbf{P}\left(\cap_{i \in I} A_i \bigcap \cap_{j \in J} \overline{A_j}\right) = \prod_{i \in I} \mathbf{P}(A_i) \prod_{j \in J'} \mathbf{P}(\overline{A_j})(1 - \mathbf{P}(A_{j_1})) = \prod_{i \in I} \mathbf{P}(A_i) \prod_{j \in J'} \mathbf{P}(\overline{A_j}) \times \mathbf{P}(\overline{A_{j_1}}) = \prod_{i \in I} \mathbf{P}(A_i) \prod_{j \in J} \mathbf{P}(\overline{A_j})$$

Donc $\mathscr{P}_{k+1}$ est vraie.

□

Remarque - Une implication

L'indépendance mutuelle $\Rightarrow$ l'indépendance deux à deux.
Mais la réciproque est fausse (voir exercice plus bas).

Exercice
Démontrer l'implication

Correction
L'ensemble des sous-ensemble de $[\![1, n]\!]$ à deux éléments est une partie de l'ensemble des sous-ensemble de $[\![1, n]\!]$ (sans autre condition).

Exercices

Exercice
On tire une carte d'un jeu de 32 cartes.
Les événements A « la carte tirée est un pique » et B « la carte tirée est un roi » sont-ils indépendants ?

Correction
On suppose que $\mathbf{P}$ est la loi uniforme :

$$\mathbf{P}(A) = \frac{8}{32} = \frac{1}{4} \qquad \mathbf{P}(B) = \frac{4}{32} = \frac{1}{8}$$

Alors que

$$\mathbf{P}(A \cap B) = \frac{1}{32} = \frac{1}{4} \times \frac{1}{8} = \mathbf{P}(A) \times \mathbf{P}(B)$$

Donc A et B sont indépendants (pour cette loi…)

Exercice
On lance deux dés parfaits. On note :

— A_1 : « le premier dé amène un nombre pair »,
— A_2 : « le deuxième dé amène un nombre pair »,
— A_3 : « la somme des nombres obtenus est paire ».

Les événements A_1, A_2, A_3 sont-ils mutuellement indépendants ? Et deux à deux ?

Correction
Toujours avec le modèle uniforme, on trouve :

$$\mathbf{P}(A_1) = \frac{18}{36} = \mathbf{P}(A_2) \qquad \mathbf{P}(A_3) = \frac{18}{36} = \frac{1}{2}$$

$$\mathbf{P}(A_1 \cap A_2) = \frac{9}{36} = \frac{1}{4} = \mathbf{P}(A_1)\mathbf{P}(A_2)$$

$$\mathbf{P}(A_1 \cap A_3) = \frac{9}{36} = \frac{1}{4} = \mathbf{P}(A_2 \cap A_3)$$

Et

$$\mathbf{P}(A_1 \cap A_2 \cap A_3) = \mathbf{P}(A_1 \cap A_2) = \frac{1}{4} \neq \mathbf{P}(A_1)\mathbf{P}(A_2)\mathbf{P}(A_3)$$

Par conséquent, les événements A_1, A_2 et A_3 sont indépendants 2 à 2 mais pas mutuellement indépendants.

Exercice

On permute au hasard les chiffres $1, 2, 3, 4$. On considère les événements

— A : « 1 est avant 2 »

— B : « 3 est avant 4 ».

A et B sont-ils indépendants ?

Correction

Pour des raisons de symétries : $\mathbf{P}(A) = \mathbf{P}(B) = \frac{1}{2}$.

$$\mathbf{P}(A \cap B) = \frac{\text{Card}\,(\{1,2,3,4\},\{1,3,2,4\},\{1,3,4,2\},\{3,4,1,2\},\{3,1,4,2\},\{3,1,2,4\})}{4!} = \frac{1}{4}$$

Les événements A et B sont indépendants.

Exercice

On considère une famille ayant n enfants ($n \geqslant 2$). On suppose que toutes les répartitions possibles des sexes des n enfants sont équiprobables.
Les événements « la famille a des enfants des deux sexes » et « la famille a au plus une fille » sont-ils indépendants ?

Correction

On note A et B ces événements.

$$\mathbf{P}(A) = 1 - \mathbf{P}(\overline{A}) = 1 - \frac{1}{2^{n-1}} \qquad \mathbf{P}(B) = \frac{\binom{n}{0} + \binom{n}{1}}{2^n} = \frac{n+1}{2^n}$$

Alors que

$$\mathbf{P}(A \cap B) = \frac{n}{2^n} \neq \mathbf{P}(A)\mathbf{P}(B)$$

sauf si $2^{n-1}n = (n+1)(2^{n-1}-1) = 2^{n-1}n + 2^{n-1} - (n+1)$ i.e. $2^{n-1} = n+1$, i.e. $n = 3$

5. Bilan

Synthèse

⇝ De nombreuses phénomènes ne peuvent s'étudier (aujourd'hui) qu'en introduisant le « hasard » (réel ou plus souvent par manque d'informations). Les mathématiciens proposent alors de modéliser numériquement ces phénomènes, en s'appuyant sur un univers Ω (de tous les cas possibles, imaginés), une tribu des événements probabilisables (souvent $\mathscr{P}(\Omega)$) et une mesure de probabilité $\mathbf{P}$ qui indique la potentielle réalisation de l'événement.
Ce triplet doit vérifier des propriétés mathématiques précises (σ-additivité). Elles sont dans un premier temps associées à la réunion d'ensembles.

⇝ Nous étudions de nombreux exemples dont la probabilité uniforme sur un univers fini, mais également d'autres exemples (même si le programme officiel nous limite en première année qu'à des situations où Ω est fini).

⇝ Après la modélisation, la seconde idée forte du cours est la notion de conditionnement/(in)dépendance entre événements. Elle permet d'étudier l'intersection d'événements en mesurant la dépendance mutuelle entre ces événements.
On exploite ces idées dans trois directions : successions d'événements (formule des probabilités composées), partition de l'univers (formule des probabilités totales) ou formule des Bayes (inverser l'ordre logique de la corrélation).

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Une bonne habitude à prendre de suite
— Savoir-faire - Suite croissante d'événements et convergence
— Savoir-faire - Exercice de probabilité (1). Choix du modèle.
— Savoir-faire - Suivre un certain formalisme
— Savoir-faire - Botanique (1)
— Savoir-faire - Botanique (2)

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$(\Omega, \mathscr{A}, \mathbf{P})$	Espace de probabilité (triplet)	Ω est un ensemble, $\mathscr{A} \subset \mathscr{P}(\Omega)$ et $\mathbf{P} : \mathscr{A} \to [0,1]$ σ-additive	$\mathbf{P}(\Omega) = 1$, $\mathbf{P}(A \uplus B) = \mathbf{P}(A) + \mathbf{P}(B)$.
A p.s.	L'événement A est vrai presque sûrement	$\mathbf{P}(A) = 1$	.
$\mathbf{P}_B : A \mapsto \dfrac{\mathbf{P}(A \cap B)}{\mathbf{P}(B)}$	Probabilité de A sachant (ou conditionné à la réalisation de l'événement) B	$\mathbf{P}_B$ est une mesure de probabilité	Parfois également noté $\mathbf{P}(\cdot\|B)$.

Retour sur les problèmes

149. Cours

150. Cours. Le lien qui lie les fréquentialistes et les subjectivistes est porté par tous les théorèmes limites. En particulier la loi faible des grands nombres dont on parlera au chapitre suivant.

151. Les simulations informatiques permettent de créer une situation comparable. La répétition d'un nombre très grand de cas, permet d'avoir une approche assez intéressante de la valeur cherchée (en exploitant toujours les théorèmes de convergence).
Simuler du hasard n'est pas vraiment possible classiquement (quantiquement, il semble que si). On exploite en fait des phénomènes chaotiques (grande sensibilité aux conditions initiales), mais finalement un lancer de dé est bien également un phénomène chaotique…

152. Cours

153. L'indépendance se définit mathématiquement avec précision. Cela rappelle notre appréciation naturelle du phénomène, mais est-ce toujours comme chacun l'entend?

154. Cours. Il manque la connaissance de la part dans la population des cas malades et des cas non malades…

Chapitre 36

Variables aléatoires (cas Ω fini)

Résumé -

La seconde grande idée du calcul des probabilités (après le conditionnement) est la notion de variables aléatoires. Il existe plusieurs façons de comprendre ce genre de variables. La manière rigoureuse est celle d'une application réciproque ou d'une classe d'équivalence puisqu'elle conduit à une partition de Ω, dont un système de représentant est $X(\Omega)$. Mais ce n'est pas la manière intuitive du physicien ou du probabiliste qui voit la ***variable aléatoire comme un nombre potentiel****. Ce nombre est multiple et prend telle ou telle valeur en fonction des événements de l'univers (on tient compte alors de la probabilité de réalisation).*
C'est typiquement le résultat chiffré d'une expérience de physique, dont la réalisation une seconde fois montre une certaine variabilité…
La question qui se pose, une fois que l'on maîtrise bien cette notion de variables aléatoires est celle de l'addition, multiplication (et autres opérations…) de variables aléatoires. Il faut dans ce cas, toujours commencer par étudier le couple de variables aléatoires dont on veut faire l'addition !

Sommaire

1. Problèmes 710
2. Variable aléatoire 711
2.1. Quelques définitions 711
2.2. Loi de probabilité 712
2.3. Lois usuelles 715
3. Couples de variables aléatoires 716
4. Indépendance 719
4.1. Indépendance de deux variables aléatoires 719
4.2. Indépendance de plusieurs variables aléatoires . . . 719
4.3. Opération de variables aléatoires (indépendantes) . 722
4.4. Suite de variables aléatoires 724
5. Moments d'une variable aléatoire réelle finie 724
5.1. Espérance 724
5.2. Variance (d'une variable aléatoire) 728
5.3. Covariance (de deux variables aléatoires) 731
6. Bilan 734

1. Problèmes

Problème 155 - Variable aléatoire

Une variable peut prendre plusieurs valeurs, potentiellement, chacune avec une probabilité (a priori, ou non) fixé. Cette variable particulière comme par exemple la note à un devoir : au hasard elle est comprise entre 0 et 20 s'appelle une variable aléatoire.
On peut alors associer à chaque valeur, une probabilité, mais plus exactement un événement de l'univers. Donc les variables aléatoires partitionnent l'univers. On peut donc créer une relation d'équivalence $\asymp$: $\omega \asymp \omega'$, si pour ces deux issues de l'univers Ω, la variable aléatoire prend la même valeur.
Mais on a vu que dans ce cas là, une autre stratégie consiste à associer à la relation $\asymp$, une fonction f sur Ω, telle que : $\omega \asymp \omega' \iff f(\omega) = f(\omega')$.
Quelle définition (mathématique, formelle) de variable aléatoire est la plus naturelle et pratique pour définir un nombre potentiel?

Problème 156 - Lois de probabilité fréquemment rencontrées

A une variable aléatoire, on associe une distribution de probabilité.
Quelles sont les distributions les plus courantes? A quels types d'expériences aléatoires sont-elles associées?

Problème 157 - Espérance, variance…

Souvent, on ne peut se contenter d'une distribution de probabilité pour exprimer le résultat numérique d'une expérience. Il faut pouvoir résumer cette variable aléatoire?
Qu'est-ce que l'espérance mathématique d'une variable aléatoire? Pourquoi résume-t-elle d'une certaine façon la valeur de l'expérience? Quelles sont les autres nombres à ajouter?

Problème 158 - Citation de Poincaré

Que pensez-vous de la citation de Henri Poincaré (Calcul des probabilités) :
« Vous me demandez de vous prédire les phénomènes qui vont se produire. Si, par malheur, je connaissais les lois de ces phénomènes, je ne pourrais y arriver que par des calculs inextricables et je devrais renoncer à vous répondre; mais, comme j'ai la chance de les ignorer, je vais vous répondre tout de suite. Et, ce qu'il y a de plus extraordinaire, c'est que ma réponse sera juste. »

Problème 159 - Deux variables aléatoires

Si l'expérience aléatoire conduit à la construction de deux (ou plus) variables aléatoires. Comment faire pour les étudier ensemble?
On peut avoir à les considérer comme une base d'autres résultats possibles (d'autres variables aléatoires).

Problème 160 - Produit scalaire

Ou bien, la question se pose parfois de mesurer la corrélation entre ces deux variables aléatoires. Sont-elles liées? Par exemple : y a-t-il un lien entre fumer et développer un cancer? Entre ne pas porter un masque et être touché par la Covid?
On crée en probabilité-statistique un objet appelé coefficient de corrélation entre deux variables aléatoires : $\rho(X,Y)$.
Il mesure si X et Y sont proches : $\rho(X,Y)=1$, indépendants (ou quasiment) : $\rho(X,Y)=0$ ou sont plutôt opposées : $\rho(X,Y)=-1$.
Cela nous rappelle le produit scalaire (vu en physique et plus tard en maths) $\vec{x}\cdot\vec{y}$ qui mesure d'une certaine façon le lien entre $\vec{x}$ et $\vec{y}$ (modulo leurs normes). Y a-t-il un rapport entre la corrélation et la notion de produit scalaire.

2. Variable aléatoire

2.1. Quelques définitions

Soit Ω un univers fini lié à une expérience aléatoire.

Définition - Variable aléatoire
On appelle variable aléatoire (v.a.) sur Ω toute application $X:\Omega\to E$, où E est un ensemble. Dans le cas où $E\subset\mathbb{R}$, on parle de variable aléatoire réelle.
$X(\Omega)$ désigne donc l'ensemble image, c'est-à-dire les valeurs que prend l'application X. Cet ensemble est ici fini (car Ω fini), on dit alors que X est une v.a. discrète finie.

Pour aller plus loin - Variable alétoire sur un espace de probabilité infini
Lorsque la tribu définie sur Ω pour $\mathbf{P}$ est plus compliqué que $\mathscr{P}(\Omega)$; pour créer une variable aléatoire réelle, il faut exiger en fait que pour tout I intervalle de $\mathbb{R}$, $X^{-1}(I)=\{\omega\in\Omega\mid X(\omega)\in I\}$ est un élément de la tribu.
Cela, afin de pouvoir écrire et calculer : $\mathbf{P}(X^{-1}(I))$, pour tout I raisonnable

La stabilité linéaires des applications permet d'affirmer :

Proposition - Stabilité linéaire
Soient X,Y deux variables aléatoires réelles sur Ω, $\lambda\in\mathbb{R}$. Alors $X+Y$, XY et λX sont des variables aléatoires sur Ω.

Proposition - Composition
Soit X une v.a. sur Ω et g une application définie sur $X(\Omega)$, à valeurs dans un ensemble E', alors $g\circ X$ est une v.a. sur Ω, notée $g(X)$:

$$\begin{array}{rccc} g(X): & \Omega & \to & E' \\ & \omega & \mapsto & g(X(\omega)) \end{array}$$

Démonstration
Ainsi définie, $g(X):\Omega\to E'$, $\omega\mapsto g(X)(\omega)=g\big(X(\omega)\big)$.
Il s'agit donc bien d'une application donc d'une variable aléatoire. □

Définition - variable aléatoire constante ou certaine
Si X est une application constante sur Ω, on dit que c'est une variable aléatoire constante ou certaine.

Définition - Notations
Soit $X:\Omega\to E$ une variable aléatoire sur Ω.
Alors, pour $A\subset E$, $X^{-1}(A)$ est un événement (car $X^{-1}(A)\in\mathscr{P}(\Omega)$) noté

$$(X\in A) \text{ ou } \{X\in A\} \quad (=X^{-1}(A)=\{\omega\in\Omega\mid X(\omega)\in A\}).$$

Dans le cas d'une variable aléatoire réelle, pour $x\in\mathbb{R}$, on note :

$$(X\leqslant x)=X^{-1}(]-\infty,x])=\{\omega\in\Omega\mid X(\omega)\leqslant x\},$$
$$(X<x)=X^{-1}(]-\infty,x[),$$
$$(X=x)=X^{-1}(\{x\})$$

de même pour $(X\geqslant x),(X>x),(a\leqslant X\leqslant b)\dots$

Heuristique - Deux points de vue sur X^{-1}
De manière générale, ce que l'on a c'est une famille d'événement paramétrée par une variable réelle et pour laquelle on cherche des probabilités de réalisation.
Par exemple, on s'intéresse à l'évolution de la température (moyenne ou sur un point du globe) sur 10 ans.
On note H, la variable qui indique cette évolution. On sait que $H\in\mathbb{R}$ (même si toutes les valeurs réelles ne sont pas réalistes).
Ce que l'on cherche alors est : la probabilité d'une hausse supérieure à 2°

$$\mathbf{P}(H\geqslant 2)$$

Il faut donc que l'ensemble $H^{-1}([2,+\infty[)$ soit un événement mesurable en probabilité.
Donc ce qui nous intéresse, dans la pratique, c'est plutôt $H^{-1}(I)$, comme élément de Ω et dont on cherche une probabilité.
On fera bien attention à la manière de lire les expressions mathématiques du type $\mathbf{P}(H=0)$
On a alors deux points de vue
- H est une application et H^{-1} est une application réciproque, en règle générale non bijective, donc une application de l'ensemble des parties de E (ou de $\mathbb{R}$ pour une var) sur l'ensemble des parties de Ω (ou une tribu de Ω).
  C'est le point de vue choisi dans le cours.
- H^{-1} fait la partition de Ω en classes d'équivalence.

$$\omega\mathscr{R}_H\omega' \iff H(\omega)=H(\omega')$$

De ce point de vue, le théorème suivant sur le système complet d'événements est trivial.

2.2. Loi de probabilité

On se place désormais sur un espace probabilisé fini $(\Omega,\mathbf{P})$.

Définition - Loi (de probabilité) d'une variable aléatoire
Soit X une v.a. sur Ω. Alors l'application

$$\begin{array}{rccc} \mathbf{P}_X: & X(\Omega) & \to & [0,1] \\ & x & \mapsto & \mathbf{P}(X=x) \end{array}$$

s'appelle la loi (de probabilité) de X.

Remarque - Changement d'espace
En fait X transforme l'espace de probabilité $(\Omega,\mathbf{P})$ en l'espace $(X(\Omega),\mathbf{P}_X)$.
A proprement parlé, il faudrait ajouter les tribus pour parler d'espace de probabilité.
Mais ici Ω est fini, donc, cette omission n'est pas grave.

Savoir faire - Définir la loi d'une variable aléatoire
Définir la loi de probabilité d'une v.a. X finie, c'est donc donner $X(\Omega)$ ainsi que les probabilités $\mathbf{P}(X=x)$ pour $x\in X(\Omega)$.

Remarque - Notation
Deux petites remarques :
- On peut noter f_X à la place de $\mathbf{P}_X$ pour éviter toute confusion avec une probabilité conditionnelle.
- On note usuellement $\mathbf{P}(X \in A)$ la probabilité de l'événement $(X \in A)$ et non $\mathbf{P}\Big((X \in A)\Big)$ ou $\mathbf{P}(\{X \in A\})$.

Définition - Relation d'équivalence sur les variables aléatoires
Soient X et Y deux variables aléatoires définies sur un même univers Ω.
On dit que X suit la même loi que Y, et on note $X \sim Y$, si $\mathbf{P}_X = \mathbf{P}_Y$.
Il s'agit d'une relation d'équivalence sur les variables aléatoires.

Attention - Les variables X et Y peuvent être différentes!
Pour une pièce bien équilibrée si X indique le nombre de pile pour n lancers et Y le nombre de face.
Alors $X \sim Y$, alors que $Y = n - X$ (et donc $X \neq Y$).

Démonstration
On a vu que si une relation est définie par l'image d'une fonction $f : x \mathcal{R} y$ si $f(x) = f(y)$, alors c'est une relation d'équivalence.
Ici $f : X \mapsto \mathbf{P}_X \ldots$
□

Exercice
Montrer que si $X \sim Y$, alors pour tout $f : \mathbb{R} \to \mathbb{R}$, $f(X) \sim f(Y)$.
La réciproque est-elle vraie ?

Correction
$\mathbf{P}_{f(X)} : x \mapsto \mathbf{P}(f(X) = x) = \sum_{z \in X(\Omega), f(z) = x} \mathbf{P}(X = z) = \sum_{z \in Y(\Omega), f(z) = x} \mathbf{P}(Y = z) = \mathbf{P}_{f(Y)}$.
La réciproque est vraie avec $f = \mathrm{id}$

Proposition - Variable aléatoire et système complet d'événements
Soit X une variable aléatoire définie sur Ω.
Alors la famille $\Big((X = x)\Big)_{x \in X(\Omega)}$ est un système complet d'événements, appelé système complet d'événements associé à X. En particulier,

$$\sum_{x \in X(\Omega)} \mathbf{P}(X = x) = 1.$$

Démonstration
Soient $[X = x]$ et $[X = x']$ deux événements de Ω.

$$(X = x) \cap (X = x') = \{\omega \in \Omega \mid X(\omega) = x \text{ et } X(\omega) = x'\}$$

Or X est une application donc $X(\omega)$ n'a qu'une valeur. Ainsi :

$$(X = x) \cap (X = x') = \begin{cases} \emptyset & \text{si} \quad x \neq x' \\ X = x & \text{si} \quad x = x' \end{cases}$$

Alors la famille $\Big((X = x)\Big)_{x \in X(\Omega)}$ est un système complet d'événements. □

Proposition - Existence d'une v.a.
Soient E un ensemble fini, $E = \{x_1, \ldots, x_n\}$ et $p_1, \ldots, p_n$ des réels positifs tels que $\sum_{i=1}^{n} p_i = 1$.
Alors, si Ω est un ensemble fini tel que $\mathrm{Card}\ \Omega \geqslant n$,
il existe une probabilité $\mathbf{P}$ sur Ω et une v.a. X définie sur Ω vérifiant :
$\forall i \in [\![1, n]\!], \mathbf{P}(X = x_i) = p_i$

Démonstration
Il suffit d'en créer une explicitement.
Prenons $\omega_1, \omega_2 \ldots \omega_n \in \Omega$. C'est possible car $n \leqslant r = \mathrm{Card}\ (\Omega) < +\infty$.
Soient $X : \Omega \to E, \omega_i \mapsto \begin{cases} x_i & \text{si} \quad i \leqslant n \\ x_n & \text{si} \quad i \geqslant n \end{cases}$.
Notons $\mathbf{P} : \Omega \to [0, 1], \omega_i \mapsto \begin{cases} p_i & \text{si} \quad i \leqslant n \\ 0 & \text{si} \quad i > n \end{cases}$.
Alors pour $i \neq n$, $\mathbf{P}(X = x_i) = \mathbf{P}(\omega_i) = p_i$ et $\mathbf{P}(X = x_n) = \mathbf{P}(\{\omega_n, \omega_{n+1}, \ldots, \omega_r\}) = x_n + 0 = x_n$.
Et $\mathbf{P}$ ainsi définie est bien une probabilité sur Ω, car $\mathbf{P}(A \cup B) = \mathbf{P}(A) + \mathbf{P}(B)$, si $A \cap B = \emptyset$, alors que $\mathbf{P}(\Omega) = \sum_{i=1}^{n} p_i = 1$. □

Proposition - Loi d'une fonction de X
Soient X v.a. sur Ω et g une fonction définie sur $X(\Omega)$.
Alors la loi de probabilité de $Y = g(X)$ est donnée par $Y(\Omega) = g(X(\Omega))$ et

$$\forall y \in Y(\Omega), \mathbf{P}(Y = y) = \sum_{x \in g^{-1}(\{y\})} \mathbf{P}(X = x) = \sum_{x | g(x) = y} \mathbf{P}(X = x)$$

Démonstration
Par composition : $Y = g \circ X : \Omega \to g(X(\Omega))$, donc $Y(\Omega) = g(X(\Omega))$
Et

$$\mathbf{P}(Y = y) = \mathbf{P}(Y^{-1}(y)) = \mathbf{P}(\{\omega \in \Omega \mid g(X(\omega)) = y\}) = \mathbf{P}(\{\omega \in \Omega \mid X(\omega) \in g^{-1}(y)\})$$
$$= \sum_{x \in g^{-1}(y)} \mathbf{P}(X = x) = \sum_{x | g(x) = y} \mathbf{P}(X = x)$$

□

Définition - Fonction de répartition
Soit X une v.a.r sur Ω. L'application

$$\begin{array}{rccc} F_X : & \mathbb{R} & \to & [0, 1] \\ & x & \mapsto & \mathbf{P}(X \leqslant x) \end{array}$$

s'appelle la fonction de répartition de X ; si $X(\Omega) = \{x_1, x_2, \ldots, x_n\}$, alors

$$\forall x \in \mathbb{R}, F_X(x) = \sum_{i | x_i \leqslant x} \mathbf{P}(X = x_i).$$

Exemple - Fonction de répartition du max
On lance deux dés de 6 faces. Les résultats sont supposés indépendants. X_i indique le résultat du dé i.
On note $X = \max(X_1, X_2)$, le meilleur résultat des deux dés.
On a $X(\Omega) = \mathbb{N}_6$. Avec les fonctions de répartitions :

$$F_X(k) = \mathbf{P}(\max(X_1, X_2) \leqslant k) = \mathbf{P}(X_1 \leqslant k, X_2 \leqslant k) = \mathbf{P}(X_1 \leqslant k)\mathbf{P}(X_2 \leqslant k)$$

par indépendance des lois X_1 et X_2. Donc des variables aléatoires $[X_1 \leqslant k]$ et $[X_2 \leqslant k]$

$$F_X(k) = F_{X_1}(k) \times F_{X_2}(k) = \sum_{i=1}^{k} \frac{1}{6} \times \sum_{i=1}^{k} \frac{1}{6} = \frac{k^2}{36}$$

Donc

$$\mathbf{P}(X = k) = F_X(k) - F_X(k-1) = \frac{k^2 - (k-1)^2}{36} = \frac{2k-1}{36}$$

(On vérifie que $\sum_{k=1}^{6} \frac{2k-1}{36} = \frac{1}{18} \times \frac{6 \times 7}{2} - \frac{6}{36} = \frac{7}{6} - \frac{1}{6} = 1$).

Exercice
On lance deux dés à six faces parfaitement équilibrés. Soit X la variable aléatoire égale à la somme des points obtenus. Donner la loi de X, sa fonction de répartition ainsi que la loi de $Y = |X - 7|$.

Correction

Ici, le modèle naturel s'appuie sur le résultat de chacun des deux dès. On peut donc considérer les variables aléatoires Y_i qui indique le résultat du dé i.
On a alors $X = Y_1 + Y_2$. Ainsi $X(\Omega) = [\![2, 12]\!]$.

$$\forall\, x \in X(\Omega), \qquad \mathbf{P}(X = x) = \mathbf{P}(Y_1 + Y_2 = x) = \mathbf{P}\left(\bigcup_{y \in [\![1, x-1]\!]} (Y_1 = y \cap Y_2 = x - y)\right)$$

Par incompatibilité $(Y_1 = y \cap Y_2 = x - y)$ et $(Y_1 = y' \cap Y_2 = x - y')$,

$$\forall\, x \in X(\Omega), \qquad \mathbf{P}(X = x) = \sum_{y=1}^{x-1} \mathbf{P}\big(Y_1 = y \cap Y_2 = x - y\big)$$

puis par indépendance des événements $(Y_1 = a)$ et $(Y_2 = b)$,

$$\forall\, x \in X(\Omega), \qquad \mathbf{P}(X = x) = \sum_{y=1}^{x-1} \mathbf{P}(Y_1 = y)\mathbf{P}(Y_2 = x - y)$$

Enfin, chacun des événements $(Y_1 = a)$ ou $(Y_2 = a)$ a une probabilité nulle si $a \notin [\![1, n]\!]$ ou égale à $\frac{1}{6}$ sinon.

Donc $\forall\, x \in X(\Omega), \quad \mathbf{P}(X = x) = \begin{cases} \frac{x-1}{36} & \text{si} \quad x \leqslant 7 \\ \frac{13-x}{36} & \text{si} \quad x > 7 \end{cases}$

La loi de $Y = |X - 7|$ est alors très simple :

$$Y(\Omega) = [\![0, 5]\!] \qquad \mathbf{P}(Y = h) = \frac{2}{36} \times (h + 1) - \text{ si } h \neq 7, \mathbf{P}(Y = 7) = \frac{1}{6}$$

Enfin la fonction de répartition est en escalier :

$$F_X(t) = \begin{cases} 0 & \text{si} \quad t < 2 \\ \frac{1}{36} & \text{si} \quad 2 \leqslant t < 3 \\ \frac{3}{36} = \frac{1}{12} & \text{si} \quad 3 \leqslant t < 4 \\ \frac{6}{36} = \frac{1}{6} & \text{si} \quad 4 \leqslant t < 5 \\ \frac{10}{36} = \frac{5}{18} & \text{si} \quad 5 \leqslant t < 6 \\ \frac{15}{36} & \text{si} \quad 6 \leqslant t < 7 \\ \frac{21}{36} = \frac{7}{12} & \text{si} \quad 7 \leqslant t < 8 \\ \frac{26}{36} = \frac{13}{18} & \text{si} \quad 7 \leqslant t < 8 \\ \frac{30}{36} = \frac{5}{6} & \text{si} \quad 7 \leqslant t < 8 \\ \frac{33}{36} = \frac{11}{12} & \text{si} \quad 7 \leqslant t < 8 \\ \frac{35}{36} & \text{si} \quad 7 \leqslant t < 8 \\ \frac{36}{36} = 1 & \text{si} \quad 7 \leqslant t < 8 \end{cases}$$

2.3. Lois usuelles

$(\Omega, \mathbf{P})$ désigne un espace probabilisé fini.

Loi uniforme

Définition - Loi uniforme
On dit qu'une v.a. X suit une loi uniforme sur $X(\Omega)$ si

$$\forall x \in X(\Omega), \mathbf{P}(X = x) = \frac{1}{\text{Card}\,(X(\Omega))}.$$

Dans le cas particulier où $X(\Omega) = [\![1, n]\!]$, on note $X \hookrightarrow \mathscr{U}_n$ et on a

$$\forall k \in [\![1, n]\!], \mathbf{P}(X = k) = \frac{1}{n}.$$

Remarque - Modèle pour la loi uniforme $\mathscr{U}_n$
On choisit un objet au hasard parmi n objets numérotés de 1 à n. X désigne le numéro de l'objet tiré. (ex : lancer d'un dé non truqué)

Loi de Bernoulli

Définition - Loi de Bernoulli
Soit $p \in [0, 1]$. On dit qu'une v.a.r. X suit une loi de Bernoulli de paramètre p si $X(\Omega) = \{0, 1\}$ et $\mathbf{P}(X = 1) = p$, et donc $\mathbf{P}(X = 0) = 1 - p$.
On note $X \hookrightarrow \mathscr{B}(p)$.

Remarque - Modèle pour la loi de Bernoulli $\mathscr{B}(p)$
Lors d'une expérience aléatoire effectuée une seule fois et ayant deux issues possibles, on note X la v.a. qui vaut 1 si l'on a l'une des issues (succès) et 0 si l'on a l'autre (échec). (ex : on lance une pièce de monnaie, le succès désignant le fait d'obtenir "pile".)
X est alors la fonction indicatrice de l'événement A "avoir un succès", usuellement notée $\mathbb{1}_A$, définie, pour tout $\omega \in \Omega$ par $\mathbb{1}_A(\omega) = 1$ si $\omega \in A$, $\mathbb{1}_A(\omega) = 0$ si $\omega \notin A$ et on a

$$\mathbb{1}_A \hookrightarrow \mathscr{B}(\mathbf{P}(A)).$$

Savoir faire - Exploitation d'indicatrice (1)
Très souvent, on associera à l'événement $A \subset \Omega$, la variable aléatoire $X = \mathbb{1}_A : \omega \mapsto \begin{cases} 1 & \text{si } \omega \in A \\ 0 & \text{si } \omega \notin A \end{cases}$.
Dans ce cas $X \hookrightarrow \mathscr{B}(p)$ avec $p = \mathbf{P}(A)$

Loi binomiale

Définition - Loi binomiale
Soient $n \in \mathbb{N}^*$ et $p \in [0, 1]$. On dit qu'une v.a.r. suit une loi binomiale de paramètres n et p si $X(\Omega) = [\![0, n]\!]$ et

$$\forall k \in [\![0, n]\!], \mathbf{P}(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}.$$

On note $X \hookrightarrow \mathscr{B}(n, p)$.

Remarque - Modèle pour la loi binomiale $\mathscr{B}(n, p)$
On considère une urne avec deux catégories de boules : des blanches en proportion p et des non blanches en proportion $q = 1 - p$. On tire n boules **avec remise** de cette urne. X désigne la v.a. égale au nombre de boules blanches obtenues dans ce tirage.
Plus généralement, c'est la loi de la variable aléatoire X égale au nombre de succès lors de la répétition de n expériences de Bernoulli indépendantes, la probabilité d'un succès étant p.

3. Couples de variables aléatoires

Soit $(\Omega, \mathbf{P})$ un espace probabilisé fini. On a déjà rencontré cette situation dans le cas du lancer de dés.

Définition - Couple de variables aléatoires
Soient X et Y deux variables aléatoires sur Ω, à valeurs respectivement dans les ensembles E et F. L'application

$$\begin{array}{rccc} Z : & \Omega & \to & E \times F \\ & \omega & \mapsto & (X(\omega), Y(\omega)) \end{array}$$

est appelée couple de variables aléatoires, c'est donc une v.a. à valeurs dans $E \times F$. On note $Z = (X, Y)$.
On a $Z(\Omega) \subset X(\Omega) \times Y(\Omega)$.

Si X et Y sont des v.a.r. on parle de couple de v.a.r.

Définition - Loi conjointe, lois marginales
On appelle loi conjointe de X et Y la loi du couple $Z=(X,Y)$, c'est-à-dire l'application

$$\begin{array}{rll}\mathbf{P}_{(X,Y)}: & Z(\Omega) & \to [0,1]\\ & (x,y) & \mapsto \mathbf{P}\Big((X,Y)=(x,y)\Big)=\mathbf{P}\Big((X=x)\cap(Y=y)\Big)\end{array}$$

On appelle lois marginales du couple (X,Y) les deux lois de probabilité, respectivement de X et Y.
On a $\mathbf{P}_X : x\mapsto \sum\limits_{y\in Y(\Omega)} \mathbf{P}\big((X,Y)=(x,y)\big)=\mathbf{P}(X=x)$ (et de même pour P_Y).

Attention - Lien entre les deux lois
A partir de la loi conjonte d'un couple de v.a. on peut déterminer les lois marginales. La réciproque est fausse.

Définition - Loi conditionnelle
Soit (X,Y) un couple de variables aléatoires.
Pour $x\in X(\Omega)$ fixé tel que $\mathbf{P}(X=x)\neq 0$, on appelle loi conditionnelle de Y sachant $(X=x)$ la loi de Y pour la probabilité $\mathbf{P}_{(X=x)}$, c'est-à-dire l'application :

$$\begin{array}{ll}Y(\Omega) & \to [0,1]\\ y & \mapsto \mathbf{P}(Y=y|X=x)\end{array}$$

De même on peut définir, pour $y\in Y(\Omega)$ tel que $\mathbf{P}(Y=y)\neq 0$, la loi conditionnelle de X sachant $(Y=y)$.

Exercice
On lance trois fois de suite une pièce équilibrée. Soient X_1 la v.a. qui vaut 1 si le premier jet donne "pile" et 0 sinon, et X_2 la v.a. égale au nombre de "face" obtenu.
Déterminer la loi conjointe ainsi que les lois marginales du couple (X_1,X_2).
Déterminer la loi conditionnelle de X_1 sachant $(X_2=1)$.

Correction
$(X_1,X_2)(\Omega)=\{0,1\}\times\{0,1,2,3\}$. Pour exprimer la valeur prise par la loi conjointe, nous allons faire deux tableaux : un qui liste les valeurs réalisations de ω et l'autre les probabilités (tous les événements sont équiprobables) :

$\omega=(A_1,A_2,A_3)$	$X_2=0$	$X_2=1$	$X_2=2$	$X_2=3$
$X_1=0$	(P_1,P_2,P_3)	$(P_1,P_2,F_3)\cup(P_1,F_2,P_3)$	(P_1,F_2,F_3)	$\emptyset$
$X_1=1$	$\emptyset$	(F_1,P_2,P_3)	$(F_1,F_2,P_3)\cup(F_1,P_2,F_3)$	(F_1,F_2,F_3)

$\mathbf{P}$	$X_2=0$	$X_2=1$	$X_2=2$	$X_2=3$
$X_1=0$	$\frac{1}{2^3}$	$\frac{2}{2^3}$	$\frac{1}{2^3}$	0
$X_1=1$	0	$\frac{1}{2^3}$	$\frac{2}{2^3}$	$\frac{1}{2^3}$

Il suffit de sommer sur les lignes ou colonnes du tableau pour obtenir les lois marginales :

$$\mathbf{P}(X_1=0)=\mathbf{P}(X_1=0)=\frac{1}{2}\qquad \mathbf{P}(X_2=0)=\mathbf{P}(X_2=3)=\frac{1}{8},\mathbf{P}(X_2=1)=\mathbf{P}(X_2=2)=\frac{3}{8}$$

Enfin :

$$\mathbf{P}(X_2=1)(X_1=0)=\frac{\frac{2}{2^3}}{\frac{3}{2^3}}=\frac{2}{3}\qquad \mathbf{P}(X_2=1)(X_1=1)=\frac{\frac{1}{2^3}}{\frac{3}{2^3}}=\frac{1}{3}$$

Exercice
Un sac contient 4 boules numérotées de 1 à 4. On tire deux boules avec remise et on note X_1 et X_2 les numéros obtenus. On pose $X=X_1$ et $Y=\max(X_1,X_2)$.
Déterminer la loi conjointe ainsi que les lois marginales du couple (X_1,X_2).
Déterminer la loi conjointe ainsi que les lois marginales du couple (X,Y).
Déterminer la loi conditionnelle de Y sachant $(X=2)$

Correction
$X_i\hookrightarrow\mathscr{U}_4$ et elles sont indépendantes (voir plus bas) donc

$$(X_1,X_2)(\Omega)=[\![1,4]\!]^2\qquad \mathbf{P}\big((X_1,X_2)=(i,j)\big)=\frac{1}{16}$$

(X_1,X_2) suit une loi uniforme.
On notera que nécessairement $Y\geqslant X$, donc ces deux variables ne sont pas indépendantes. On a donc
$\mathbf{P}\big((X,Y)=(a,b)\big)=\begin{cases}0 & \text{si } a>b\\ \frac{1}{16}=\mathbf{P}((X_1,X_2)=(a,b)) & \text{si } a<b\\ \frac{a}{16}=\mathbf{P}\big((X_1,X_2)\in\{a\}\times[\![1,a]\!]\big) & \text{si } a=b\end{cases}$
On trouve alors

$$\mathbf{P}(X=1)=\underbrace{\frac{1}{16}}_{y=1}+\underbrace{\frac{1}{16}}_{y=2}+\underbrace{\frac{1}{16}}_{y=3}+\underbrace{\frac{1}{16}}_{y=4}=\frac{1}{4}\qquad \mathbf{P}(X=2)=\underbrace{0}_{y=1}+\underbrace{\frac{2}{16}}_{y=2}+\underbrace{\frac{1}{16}}_{y=3}+\underbrace{\frac{1}{16}}_{y=4}=\frac{1}{4}$$

$$\mathbf{P}(X=3)=\underbrace{0}_{y=1}+\underbrace{0}_{y=2}+\underbrace{\frac{3}{16}}_{y=3}+\underbrace{\frac{1}{16}}_{y=4}=\frac{1}{4}\qquad \mathbf{P}(X=2)=\underbrace{0}_{y=1}+\underbrace{0}_{y=2}+\underbrace{0}_{y=3}+\underbrace{\frac{4}{16}}_{y=4}=\frac{1}{4}$$

Et

$$\mathbf{P}(Y=1)=\underbrace{\frac{1}{16}}_{x=1}+\underbrace{0}_{x=2}+\underbrace{0}_{x=3}+\underbrace{0}_{x=4}=\frac{1}{16}\qquad \mathbf{P}(Y=2)=\underbrace{\frac{1}{16}}_{x=1}+\underbrace{\frac{2}{16}}_{x=2}+\underbrace{0}_{x=3}+\underbrace{0}_{x=4}=\frac{3}{16}$$

$$\mathbf{P}(Y=3)=\underbrace{\frac{1}{16}}_{x=1}+\underbrace{\frac{1}{16}}_{x=2}+\underbrace{\frac{3}{16}}_{x=3}+\underbrace{0}_{x=4}=\frac{5}{16}\qquad \mathbf{P}(Y=4)=\underbrace{\frac{1}{16}}_{x=1}+\underbrace{\frac{1}{16}}_{x=2}+\underbrace{\frac{1}{16}}_{x=3}+\underbrace{\frac{4}{16}}_{x=4}=\frac{7}{16}$$

Et pour la loi conditionnelle :

$$\mathbf{P}_{X=2}(Y=1)=0\qquad \mathbf{P}_{X=2}(Y=2)=\frac{\mathbf{P}(X=2\cap Y=2)}{\mathbf{P}(X=2)}=\frac{1}{2}\qquad \mathbf{P}_{X=2}(Y=3)=\frac{1}{4}\qquad \mathbf{P}_{X=2}(Y=4)=\frac{1}{4}$$

Proposition - Caractérisation de loi de couple de v.a.
Soient E et F deux ensembles.

$$\left\{\Big((x_i,y_j),p_{ij}\Big)\in(E\times F)\times\mathbb{R}\;\middle|\;1\leqslant i\leqslant r,1\leqslant j\leqslant s\right\}$$

représente la loi de probabilité d'un couple de v.a. si et seulement si

$$\forall(i,j)\in[\![1,r]\!]\times[\![1,s]\!],p_{ij}\geqslant 0 \text{ et } \sum_{i=1}^{r}\sum_{j=1}^{s}p_{ij}=1.$$

Démonstration
Il s'agit d'une généralisation de la proposition : existence d'une va a priori.
On peut faire comme pour cette démonstration : suivre une démarche constructive □

Les définitions précédentes peuvent se généraliser à des n-uplets de v.a.

Définition - Vecteur aléatoire
Soient $n\in\mathbb{N}^*$, $E_1,\dots,E_n$ des ensembles et $X_1,\dots,X_n$ n v.a. sur Ω. La variable aléatoire à valeurs dans $E_1\times\cdots\times E_n$

$$\begin{array}{rll}X: & \Omega & \to E_1\times\cdots\times E_n\\ & \omega & \mapsto (X_1(\omega),\dots,X_n(\omega))\end{array}$$

est appelée n-uplet de variables aléatoires. On note $X=(X_1,\dots,X_n)$.
On a $X(\Omega)\subset X_1(\Omega)\times\cdots\times X_n(\Omega)$.
Si les X_i sont des v.a.r. on parle de n-uplet de v.a.r. ou de vecteur aléatoire à valeur dans $\mathbb{R}^n$.
La loi conjointe de $X_1,\dots,X_n$ est la loi du n-uplet $X=(X_1,\dots,X_n)$ Les lois marginales du n-uplet $X=(X_1,\dots,X_n)$ sont les n lois de probabilité des v.a. $X_1,\dots,X_n$, elles peuvent se déduire de la loi conjointe.

4. Indépendance

4.1. Indépendance de deux variables aléatoires

Définition - Indépendance de deux v.a.
Deux variables aléatoires discrètes X et Y sur l'espace probabilisable $(\Omega, \mathbf{P})$ sont dites indépendantes si, pour tout couple (x,y) de $X(\Omega)\times Y(\Omega)$, les événements $(X=x)$ et $(Y=y)$ sont indépendants, c'est-à-dire si

$$\forall (x,y)\in X(\Omega)\times Y(\Omega),\ \mathbf{P}(\{X=x\}\cap\{Y=y\}) = \mathbf{P}(X=x)\mathbf{P}(Y=y).$$

On notera (en MPSI3) : $X \perp\!\!\!\perp Y$ pour indiquer que X et Y sont indépendantes

C'est une relation symétrique, elle n'est ni réflexive, ni transitive.

Proposition - Caractérisation d'indépendance
Deux v.a. X et Y sur $(\Omega,\mathbf{P})$ sont indépendantes si et seulement si,
pour tout $A\subset X(\Omega)$ et $B\subset Y(\Omega)$, les événements $(X\in A)$ et $(Y\in B)$ sont indépendants.

Démonstration
Supposons que pour tout $(A,B)\subset X(\Omega)\times Y(\Omega)$, les événements $(X\in A)$ et $(Y\in B)$ sont indépendants.
En prenant $A=\{x\}$ et $B=\{y\}$, alors $[X=x]$ et $[Y=y]$ sont indépendants.
Ceci est vrai pour tout $(x,y)\in X(\Omega)\times Y(\Omega)$, donc X et Y sont indépendantes.
Supposons que X et Y sont indépendantes.
Soient $A\subset X(\Omega)$ et $B\subset Y(\Omega)$,

$$\mathbf{P}(X\in A\cap Y\in B) = \mathbf{P}\left(\bigcup_{x\in A}(X=x)\cap\bigcup_{y\in B}(Y=y)\right) = \mathbf{P}\left(\bigcup_{x\in A}\bigcup_{y\in B}(X=x)\cap(Y=y)\right)$$

Or les événements $(X=x)\cap(Y=y)$ et $(X=x')\cap(Y=y')$ sont incompatibles dès que $x\neq x'$ ou $y\neq y'$.

$$\mathbf{P}(X\in A\cap Y\in B) = \sum_{x\in A}\sum_{y\in B}\mathbf{P}(X=x\cap Y=y) = \sum_{x\in A}\sum_{y\in B}\mathbf{P}(X=x)\mathbf{P}(Y=y),$$

par indépendance

$$\mathbf{P}(X\in A\cap Y\in B) = \sum_{x\in A}\mathbf{P}(X=x)\sum_{y\in B}\mathbf{P}(Y=y) = \mathbf{P}(X\in A)\mathbf{P}(Y\in B)$$

□

Théorème - de Coalition
Soient X et Y deux variables aléatoires sur $(\Omega,\mathbf{P})$, indépendantes.
Alors, pour toutes fonctions f et g, les v.a. (si elles sont bien définies) $f(X)$ et $g(Y)$ sont indépendantes.

Démonstration
On note $U=f(X)$ et $V=g(Y)$.
Soient $A\in U(\Omega)$ et $B\in V(\Omega)$, puis $\overline{A}=f^{-1}(A)$, $\overline{B}=g^{-1}(B)$.

$$\mathbf{P}(U\in A, V\in B) = \mathbf{P}(f(X)\in A, g(Y)\in B) = \mathbf{P}(X\in\overline{A}, Y\in\overline{B}) = \mathbf{P}(X\in\overline{A})\mathbf{P}(Y\in\overline{B}),$$

par indépendance des variables X et Y.
Puis $(X\in\overline{A})\Longleftrightarrow(f(X)\in A)$ et $(Y\in\overline{B})\Longleftrightarrow(g(Y)\in B)$, donc

$$\mathbf{P}(U\in A, V\in B) = \mathbf{P}(f(X)\in A)\mathbf{P}(g(Y)\in B) = \mathbf{P}(U\in A)\mathbf{P}(V\in B)$$

Les variables U et V sont donc indépendantes. □

4.2. Indépendance de plusieurs variables aléatoires

Définition - Indépendance mutuelle
Soient n variables aléatoires $X_1,\dots,X_n$ définies sur (Ω,P).
On dit que $X_1,\dots,X_n$ sont mutuellement indépendantes (ou indépendantes) si pour tout $(x_1,x_2,\dots,x_n)\in X_1(\Omega)\times X_2(\Omega)\times\dots\times X_n(\Omega)$, on a

$$\mathbf{P}(\bigcap_{i=1}^{n}\{X_i=x_i\}) = \prod_{i=1}^{n}\mathbf{P}(X_i=x_i)$$

c'est-à-dire si les événements $\left((X_i=x_i)\right)_{1\leqslant i\leqslant n}$ sont mutuellement indépendants.

Proposition - Caractérisation de l'indépendance mutuelle
Soient n variables aléatoires $X_1,\dots,X_n$ définies sur (Ω,P).
$X_1,\dots,X_n$ sont mutuellement indépendantes si et seulement si pour tout $(A_1,\dots,A_n)\subset X_1(\Omega)\times\cdots\times X_n(\Omega)$, les événements $(X_i\in A_i)$ sont mutuellement indépendants.

Démonstration
Il s'agit de la même démonstration que pour l'indépendance de deux variables aléatoires mais avec n sommes.
Supposons que pour tout $(A_1\dots,A_n)\subset X_1(\Omega)\times\cdots\times X_n(\Omega)$, les événements $(X_1\in A_1)$, $X_2\in A_2$,… $(X_n\in A_n)$ sont indépendants.
En prenant pour tout $i\in\mathbb{N}_n$, $A_i=\{x_i\}$ alors $[X_1=x_1]$, $[X_2=x_2]$,… $[X_n=x_n]$ sont mutuellement indépendants.
Ceci est vrai pour tout $(x_i)\in X_i(\Omega)$, donc X_1, X_2,… X_n sont mutuellement indépendantes.
Supposons que X_1, X_2… X_n sont indépendantes.
Soit, pour tout $i\in\mathbb{N}_N$, $A_i\subset X_i(\Omega)$,

$$\mathbf{P}\left(\bigcap_{i=1}^{n}(X_i\in A_i)\right) = \mathbf{P}\left(\bigcap_{i=1}^{n}(\bigcup_{x\in A_i}(X_i=x))\right) = \mathbf{P}\left(\bigcup_{x_1\in A_1}\bigcup_{x_2\in A_2}\cdots\bigcup_{x_n\in A_n}(\bigcap_{i=1}^{n}(X_i=x_i))\right)$$

Or les événements $(X_1=x_1)\cap(X_2=x_2)\cdots\cap(X_n=x_n)$ et $(X_1=x_1')\cap(X_2=x_2')\cdots\cap(X_n=x_n')$ sont incompatibles dès que $x_1\neq x_1'$ ou $x_2\neq x_2'$ ou $x_n\neq x_n'$.

$$\mathbf{P}\left(\bigcap_{i=1}^{n}(X_i\in A_i)\right) = \sum_{x_1\in A_1}\sum_{x_2\in A_2}\cdots\sum_{x_n\in A_n}\mathbf{P}(X=x_1\cap X_2=x_2\cap\dots X_n=x_n) = \sum_{x_1\in A_1}\cdots\sum_{x_2\in A_n}\mathbf{P}(X_1=x_1)\dots\mathbf{P}(X_n=x_n),$$

par indépendance

$$\mathbf{P}\left(\bigcap_{i=1}^{n}(X_i\in A_i)\right) = \sum_{x_1\in A_1}\mathbf{P}(X_1=x_1)\sum_{x_2\in A_2}\mathbf{P}(X_2=x_2)\cdots\sum_{x_n\in A_n}\mathbf{P}(X_n=x_n) = \mathbf{P}(X_1\in A_1)\mathbf{P}(X_2\in A_2)\cdots\mathbf{P}(X_n\in A_n)$$

□

Proposition - Indépendance mutuelle implique l'indépendance deux à deux
n variables aléatoires $X_1,\dots,X_n$ sur $(\Omega,\mathbf{P})$ mutuellement indépendantes sont indépendantes deux à deux.

Démonstration
On se place sur l'espace probabilisé fini $(\Omega,\mathbf{P})$.
Pour tout $i,j\in\mathbb{N}_n$, et tout $x_i\in X_i(\Omega)$, $x_j\in X_j(\Omega)$,
les événements $[X_i=x_i]$ et $[X_j=x_j]$ sont indépendants.
Donc X_i et X_j sont des variables aléatoires indépendantes.
Les variables aléatoires (X_i) sont deux à deux indépendantes. □

Théorème - Coalitions (n vari ables)
Soient $X_1,\dots,X_n$ n variables aléatoires définies sur (Ω,P) mutuellement indépendantes. Alors :
— pour toutes fonctions $g_1,\dots,g_n$, les v.a. (si elles sont bien définies) $g_1(X_1),\dots,g_n(X_n)$ sont mutuellement indépendantes ;
— pour toutes fonctions φ et ψ, les deux variables aléatoires (si elles sont définies) $\varphi(X_1,X_2,\dots,X_p)$ et $\psi(X_{p+1},\dots,X_n)$ sont indépen-

dantes ;
— plus généralement si $Y_1,\dots,Y_k$ sont k variables aléatoires telles que Y_i soit fonction des X_j pour $j\in J_i$, avec les ensembles J_i deux à deux disjoints, alors $Y_1,\dots,Y_k$ sont mutuellement indépendantes.

On ne fait pas la première démonstration, il suffit d'apter le cas de deux variables.
On ne fait pas non plus la dernière démonstration, très pénible dans les notations.

Démonstration
Soient $A\in\varphi(X_1,X_2,\dots X_p)(\Omega)$, $\overline{A}=\varphi^{-1}(A)$ et $B\in\psi(X_{p+1},X_{p+2},\dots X_n)(\Omega)$, $\overline{B}=\psi^{-1}(B)$.
C'est-à-dire $\overline{A}=\{\omega\in\Omega\mid\forall\ i\in\mathbb{N}_p,[\varphi(\omega)]_i\in X_i\}\dots$

$$\mathbf{P}(\varphi(X_1,X_2,\dots X_p)\in A\cap\psi(X_{p+1},X_{p+2},\dots X_n)\in B)$$
$$=\mathbf{P}\left(\left(\bigcup_{(x_1,\dots x_p)\mid\varphi(x_1,\dots x_p)\in A}(X_1=x_1,X_2=x_2\dots X_p=x_p)\right)\bigcap\left(\bigcup_{(x_{p+1},\dots x_n)\mid\psi(x_{p+1},\dots x_n)\in B}(X_{p+1}=x_{p+1},\dots X_n=x_n)\right)\right)$$
$$=\mathbf{P}\left(\bigcup_{(x_1,\dots x_p)\mid\varphi(x_1,\dots x_p)\in A}\left(X_1=x_1,X_2=x_2\dots X_p=x_p\right)\bigcap\bigcup_{(x_{p+1},\dots x_n)\mid\psi(x_{p+1},\dots x_n)\in B}\left(X_{p+1}=x_{p+1},\dots X_n=x_n\right)\right)$$
$$=\sum_{(x_1,\dots x_p)\mid\varphi(x_1,\dots x_p)\in A}\ \sum_{(x_{p+1},\dots x_n)\mid\psi(x_{p+1},\dots x_n)\in B}\mathbf{P}(X_1=x_1,X_2=x_2\dots X_p=x_p,X_{p+1}=x_{p+1},\dots X_n=x_n)$$
$$=\sum_{\substack{(x_1,\dots x_p)\mid\varphi(x_1,\dots x_p)\in A\\(x_{p+1},\dots x_n)\mid\psi(x_{p+1},\dots x_n)\in B}}\mathbf{P}(X_1=x_1,X_2=x_2\dots X_p=x_p)\times\mathbf{P}(X_{p+1}=x_{p+1},\dots X_n=x_n)$$
$$=\sum_{(x_1,\dots x_p)\mid\varphi(x_1,\dots x_p)\in A}\mathbf{P}(X_1=x_1,X_2=x_2\dots X_p=x_p)\times\sum_{(x_{p+1},\dots x_n)\mid\psi(x_{p+1},\dots x_n)\in B}\mathbf{P}(X_{p+1}=x_{p+1},\dots X_n=x_n)$$
□

Exemple - Une pièce qui n'en finit pas d'être tirée

On considère une pièce que l'on lance infiniment, elle retombe avec une probabilité p sur pile et $q=1-p$ sur face.
On appelle X, la v.a.r. qui mesure le première fois que l'on obtient pile.
On appelle Y, la v.a.r. qui mesure le seconde fois que l'on obtient pile.
On considère que les résultats des lancers sont indépendants les uns les autres (modélisation).
Cherchons la loi conjointe et les lois de chacune des v.a.r.
On a $X(\Omega)=\mathbb{N}$ et $Y(\Omega)=[\![2;+\infty[\![$, et $(X,Y)(\Omega)=\mathbb{N}\times[\![2;+\infty[\![$ *(produit cartésien).*
Pour avoir un résultat plus joli, on peut considérer :
$(X,Y)(\Omega)=\mathbb{N}^2$
avec $\forall\ x\in\mathbb{N}$, $\mathbf{P}((X,Y)=(x,0))=0$
Comme il faut d'avantage de lancer pour obtenir un deuxième pile qu'un premier,
$\forall\ (i,j)\in\mathbb{N}\times[\![2;+\infty[\![,i\geqslant j\qquad\mathbf{P}(X=i,Y=j)=0$
Puis si l'on a pile en i puis en j, cela signifie **exactement** que l'on a eu :
d'abord $(i-1)$ lancer face, puis un pile, puis $j-i-1$ face et encore un pile
$\forall\ (i,j)\in\mathbb{N}\times[\![2;+\infty[\![,i<j\qquad\mathbf{P}(X=i,Y=j)=q^{i-1}pq^{j-i-1}p=q^{j-2}p^2$
Ces deux lois sont-elles indépendantes?
$\mathbf{P}(X=i)=q^{i-1}p$ et $\mathbf{P}(Y=j)=(j-1)q^{j-2}p^2$
Ainsi $\mathbf{P}(X=i,Y=j)\neq\mathbf{P}(X=i)\mathbf{P}(Y=j)$, les deux v.a.r. ne sont pas indépendantes.
(Au passage : $\sum_{j=2}^{\infty}(j-1)q^{j-2}p^2=1\dots$)
On considère avec le même modèle, non plus (X,Y) mais le couple (X,Z),
où Z indique le nombre de lancers supplémentaires pour obtenir le second pile.
Ainsi $Z(\Omega)=\mathbb{N}$ et donc $(X,Z)(\Omega)=\mathbb{N}^2$ *(produit cartésien).*
Si l'on obtient le premier pile en i et le second j coups plus tard, on a :
d'abord $(i-1)$ lancer face, puis un pile, puis $j-1$ face et encore un pile
$\forall\ (i,j)\in\mathbb{N}^2,\qquad\mathbf{P}(X=i,Z=j)=q^{i-1}pq^{j-1}p=q^{i+j-2}p^2$
Et l'on a toujours $\mathbf{P}(X=i)=q^{i-1}p$ et de même $\mathbf{P}(Z=j)=q^{j-1}p$,
Ainsi $\mathbf{P}(X=i,Z=j)=\mathbf{P}(X=i)\mathbf{P}(Z=j)$, les deux v.a.r. sont dans ce cas indépendantes.

4.3. Opération de variables aléatoires (indépendantes)

Si E est un ensemble muni d'une loi (E : espace vectoriel, par exemple), on peut faire agir la même loi sur des variables aléatoires X_i à valeurs dans E.

Théorème - Stabilité de la loi binomiale pour la somme
Soit $(\Omega,\mathbf{P})$ un espace de probabilité fini.
— Si X et Y sont deux v.a.r. indépendantes sur (Ω,P) telles que $X\hookrightarrow\mathscr{B}(n,p)$ et $Y\hookrightarrow\mathscr{B}(m,p)$, alors
$$X+Y\hookrightarrow\mathscr{B}(n+m,p).$$
— Si $X_1,\dots,X_n$ sont des v.a.r. mutuellement indépendantes sur (Ω,P) telles que pour tout i,
$X_i\hookrightarrow\mathscr{B}(n_i,p)$, alors
$$\sum_{i=1}^{n}X_i\hookrightarrow\mathscr{B}\Big(\sum_{i=1}^{n}n_i,p\Big).$$

La loi de Bernoulli étant un cas particulier de la loi binomiale ($n=1$), on a

Corollaire - Addition de Bernoulli
Si $X_1,\dots,X_n$ sont des v.a.r. mutuellement indépendantes sur $(\Omega,\mathbf{P})$, toutes de loi $\mathscr{B}(p)$, alors
$$\sum_{i=1}^{n}X_i\hookrightarrow\mathscr{B}(n,p).$$

Attention - Le même coefficient p
On soulignera qu'il faut que ce soit la même probabilité p en paramètre aux lois additionnées

Démonstration
On étudie le cas de deux variables. On généralise par récurrence.
$(X+Y)(\Omega)$ est un ensemble d'entiers consécutifs dont le plus petit est $0=0+0$ et le plus grand $n+m$.
Puis, pour tout $k\in[\![0,n+m]\!]$,
$$X+Y=k\Longleftrightarrow\bigcup_{h=\min(m-k,0)}^{\max(n,k)}X=h\cap Y=k-h$$
Par incompatibilité, puis indépendance :
$$\mathbf{P}(X+Y=k)=\sum_{h=\min(0,m-k)}^{\max(n,k)}\mathbf{P}(X=h\cap Y=k-h)=\sum_{h=\min(0,m-k)}^{\max(n,k)}\mathbf{P}(X=h)\mathbf{P}(Y=k-h)$$
En exploitant la loi binomiale :
$$\mathbf{P}(X+Y=k)=\sum_{h=\min(0,m-k)}^{\max(n,k)}\binom{n}{h}\binom{m}{k-h}p^h(1-p)^{n-h}p^{k-h}(1-p)^{m-k+h}$$
$$=\sum_{h=\min(0,m-k)}^{\max(n,k)}\binom{n}{h}\binom{m}{k-h}p^k(1-p)^{n+m-k}$$
$$=p^k(1-p)^{n+m-k}\times\sum_{h=\min(0,m-k)}^{\max(n,k)}\binom{n}{h}\binom{m}{k-h}=\binom{n+m}{k}p^k(1-p)^{n+m-k}$$
d'après la formule de Vandermonde □

Pour aller plus loin - Comment redémontrer la formule de Vandermonde
Deux stratégies :
— *par combinatoire.*
On décompose un ensemble de $m+n$ éléments en deux sous ensembles : un de n et l'autre de m éléments.
Et on calcule de deux façons différentes le nombre de sous-ensembles à k élé-

Savoir faire - Modélisation

Une suite finie $(X_i)_{1\leqslant i\leqslant n}$ de variables aléatoires indépendantes fournit un moyen de modéliser une succession de n épreuves dont les résultats sont indépendants, en particulier les répétitions indépendantes d'une même épreuve se modélisent par la donnée de n v.a. indépendantes **équidistribuées** (c'est-à-dire de même loi).
Une suite de n lancers de pile ou face aux résultats indépendants se modélise par la donnée de n v.a. indépendantes $X_1,\dots,X_n$ de loi $\mathscr{B}(p)$, X_i étant le résultat du i-ième lancer.

Exercice

Soit $(X_1,\dots,X_n)$ un n-uplet de v.a.r. indépendantes de même loi $\mathscr{B}(100,\frac{1}{5})$.
On note N la variable aléatoire égale à Card $\{k\in[\![1,n]\!]\,|\,X_k=99\}$. Déterminer la loi de N.

Correction

Notons Y_i, l'indicatrice de $[X_i=99]$. Alors Y_i suit une loi de Bernoulli,
son paramètre est $p=\mathbf{P}(Y_i=1)=\mathbf{P}(X_i=99)=\binom{100}{99}\frac{1}{5^{99}}\frac{4}{5}=\frac{99}{5^{100}}$.
Les variables X_i sont indépendantes, il en est de même des Y_i.
Notons que $N=Y_1+Y_2+\dots Y_n$, alors $S\hookrightarrow\mathscr{B}(100,p)=\mathscr{B}\left(100,\frac{99}{5^{100}}\right)$.

Exercice

Une urne contient n boules indiscernables au toucher numérotées de 1 à n.
On prélève deux boules successivement et on note X_1 (resp. X_2) la v.a. égale au numéro de la première (resp. deuxième) boule tirée. On pose $Z=\max(X_1,X_2)$.
Déterminer la loi conjointe du couple (X_1,X_2), les lois marginales, ainsi que la loi de Z dans les deux cas suivants :

— le tirage se fait avec remise ;
— le tirage se fait sans remise.

Correction

Considérons le cas avec remise.
Dans cette situation, on peut légitimement modéliser que X_1 et X_2 sont indépendantes.
On a $X_1(\Omega)=X_2(\Omega)=[\![1,n]\!]$ et pour tout $i,j\in[\![1,n]\!]$

$$\mathbf{P}(X_1=i,X_2=j)=\mathbf{P}(X_1=i)\mathbf{P}(X_2=j)=\frac{1}{n^2}$$

Les lois marginales sont (évidemment par indépendance) les lois uniformes : $\mathbf{P}(X_1=i)=\frac{1}{n}=\mathbf{P}(X_2=j)$.
Enfin, $[Z=k]=[X_1=k\cap X_2=k]\cup[X_1=k,X_2\leqslant k-1]\cup[X_1\leqslant k-1,X_2=k]$,
Par incompatibilité :

$$\mathbf{P}(Z=k)=\frac{1}{n^2}+\frac{k-1}{n^2}+\frac{k-1}{n^2}=\frac{2k-1}{n^2}$$

Considérons le cas sans remise.
Dans cette situation, on ne peut plus modéliser que X_1 et X_2 sont indépendantes.
On a toujours $X_1(\Omega)=X_2(\Omega)=[\![1,n]\!]$ et pour tout $i,j\in[\![1,n]\!]$

$$\mathbf{P}(X_1=i,X_2=j)=\begin{cases}0 & \text{si} \quad i=j\\ \frac{1}{n(n-1)} & \text{si} \quad i\neq j\end{cases}$$

Les lois marginales sont alors : $\mathbf{P}(X_1=i)=\sum_{j=1}^{n}\mathbf{P}(X_1=i,X_2=j)=\sum_{j=1,j\neq i}^{n}\frac{1}{n(n-1)}=\frac{1}{n}=\mathbf{P}(X_2=j)$.
Ainsi bien que dépendantes, X_1 et X_2 suivent encore la même que précédemment : la loi uniforme.
Enfin, $[Z=k]=[X_1=k\cap X_2=k]\cup[X_1=k,X_2\leqslant k-1]\cup[X_1\leqslant k-1,X_2=k]$,
Par incompatibilité :

$$\mathbf{P}(Z=k)=0+\frac{k-1}{n(n-1)}+\frac{k-1}{n(n-1)}=\frac{2k-2}{n(n-1)}$$

(On vérifie : $\sum_{k=1}^{n}\mathbf{P}(Z=k)=\frac{2}{n(n-1)}\sum_{k=1}^{n}(k-1)=1$)

Truc & Astuce pour le calcul - Etude du $\max(X_i)$, où les X_i sont indépendantes

On note $Z=\max(X_1,X_2,\dots X_n)$. En deux temps :

1. On constate que $Z\leqslant k\iff\forall\ i\leqslant n, X_i\leqslant k$.

Par indépendance : $\mathbf{P}(Z\leqslant k)=\prod_{i=1}^{n}\mathbf{P}(X_i\leqslant k)$

2. Revenir au cas $Z=k$:
$[Z\leqslant k]=[Z=k]\cup[Z\leqslant k-1]$, événements incompatibles,
Donc $\mathbf{P}(Z\leqslant k)=\mathbf{P}(Z=k)+\mathbf{P}(Z\leqslant k-1)$,
et $\mathbf{P}(Z=k)=\mathbf{P}(Z\leqslant k)-\mathbf{P}(Z\leqslant k-1)$

Exercice

Retrouver la loi de Z dans l'exercice précédent, en exploitant le savoir-faire

Correction

Notons la méthode suivante dans le cas indépendant : $Z\leqslant k\Leftrightarrow(X_1\leqslant k)\cap(X_2\leqslant k)$ On a donc $\mathbf{P}(Z\leqslant k)=\mathbf{P}(X_1\leqslant k)\times\mathbf{P}(X_2\leqslant k)=\frac{k^2}{n^2}$.
Et donc, comme $[Z\leqslant k]=[Z=k]\cup[Z\leqslant k-1]$, événements incompatibles,
$\mathbf{P}(Z\leqslant k)=\mathbf{P}(Z=k)+\mathbf{P}(Z\leqslant k-1)$, donc $\mathbf{P}(Z=k)=\frac{k^2-(k-1)^2}{n^2}=\frac{2k-1}{n^2}$.

4.4. Suite de variables aléatoires

Définition - Indépendance pour une suite de v.a.
Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires définies sur $(\Omega,\mathbf{P})$.
$(X_n)_{n\in\mathbb{N}}$ est une suite de variables aléatoires mutuellement indépendantes si, pour tout $n\in\mathbb{N}^*$, les variables aléatoires $X_1,\dots,X_n$ sont mutuellement indépendantes.

5. Moments d'une variable aléatoire réelle finie

$(\Omega,\mathbf{P})$ désigne un espace probabilisé fini.

5.1. Espérance

Définition - Espérance. Loi centrée
Soit X une v.a.réelle, $X(\Omega)=\{x_1,\dots,x_n\}$.
On appelle **espérance** de X le réel noté $\mathbf{E}(X)$ défini par :

$$\mathbf{E}(X)=\sum_{k=1}^{n}x_k\mathbf{P}(X=x_k)=\sum_{x\in X(\Omega)}x\mathbf{P}(X=x)$$

X est dite **centrée** si $\mathbf{E}(X)=0$.

Proposition - Espérance des lois usuelles
Soit $(\Omega,\mathbf{P})$ un espace de probabilité fini
— si X est constante égale à a alors $\mathbf{E}(X)=a$;
— si $X\hookrightarrow\mathscr{B}(p)$ alors $\mathbf{E}(X)=p$;
— si $X\hookrightarrow\mathscr{B}(n,p)$ alors $\mathbf{E}(X)=np$.

Démonstration
Au cas par cas :
— $\mathbf{E}(X)=a\mathbf{P}(X=a)=a1=a$ p.s. (presque sûrement).
— $\mathbf{E}(X)=0\mathbf{P}(X=0)+1\mathbf{P}(X=1)=0(1-p)+1p=p$.
— $\mathbf{E}(X)=\sum_{k=0}^{n}k\mathbf{P}(X=k)=\sum_{k=1}^{n}\binom{n}{k}kp^k(1-p)^{n-k}$
$=np\sum_{k=1}^{n}\binom{n-1}{k-1}p^{k-1}(1-p)^{(n-1)-(k-1)}=np(p+(1-p))^{n-1}=np$
□

Pour aller plus loin - $\int_x$
Selon la nature de $X(\omega)$, le calcul de l'espérance sera une somme (potentiellement infinie) si $X(\Omega)$ est dénombrable ou une intégrale si $X(\Omega)$ à la puissance du continue.
Pour ce dernier cas (hors-programme des

Savoir faire - Exploitation d'indicatrice (2)

Si $A \subset \Omega$ est un événement, alors $\mathbb{1}_A \hookrightarrow \mathscr{B}(\mathbf{P}(A))$ et donc $\mathbf{E}(\mathbb{1}_A) = \mathbf{P}(A)$.
On exploitera cette relation associée à des propriétés essentielles de l'espérance (linéarité…)

Proposition - Formulation équivalente

Soit X une v.a.r. On a

$$\mathbf{E}(X) = \sum_{\omega\in\Omega} X(\omega)\mathbf{P}(\{\omega\}).$$

On peut aussi noter que $X = \sum_{i=1}^{p} x_i \mathbb{1}_{[X=x_i]}$.

Démonstration

Supposons que $X(\Omega) = E = \{x_1, x_2, \dots x_p\}$, alors on peut réunir ensemble les ω selon la valeur de $X(\omega)$.

$$\sum_{\omega\in\Omega} X(\omega)P(\{\omega\}) = \sum_{i=1}^{p}\left(\sum_{\omega\in\Omega \mid X(\omega)=x_i} x_i\mathbf{P}(\{\omega\})\right) = \sum_{i=1}^{p}\left(x_i \sum_{\omega\in\Omega \mid X(\omega)=x_i} \mathbf{P}(\{\omega\})\right) = \sum_{i=1}^{p} x_i\mathbf{P}(X=x_i) = \mathbf{E}(X)$$

□

Théorème - Formule de transfert

Soient X une v.a. définie sur Ω, à valeurs dans un ensemble E et $g : X(\Omega) = \{x_1, \dots, x_n\} \to \mathbb{R}$.
Alors l'espérance de la v.a.r. $Z = g(X)$ est donnée par la formule :

$$\mathbf{E}(Z) = \sum_{k=1}^{n} g(x_k)\mathbf{P}(X=x_k) = \sum_{x\in X(\Omega)} g(x)\mathbf{P}(X=x)$$

C'est-à-dire que l'on n'a pas besoin de connaître la loi de Z pour calculer son espérance, la loi de X suffit.

Démonstration

Notons $F = Z(\Omega)$

$$\mathbf{E}(Z) = \sum_{\omega\in\Omega} Z(\omega)\mathbf{P}(\{\omega\}) = \sum_{\omega\in\Omega} g(X(\omega))\mathbf{P}(\{\omega\}) = \sum_{x\in X(\Omega)} g(x)\mathbf{P}(X=x) = \sum_{k=1}^{n} g(x_k)\mathbf{P}(X=x_k)$$

□

Corollaire - Application : pseudo-linéarité

Soient X une v.a.r., a et b deux réels. Alors $\mathbf{E}(aX+b) = a\mathbf{E}(X) + b$.
En particulier $X - \mathbf{E}(X)$ est une v.a. centrée (appelée v.a. centrée associée à X).

Démonstration

Ici $g : x \mapsto ax + b$, donc

$$\mathbf{E}(aX+b) = \sum_{x\in\Omega} (ax+b)\mathbf{P}(X=x) = a\sum_{x\in\Omega} x\mathbf{P}(X=x) + b\sum_{x\in\Omega}\mathbf{P}(X=x) = a\mathbf{E}(X) + b1$$

□

Corollaire - Espérance de couple

Soient (X,Y) un couple de v.a. définies sur Ω et $g : (X,Y)(\Omega) \to \mathbb{R}$.
Alors l'espérance de la v.a.r. $g(X,Y)$ est donnée par la formule :

$$\mathbf{E}(g(X,Y)) = \sum_{(x,y)\in(X,Y)(\Omega)} g(x,y)\mathbf{P}\big((X,Y)=(x,y)\big)$$

Démonstration

On applique à $Z : \Omega \to \mathbb{R}, \omega \mapsto g(X(\omega), Y(\omega))$ la formule de transfert.
Même si on « passe » par $\mathbb{R}^2$, il s'agit bien d'une variable aléatoire réelle. □

On peut généraliser la formule à une v.a. du type $g(X_1, \cdots, X_n)$.

Proposition - Propriétés

Si X et Y sont deux v.a.r. (plus généralement si $X_1, \cdots, X_n$ sont n v.a.r) définies sur un même espace probabilisé fini $(\Omega, \mathbf{P})$. Alors :

i) $\mathbf{E}(\lambda X + \mu Y) = \lambda\mathbf{E}(X) + \mu\mathbf{E}(Y)$ (linéarité de l'espérance)

ii) si $X \geqslant 0$ p.s. alors $\mathbf{E}(X) \geqslant 0$ (positivité de l'espérance)

iii) si $X \geqslant 0$ p.s. et $\mathbf{E}(X) = 0$ alors $X = 0$ p.s.

iv) si $X \leqslant Y$ p.s. alors $\mathbf{E}(X) \leqslant \mathbf{E}(Y)$ (croissance de l'espérance)

v) si X, Y sont indépendantes, $\mathbf{E}(XY) = \mathbf{E}(X)\mathbf{E}(Y)$

vi) $\mathbf{E}(X_1 + X_2 + \cdots + X_n) = \mathbf{E}(X_1) + \mathbf{E}(X_2) + \cdots + \mathbf{E}(X_n)$

vii) si $X_1, \cdots, X_n$ sont indépendantes, $\mathbf{E}(X_1X_2\cdots X_n) = \mathbf{E}(X_1)\mathbf{E}(X_2)\cdots\mathbf{E}(X_n)$

Pour aller plus loin - Lien avec l'intégration

Les formules suivantes rappellent en grande partie des résultat équivalent sur le calcul d'intégrale de fonctions positives.

Pour l'intégration : si $f \geqslant 0$ alors $\int_I f \geqslant 0$.

L'équivalence pour la nullité étaient assurée à condition que f soit continue (et positive).
Dans le cadre des var, la continuité n'a pas de sens, alors il est nécessaire de considérer des ***var nulle presque sûrement***

Démonstration

On démontre point par point

i) On applique la formule du couple pour $g : (x,y) \mapsto \lambda x + \mu y$.

$$\begin{aligned}\mathbf{E}(\lambda X+\mu Y) &= \sum_{(x,y)\in X(\Omega)\times Y(\Omega)} \lambda x + \mu y\mathbf{P}\big((X,Y)=(x,y)\big)\\ &= \lambda\sum_{(x,y)\in X(\Omega)\times Y(\Omega)} x\mathbf{P}\big((X,Y)=(x,y)\big) + \mu\sum_{(x,y)\in X(\Omega)\times Y(\Omega)} \mu\mathbf{P}\big((X,Y)=(x,y)\big)\\ &= \lambda\sum_{x\in X(\Omega)}\left(x\sum_{y\in Y(\Omega)}\mathbf{P}\big((X,Y)=(x,y)\big)\right) + \mu\sum_{y\in Y(\Omega)} y\left(\sum_{x\in X(\Omega)}\mathbf{P}\big((X,Y)=(x,y)\big)\right)\\ &= \lambda\sum_{x\in X(\Omega)} x\mathbf{P}\big(X=x\big) + \mu\sum_{y\in Y(\Omega)} y\mathbf{P}\big(Y=y\big) = \lambda\mathbf{E}(X) + \mu\mathbf{E}(Y)\end{aligned}$$

ii) Il s'agit d'une somme de nombre positif.

iii) Supposons que $X \geqslant 0$ p.s. et $\mathbf{E}(X) = 0$.
Soit $\epsilon > 0$ et $A_\epsilon = (X > \epsilon)$. Comme $X \geqslant 0$:

$$0\mathbf{E}(X) = \sum_{x\in E, x>\epsilon} x\mathbf{P}(X=x) + \sum_{x\in E, x\leqslant\epsilon} x\mathbf{P}(X=x) \geqslant \epsilon\mathbf{P}(A_\epsilon)$$

Donc nécessairement, pour tout $\epsilon > 0$, $\mathbf{P}(A_\epsilon) = 0$.
$X(\omega)$ est fini, positif. Si $X(\Omega)\setminus\{0\}$ et non vide, on peut considérer $\epsilon = \frac{1}{2}\min(X(\Omega)\setminus\{0\})$.
Alors $\mathbf{P}(X>\epsilon) = \sum_{x\neq 0}\mathbf{P}(X=x) = 0$, ce qui signifie que pour tout $x \in X(\Omega)$, $x \neq 0$, alors $\mathbf{P}(X=x) = 0$.
Donc $\mathbf{P}(X=0) = 1$, donc $X = 0$ p.s.

iv) Soit $Z = Y - X \geqslant 0$ p.s. Donc $\mathbf{E}(Z) \geqslant 0$.
Puis par linéarité de l'espérance : $\mathbf{E}(X) \leqslant \mathbf{E}(Y)$.

v) Supposons que X, Y sont indépendantes, avec $g : (x,y) \mapsto x \times y$

$$\mathbf{E}(XY) = \sum_{(x,y)\in(X,Y)(\Omega)} xy\mathbf{P}\big((X,Y)=(x,y)\big) = \sum_{x\in X(\Omega)}\left(x\sum_{y\in Y(\Omega)} y\mathbf{P}\big((X,Y)=(x,y)\big)\right)$$

Et par indépendance :

$$\mathbf{E}(XY) = \sum_{x\in X(\Omega)}\left(x\sum_{y\in Y(\Omega)} y\mathbf{P}(X=x)\mathbf{P}(Y=y)\right) = \sum_{x\in X(\Omega)}(x\mathbf{P}(X=x)\mathbf{E}(Y)) = \mathbf{E}(X)\mathbf{E}(Y)$$

vi) Notons $r_n = \mathbf{E}(X_1 + X_2 + \cdots + X_n) - (\mathbf{E}(X_1) + \mathbf{E}(X_2) + \cdots + \mathbf{E}(X_n))$ D'après le point i)

$$r_{n+1} = \mathbf{E}(X_1 + X_2 + \cdots + X_n + X_{n+1}) - (\mathbf{E}(X_1) + \mathbf{E}(X_2) + \cdots + \mathbf{E}(X_n) + \mathbf{E}(X_{n+1})) = r_n$$

Donc r_n est une suite constante. Et comme $r_1 = 0$, on en déduit :

$$\mathbf{E}(X_1 + X_2 + \cdots + X_n) = \mathbf{E}(X_1) + \mathbf{E}(X_2) + \cdots + \mathbf{E}(X_n)$$

vii) Supposons $X_1, \cdots, X_n$ indépendantes, et notons pour $k \leqslant n$, $s_k = \dfrac{\mathbf{E}(X_1 X_2 \cdots X_k)}{\mathbf{E}(X_1)\mathbf{E}(X_2)\cdots\mathbf{E}(X_k)}$
D'après le point v), puisque X_{k+1} est indépendante de la variable $X_1 X_2 \cdots X_k$,

$$s_{k+1} = \frac{\mathbf{E}(X_1 X_2 \cdots X_k X_{k+1})}{\mathbf{E}(X_1)\mathbf{E}(X_2)\cdots\mathbf{E}(X_k)\mathbf{E}(X_{k+1})} = s_k$$

Donc s_n est une suite constante. Et comme $s_1 = 1$, on en déduit :

$$\mathbf{E}(X_1 X_2 \cdots X_n) = \mathbf{E}(X_1)\mathbf{E}(X_2)\cdots\mathbf{E}(X_n)$$

□

Remarque - Espérance d'une loi binomiale
On peut ainsi retrouver facilement l'espérance d'une v.a. binomiale : c'est une somme de n Bernoulli.
Exercice
Faites le calcul

Correction
On suppose que $X = X_1 + X_2 + \ldots X_n$, indépendantes.

$$\mathbf{E}(X) = \mathbf{E}(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} \mathbf{E}(X_i) = np$$

(l'indépendance ne sert pas !)

Proposition - Inégalité de Markov
Toute v.a.r. positive sur Ω fini vérifie l'inégalité :

$$\forall a > 0, \mathbf{P}(X \geqslant a) \leqslant \frac{\mathbf{E}(X)}{a}$$

Savoir faire - Exploitation d'indicatrice (3)
Il y a un événement naturel à étudier ici $A = [X \geqslant a]$, puis on exploite la propriété de l'espérance de la variable $\mathbb{1}_A$.

Démonstration
On note $A = [X \geqslant a]$. Notons que $X \geqslant a\mathbf{1}_{[X \geqslant a]} + 0$, puisque X est positif.

$$\mathbf{P}(X \geqslant a) = \mathbf{E}(\mathbf{1}_A) \leqslant \frac{1}{a}\mathbf{E}(X)$$

par linéarité de l'espérance. □

Exercice
Soit X, une variable aléatoire à valeurs entières.
Montrer que $\mathbf{P}(X = 0) \geqslant 1 - \mathbf{E}(X)$

Correction
On a $X \geqslant 0$, on peut appliquer la formule de Markov pour $a = 1$.

$$\mathbf{P}(X = 0) = 1 - \mathbf{P}(X \geqslant 1) \geqslant 1 - \frac{\mathbf{E}(X)}{1}$$

Savoir faire - Composition avec exp (pour avoir une va positive). Méthode de Chernoff
Il arrive fréquemment qu'on compose avec exp la variable X. On parle de comparaison avec des vecteurs sous-gaussiens.
On a alors $\mathbf{P}(X \geqslant x) = \mathbf{P}(e^X \geqslant e^x) \leqslant \dfrac{\mathbf{E}(e^X)}{e^x}$.

Pour aller plus loin - Minoration de la probabilité d'absence (ou majoration de présence)
On trouve pour $X(\Omega) \in \mathbb{N}$, $\mathbf{P}(X = 0) \geqslant 1 - \mathbf{E}(X)$, une minoration de la probabilité d'absence

Exercice
On suppose que $X(\Omega) = \{-2, -1, 0, 1, 2\}$, avec $p_2 = \mathbf{P}(X = 2) = \mathbf{P}(X = -2)$ et $p_1 = \mathbf{P}(X = 1) = \mathbf{P}(X = -1)$.
Majorer $\mathbf{P}(X \geqslant e)$.

Correction
$Y = \exp(X)$ est une variable aléatoire positive.
On a l'égalité d'événements : $X \geqslant e \iff Y \geqslant e^e$ par croissance de exp.
Enfin $\mathbf{E}(Y) = p_2 e^{-2} + p_1 e^{-1} + (1 - p_2 - p_1)e^0 + p_1 e^1 + p_2 e^2 = p_2(2\operatorname{ch}(2) - 1) + p_1(2\operatorname{ch}(1) - 1) + 1$.
En appliquant l'inégalité de Markov à Y, on trouve

$$\mathbf{P}(X \geqslant e) = \mathbf{P}(Y \geqslant e^e) \leqslant \frac{p_2(2\operatorname{ch}(2) - 1) + p_1(2\operatorname{ch}(1) - 1) + 1}{e^e}$$

5.2. Variance (d'une variable aléatoire)

Définition - Moment d'ordre r
Soit X une v.a.r. sur $(\Omega, \mathbf{P})$ fini. On appelle **moment d'ordre r** ($r \in \mathbb{N}$) de X le réel $m_r(X) = \mathbf{E}(X^r)$ et **moment centré d'ordre r** de X le réel $\mu_r(X) = \mathbf{E}[(X - \mathbf{E}(X))^r]$.

Savoir faire - Formulation calculatoire (transfert) - moment
Si X est centrée : $\mu_r(X) = \sum_{x \in X(\Omega)} x^r \mathbf{P}(X = x)$.

Définition - Variance et écart-type
Soit X une v.a.r. sur $(\Omega, \mathbf{P})$ fini. On appelle **variance** de X, notée $\mathbf{V}(X)$, le moment centré d'ordre 2 de X : $\mathbf{V}(X) = \mathbf{E}\left((X - \mathbf{E}(X))^2\right)$.
$\sigma(X) = \sqrt{\mathbf{V}(X)}$ est appelé **écart-type** de X.
Si $\sigma(X) = 1$ on dit que X est **réduite**.

Remarque - Positivité de la variance
On notera que $Y = \left(X - \mathbf{E}(X)\right)^2 \geqslant 0$, donc $\mathbf{V}(X) = \mathbf{E}(Y) \geqslant 0$.

Savoir faire - Formulation calculatoire (transfert) - variance
On a donc $\mathbf{V}(X) = \sum_{x \in X(\Omega)} (x - \mathbf{E}(X))^2 \mathbf{P}(X = x)$.

Proposition - Propriétés
Soit $(\Omega, \mathbf{P})$ un espace de probabilité fini. Alors
- **i)** $\mathbf{V}(X) = \mathbf{E}(X^2) - \mathbf{E}(X)^2$ formule de Huygens
- **ii)** $\mathbf{V}(aX + b) = a^2\mathbf{V}(X)$
- **iii)** $\sigma(aX + b) = |a|\sigma(X)$
- **iv)** si $\sigma(X) > 0$, $X^* = \frac{X - \mathbf{E}(X)}{\sigma(X)}$ est centrée réduite, on l'appelle **v.a. centrée réduite associée** à X
- **v)** $\mathbf{V}(X) = 0 \Leftrightarrow X$ est constante presque sûrement

Exemple - Variance de la loi uniforme sur $[\![1, n]\!]$.
Avec la formule de Huygens (et transfert) :

$$\mathbf{V}(U) = \sum_{k=1}^{n} \frac{k^2}{n} - \left(\frac{n+1}{2}\right)^2 = \frac{(n+1)(2n+1)}{6} - \frac{(n+1)^2}{4} = \frac{(n+1)(2(n+1) - 3(n+1))}{12}$$

Donc $\mathbf{V}(U) = \dfrac{n^2 - 1}{12}$

Démonstration
Un par un :

i) Par pseudo-linéarité : comme $\mathbf{E}(X)=e$ est un nombre,

$$\mathbf{V}(X)=\mathbf{E}\big((X-\mathbf{E}(X))^2\big)=\mathbf{E}(X^2-2e\mathbf{E}(X)+e^2)=\mathbf{E}(X^2)-2e\mathbf{E}(X)+e^2=\mathbf{E}(X^2)-e^2$$

ii) $\mathbf{E}(aX+b)=a\mathbf{E}(X)+b$, donc

$$\mathbf{V}(aX+b)=\mathbf{E}\big((aX+b-\mathbf{E}(aX+b))^2\big)=\mathbf{E}\big(a^2(X-\mathbf{E}(X))^2\big)=a^2\mathbf{V}(X)$$

iii) Donc $\sigma(aX+b)=\sqrt{\mathbf{V}(aX+b)}=\sqrt{a^2}\sqrt{\mathbf{V}(X)}=|a|\sigma(X)$

iv) D'après les calculs précédents,

$$\mathbf{E}(X^*)=\frac{1}{\sigma(X)}\mathbf{E}\big(X-\mathbf{E}(X)\big)=\frac{1}{\sigma(X)}\big(\mathbf{E}(X)-\mathbf{E}(X)\big)=0$$

$$\mathbf{V}(X^*)=\frac{1}{\sigma^2(X))}\mathbf{V}(X)=1$$

Donc $X^*=\dfrac{X-\mathbf{E}(X)}{\sigma(X)}$ est centrée réduite

v) Si $X=a$ presque sûrement, alors $\mathbf{P}(X=a)=1$,
$\mathbf{E}(X)=a$ et $\mathbf{V}(X)=\mathbf{E}(X-a)=0\mathbf{P}(X=a)=0$.
Réciproquement, supposons qu'il existe $a\neq b$ tel que $\mathbf{P}(X=a)>0$ et $\mathbf{P}(X=b)>0$.
Notons $e=\mathbf{E}(X)$

$$\mathbf{V}(X)=\mathbf{E}((X-e)^2)=(a-e)^2\mathbf{P}(X=a)+(b-e)^2\mathbf{P}(X=b)+\sum_{x\neq a,b}(x-e)^2\mathbf{P}(X=x)\geqslant(a-e)^2\mathbf{P}(X=a)+(b-e)^2\mathbf{P}(X=b)$$

Or comme $a\neq b$, au moins un des deux nombres $(a-e)$ ou $(b-e)^2$ est non nul.
Ainsi $\mathbf{V}(X)>0$

□

Proposition - Variance des lois usuelles
— si $X\hookrightarrow\mathscr{B}(p)$ alors $\mathbf{V}(X)=p(1-p)$;
— si $X\hookrightarrow\mathscr{B}(n,p)$ alors $\mathbf{V}(X)=np(1-p)$.

Démonstration
Supposons que $X\hookrightarrow\mathscr{B}(p)$.

$$\mathbf{V}(X)=(0-p)^2(1-p)+(1-p)^2p=p(1-p)[p+(1-p)]=p(1-p)$$

Supposons que $X\hookrightarrow\mathscr{B}(n,p)$. Comme $(X-\mathbf{E}(X))^2=X^2-2\mathbf{E}(X)X+[\mathbf{E}(X)]^2=X(X-1)+(1-2\mathbf{E}(X))X+\mathbf{E}(X)^2$,

$$\mathbf{V}(X)=\mathbf{E}\big(X(X-1)+(1-2\mathbf{E}(X))X+\mathbf{E}(X)^2\big)=\mathbf{E}(X(X-1))+(1-2\mathbf{E}(X))\mathbf{E}(X)+\mathbf{E}(X)^2=\mathbf{E}(X(X-1))+\mathbf{E}(X)-\mathbf{E}(X)^2)$$

Et ici $\mathbf{E}(X)=np$, on a donc

$$\mathbf{V}(X)=\sum_{k=0}^{n}\binom{n}{k}(k(k-1)p^k(1-p)^{n-k}+np-n^2p^2)$$

$$=n(n-1)p^2(p+(1-p))^{n-2}+np-n^2p^2)=n^2p^2-np^2+np-n^2p^2$$

$$\mathbf{V}(X)=np(1-p)$$

□

Remarque - A propos de la loi hypergéométrique
Il est bon de connaître et reconnaître la loi définie dans l'exercice suivant. C'est la loi hypergéométrique.
Il s'agit d'une sorte de répétition de loi de Bernoulli, avec dépendance cette fois-ci.
Notons enfin que dans l'exercice, on considère une succession de tirage sans remise. Le résultat est identique (même loi) si l'on considère plutôt un tirage d'une poignée de n boules.

Exercice
Une urne contient N boules, de deux catégories : des blanches en proportion p et des non blanches en proportion $q=1-p$ ($Np\in\mathbb{N}$ désigne donc le nombre de boules blanches et $Nq\in\mathbb{N}$ celui de non blanches).
On tire successivement n boules de cette urne **sans remise** et on note X la v.a. égale au nombre de boules blanches obtenues.
Déterminer la loi de X, son espérance et sa variance (on pourra, pour cette dernière, commencer par calculer $\mathbf{E}(X(X-1))$).

Correction
Remarque : On note $X_i=1$, si la boule est blanche lors du tirage i et $X_i=0$ sinon.

En fait $X=\sum_{i=1}^{n}X_i$, où chaque X_i suit une loi binomiale.
Mais il n'y a plus d'indépendance. Mais cela n'est pas trop grave concernant le calcul de l'espérance.

On va raisonner avec une méthode ensembliste.
On pourrait essayer de considérer Ω sous la forme $\{B,N\}^N$, mais il faudrait ajouter des conditions (pas de tirages à nouveau, précision sur les boules…).
On va plutôt considérer que les N boules sont numérotés de 1 à N (les Np premières sont blanches).
Un tirage de n boules consiste à créer une fonction f injective de $[\![1,n]\!]$ sur $[\![1,N]\!]$, avec $f(k)$ indiquant le numéro de la boule tirée au k tirage. Donc $\text{Card}\,(\Omega)=A_N^n=\dfrac{N!}{(N-n)!}$.
On note $X(\Omega)=[\![\min(0,Nq),\max(n,Np)]\!]$ Puis $\text{Card}\,([X=k])=\binom{k}{n}A_{Np}^k\times A_{n-k}^{Nq}$, en effet un tel tirage est constitué de

1. le choix des k tirages qui donnent une boule blanche (formant l'ensemble I_k)
2. l'injection de I_k sur $[\![1,Np]\!]$
3. l'injection de $\overline{I_k}$ sur $[\![Np+1,N]\!]$

Et donc

$$\mathbf{P}(X=k)=\frac{n!Np!Nq!(n-k)!}{k!(n-k)!(Np-k)!(Nq-n+k)!n!}=\frac{Np!Nq!}{k!(Np-k)!(Nq-n+k)!}=\frac{\binom{Np}{k}\binom{Nq}{n-k}}{\binom{N}{n}}$$

On vérifie que $\sum_{\min(0,Nq)}^{\max(n,Np)}\mathbf{P}(X=k)=1$, c'est la formule de Vandermonde.
En outre

$$\mathbf{E}(X)=\frac{1}{\binom{N}{n}}\sum_{k=\min(0,Nq)}^{\max(n,Np)}k\binom{Np}{k}\binom{Nq}{n-k}=\frac{Np}{\binom{N}{n}}\sum_{k=\min(1,Nq-1)}^{\max(n,Np)}\binom{Np-1}{k-1}\binom{Nq}{n-k}=Np\frac{\binom{N-1}{n-1}}{\binom{N}{n}}=\frac{nNp}{N}=np$$

De même :

$$\mathbf{E}(X(X-1))=\frac{1}{\binom{N}{n}}\sum_{k=\min(0,Nq)}^{\max(n,Np)}k(k-1)\binom{Np}{k}\binom{Nq}{n-k}=\frac{Np(Np-1)}{\binom{N}{n}}\sum_{h=\min(0,Nq)}^{\max(n-2,Np-2)}\binom{Np-2}{h}\binom{Nq}{n-2-h}=\frac{pn(n-1)(Np-1)}{N-1}$$

Donc

$$\mathbf{V}(X)=\mathbf{E}(X(X-1))+\mathbf{E}(X)-\mathbf{E}(X)^2=\frac{pn(n-1)(Np-1)}{N-1}+np-n^2p^2=\frac{p^2n^2N-pn^2-npN+np+npN-np-n^2p^2N+n^2p^2}{N-1}$$

$$\mathbf{V}(X)=\frac{np(pN-n+N+np}{N-1}=\frac{npq(N-n)}{N-1}$$

où $q=1-p$

Théorème - Inégalité de Bienaymé-Tchebychev
Soit X une v.a.r. sur $(\Omega,\mathbf{P})$ fini. Alors :

$$\forall\,\epsilon>0,\ \mathbf{P}(|X-\mathbf{E}(X)|\geqslant\epsilon)\leqslant\frac{\mathbf{V}(X)}{\epsilon^2}$$

Pour aller plus loin - Majoration de la probabilité d'absence (ou minoration de présence)
On trouve pour $X(\Omega)\in\mathbb{N}$, $\mathbf{P}(X=0)\leqslant\dfrac{\mathbf{V}(X)}{\mathbf{E}(X)^2}$, une majoration de la probabilité d'absence

Démonstration
On applique l'inégalité de Markov à $Y=(X-\mathbf{E}(X))^2$, il s'agit bien d'une variable aléatoire positive.
Notons alors l'égalité des événements :

$$|X-\mathbf{E}(X)|\geqslant\epsilon\Longleftrightarrow Y>\epsilon^2$$

Donc, en notant $a=\epsilon^2$

$$\mathbf{P}(|X-\mathbf{E}(X)|\geqslant\epsilon)=\mathbf{P}(Y>a)\leqslant\frac{\mathbf{E}(Y)}{a}=\frac{\mathbf{E}((X-\mathbf{E}(X))^2)}{\epsilon^2}=\frac{\mathbf{V}(X)}{\epsilon^2}$$

□

Exercice
Soit X, une variable aléatoire à valeurs entières.
Montrer que $\mathbf{P}(X=0)\leqslant\dfrac{\mathbf{V}(X)}{\mathbf{E}(X)^2}$

Correction
On a $X\leqslant 0$, on peut appliquer la formule de Tchebychev avec $\epsilon=\mathbf{E}(X)$.

$$|X-\mathbf{E}(X)|\leqslant\mathbf{E}(X)\Longleftrightarrow-2\mathbf{E}(X)\leqslant X\leqslant 0$$

Or $X\geqslant 0$, donc $|X-\mathbf{E}(X)|\leqslant\mathbf{E}(X)\Longleftrightarrow X=0$.

$$\mathbf{P}(X=0)=\mathbf{P}(|X-\mathbf{E}(X)|\leqslant\mathbf{E}(X))\leqslant\frac{\mathbf{V}(X)}{\mathbf{E}(X)^2}$$

5.3. Covariance (de deux variables aléatoires)

Définition - Covariance
Soient X, Y deux v.a.r sur (Ω, P) fini. On appelle **covariance** de X et Y le réel :

$$\mathbf{Cov}(X,Y) = \mathbf{E}\Big(\big(X-\mathbf{E}(X)\big)\big(Y-\mathbf{E}(Y)\big)\Big)$$

Exemple - Application
Considérons deux variables aléatoires X et Y dont le la loi conjointe est donnée par le tableau :

$X\backslash Y$	0	1	2
0	$\frac{1}{6}$	0	$\frac{1}{6}$
1	$\frac{1}{6}$	$\frac{1}{6}$	0
2	0	$\frac{1}{3}$	0

On a $X(\Omega) = \{0,1,2\} = Y(\Omega)$, puis $\mathbf{E}(X) = \frac{1}{3} + \frac{2}{3} = 1$ et $\mathbf{E}(Y) = \frac{1}{2} + \frac{1}{3} = \frac{5}{6}$.
La covariance de X et Y est alors :

$$\mathbf{Cov}(X,Y) = \mathbf{E}((X-1)(Y-\tfrac{5}{6})) = \frac{1}{6}(-1)(-\tfrac{5}{6}) + \frac{1}{6}(-1)(2-\tfrac{5}{6}) + \frac{1}{6}(1-1)(-\tfrac{5}{6}) + \frac{1}{6}(1-1)(1-\tfrac{5}{6}) + \frac{1}{3}(2-1)(1-\tfrac{5}{6})$$

$$\mathbf{Cov}(X,Y) = \frac{5}{36} - \frac{7}{36} + \frac{1}{18} = 0$$

Proposition - Propriétés de la covariance
Soient X, X', Y, Y' des v.a.r. sur $(\Omega, \mathbf{P})$ fini et $a, b, c, d, \lambda \in \mathbb{R}$. On a

i) $\mathbf{Cov}(X,Y) = \mathbf{E}(XY) - \mathbf{E}(X)\mathbf{E}(Y)$

ii) $\mathbf{Cov}(aX+b, cY+d) = ac\mathbf{Cov}(X,Y)$

iii) $\mathbf{Cov}(X,Y) = \mathbf{Cov}(Y,X)$

iv) $\mathbf{Cov}(X,X) = \mathbf{V}(X)$

v) $\mathbf{Cov}(X+X',Y) = \mathbf{Cov}(X,Y) + \mathbf{Cov}(X',Y)$ et $\mathbf{Cov}(\lambda X, Y) = \lambda \mathbf{Cov}(X,Y)$
$\mathbf{Cov}(X, Y+Y') = \mathbf{Cov}(X,Y) + \mathbf{Cov}(X,Y')$ et $\mathbf{Cov}(X, \lambda Y) = \lambda \mathbf{Cov}(X,Y)$

Démonstration
Une par une :

i) On développe :

$$\mathbf{Cov}(X,Y) = \mathbf{E}\big(XY - \mathbf{E}(X)Y - \mathbf{E}(Y)X + \mathbf{E}(X)\mathbf{E}(Y)\big) =$$
$$= \mathbf{E}(XY) - \mathbf{E}(X)\mathbf{E}(Y) - \mathbf{E}(Y)\mathbf{E}(X) + \mathbf{E}(X)\mathbf{E}(Y) = \mathbf{E}(XY) - \mathbf{E}(X)\mathbf{E}(Y)$$

ii) $\mathbf{Cov}(aX+b, cY+d) = \mathbf{E}\big((aX+b)(cY+d)\big) - \mathbf{E}(aX+b)\mathbf{E}(cY+d) = ac\mathbf{E}(XY) + bc\mathbf{E}(Y) + ad\mathbf{E}(X) + bd - (a\mathbf{E}(X)+b)(c\mathbf{E}(Y)+d) = ac\mathbf{E}(XY) - ac\mathbf{E}(X)\mathbf{E}(Y) = ac\mathbf{Cov}(X,Y)$

iii) C'est immédiat car le produit de variable aléatoire est commutatif : $\mathbf{Cov}(X,Y) = \mathbf{Cov}(Y,X)$

iv) Il suffit de remplacer Y par X et on retrouve les formules de la variance (définition et Huygens) : $\mathbf{Cov}(X,X) = \mathbf{V}(X)$

v) Par symétrie (iii)) et pseudo-linéarité (ii)), il suffit ici de démontrer la première des relation

$$\mathbf{Cov}(X+X', Y) = \mathbf{E}((X+X')Y) - \mathbf{E}(X+X')\mathbf{E}(Y)$$
$$= \mathbf{E}(XY) + \mathbf{E}(X'Y) - \mathbf{E}(X)\mathbf{E}(Y) - \mathbf{E}(X')\mathbf{E}(Y) = \mathbf{Cov}(X,Y) + \mathbf{Cov}(X',Y)$$

□

Remarque - Cov comme un produit scalaire
La dernière propriété est répétée pour souligner le caractère de la bilinéarité de **Cov** sur l'espace $(\Omega, \mathbf{P})$.
Est-ce un produit scalaire?
On a également : $\mathbf{Cov}(X,X) = \mathbf{V}(X) \geqslant 0$.
En revanche, on n'a pas : $\mathbf{Cov}(X,X) = 0 \Rightarrow X = 0$. Seulement $X = c$ (une constante) p.s.
On peut alors changer l'égalité pour obtenir un produit scalaire : $X \doteq Y$, pour exprimer $\mathbf{V}(X-Y) = 0$.

Pour aller plus loin - $\mathbf{Cov}(X) = 0 \Longrightarrow X = 0$ ***ps.***
On retrouve le même problème que pour l'intégrale

C'est bien une relation d'équivalence. On préfère noter $X = Y + c$ p.s. (lire presque sûrement),
la valeur de c est alors $\mathbf{E}(X) - \mathbf{E}(Y)$.
C'est équivalent à : $\{\omega \mid X(\omega) - \mathbf{E}(X) \neq Y(\omega) - \mathbf{E}(Y)\} = [(X-Y) \neq \mathbf{E}(X-Y)]$ a une probabilité nulle.
Si les variables aléatoires X et Y ne sont pas indépendantes :

Théorème - Lien variance-covariance
Pour des v.a.r. définies sur $(\Omega, \mathbf{P})$ fini, on a

$$\mathbf{V}(X+Y) = \mathbf{V}(X) + \mathbf{V}(Y) + 2\mathbf{Cov}(X,Y)$$

$$\mathbf{V}(X_1 + \cdots + X_n) = \mathbf{V}(X_1) + \cdots + \mathbf{V}(X_n) + 2\sum_{i<j} \mathbf{Cov}(X_i, X_j) = \sum_{i,j} \mathbf{Cov}(X_i, X_j)$$

Démonstration
$\mathbf{V}(X+Y) = \mathbf{E}((X+Y)^2) - [\mathbf{E}(X+Y)]^2 = \mathbf{E}(X^2) + 2\mathbf{E}(XY) + \mathbf{E}(Y^2) - [\mathbf{E}(X)]^2 - 2\mathbf{E}(X)\mathbf{E}(Y) - [\mathbf{E}(Y)]^2 = \mathbf{V}(X) + \mathbf{V}(Y) + 2\mathbf{Cov}(X,Y)$.
Puis par récurrence, et linéarité à gauche de la covariance :

$$\mathbf{V}(X_1 + \cdots + X_n + X_{n+1}) = \mathbf{V}(\sum_{i=1}^{n} X_i + X_{n+1}) = \mathbf{V}(\sum_{i=1}^{n} X_i) + \mathbf{V}(X_{n+1}) + 2\mathbf{Cov}((\sum_{i=1}^{n} X_i), X_{n+1})$$

$$= \sum_{i=1}^{n} \mathbf{V}(X_i) + 2\sum_{1 \leqslant i < j \leqslant n} \mathbf{Cov}(X_i, X_j) + \mathbf{V}(X_{n+1}) + 2\sum_{i=1}^{n} \mathbf{Cov}(X_i, X_{n+1})$$

Donc, l'hérédité est vérifiée :

$$\mathbf{V}(X_1 + X_2 + \cdots + X_{n+1}) = \mathbf{V}(X_1) + \mathbf{V}(X_2) + \cdots + \mathbf{V}(X_{n+1}) + 2\sum_{1 \leqslant i < j \leqslant n} \mathbf{Cov}(X_i, X_j) = \sum_{i,j} \mathbf{Cov}(X_i, X_j)$$

□

Théorème - Cas d'indépendance
Si X et Y sont deux v.a. **indépendantes** (plus généralement si $X_1, \cdots, X_n$ sont n v.a. **deux à deux indépendantes**) définies sur un même espace probabilisé fini. Alors :

i) $\mathbf{Cov}(X,Y) = 0$ (on dit que X et Y sont **non corrélées**)

ii) $\mathbf{V}(X+Y) = \mathbf{V}(X) + \mathbf{V}(Y)$

iii) $\mathbf{V}(X_1 + X_2 + \cdots + X_n) = \mathbf{V}(X_1) + \mathbf{V}(X_2) + \cdots + \mathbf{V}(X_n)$

D'une certaines façons, deux variables aléatoires non corrélées sont orthogonales pour le pseudo-produit scalaire **Cov** d'où la notation :

Définition - Variables non corrélées (notation)
Si X et Y sont deux variables aléatoires, non corrélées (i.e. $\mathbf{Cov}(X,Y) = 0$), on note $X \perp Y$.
On a donc $X \perp\!\!\!\perp Y \Longrightarrow X \perp Y$

Démonstration
On a vu que si X et Y sont indépendantes, $\mathbf{E}(XY) = \mathbf{E}(X)\mathbf{E}(Y)$, ce qui signifie exactement que $\mathbf{Cov}(X,Y) = \mathbf{E}(XY) - \mathbf{E}(X)\mathbf{E}(Y) = 0$.
Puis $\mathbf{V}(X+Y) = \mathbf{V}(X) + \mathbf{V}(Y) - 2\mathbf{Cov}(X,Y) = \mathbf{V}(X) + \mathbf{V}(Y)$.
Le cas généralisé tombe simplement par récurrence. □

Remarque - Variance d'une binomiale
On peut ainsi retrouver facilement la variance d'une v.a. binomiale.
Comme lors d'un exercice précédent, $\mathbf{V}(X) = \sum_{i=1}^{n} \mathbf{V}(X_i) = np(1-p)$.
Ce coup-ci l'indépendance est très importante.
La variance d'une hypergéométrique (addition de Bernoulli non indépendantes) est plus compliquée.

Attention - La réciproque est fausse.
Cela signifie que deux var peuvent avoir une covariance nulle (ou plus loin un coefficient de corrélation linéaire), sans être indépendantes.

Exercice
Soit X et Y deux variables aléatoires qui suivent une loi de Bernoulli et telles que la loi conjointe est donnée par le tableau :

$Y\backslash X$	0	1
0	a	b
1	c	d

1. Calculer la $\mathbf{Cov}(X,Y)$.
2. Montrer que (X,Y) sont indépendantes ssi la matrice est de rang 1.
   En déduire que si (X,Y) sont indépendantes, il existe $\lambda,\mu>0$ tel que $b=\lambda d$, $c=\lambda d$ et $a=\lambda\mu d$.
   Calculer $\mathbf{Cov}(X,Y)$
3. Montrer que dans ce cas $\mathbf{Cov}(X,Y)=0$ si et seulement si X et Y sont indépendantes.

Correction
On suppose $d\neq 0$ sinon $XY=0$ p.s.

1. $XY\hookrightarrow\mathscr{B}(d)$, donc $\mathbf{E}(XY)=d$.
   Alors que $\mathbf{P}(X=1)=b+d$, donc $\mathbf{E}(X)=b+d$ et de même $\mathbf{E}(Y)=c+d$.
   Donc $\mathbf{Cov}(X,Y)=d-(b+d)(c+d)$
2. L'indépendance entre X et Y est donnée ssi la matrice est de rang 1 i.e. $\exists\,\lambda\mu$ tel que $b=\lambda d$, $c=\mu d$, $a=\lambda\mu d$ et $d(1+\lambda+\mu+\lambda\mu)=d(1+\lambda)(1+\mu)=1$ Dans ce cas $\mathbf{Cov}(X,Y)=d-d^2(1+\lambda)(1+\mu)d-d=0$.
3. Si X et Y ne sont pas indépendants, en notant $\lambda=\frac{b}{d}$ et $\mu=\frac{c}{d}$.
   On a toujours $\mathbf{Cov}(X,Y)=d-d^2(1+\lambda)(1+\mu)=d(1-(d+b+c+\lambda\mu d)=d(a-\lambda\mu d))$.
   Et donc $\mathbf{Cov}(X,Y)=0\Rightarrow a=\lambda\mu d$, donc X et Y indépendantes.

Analyse - Inégalité de Cauchy-Schwarz
Si **Cov** définit un produit scalaire, que devient l'inégalité de Cauchy-Schwarz?

$$\mathbf{Cov}(X,Y)\leqslant\sqrt{\mathbf{V}(X)}\sqrt{\mathbf{V}(Y}=\sigma(X)\sigma(Y)$$

On a alors égalité ssi $X-\mathbf{E}(X)$ et $Y-\mathbf{E}(Y)$ sont colinéaires presque sûrement.
C'est-à-dire, (si X est non nul) : il existe $a\in\mathbb{R}$ tel que $Y=aX+a\mathbf{E}(X)-\mathbf{E}(Y)$ p.s.

Définition - Coefficient de corrélation linéaire
Soient X et Y deux v.a. d'écart type non nul, (i.e. X,Y non constants presque sûrement).
On appelle **coefficient de corrélation linéaire** de X et Y le réel

$$\rho(X,Y)=\frac{\mathbf{Cov}(X,Y)}{\sigma(X)\sigma(Y)}$$

Proposition - Propriétés
$|\rho(aX+b,cY+d)|=|\rho(X,Y)|$.
On a toujours $|\rho(X,Y)|\leqslant 1$, c'est-à-dire $|\mathbf{Cov}(X,Y)|\leqslant\sigma(X)\sigma(Y)$, et $|\rho(X,Y)|=1$ si et seulement si il existe a et b réels tels que $Y=aX+b$ presque sûrement, c'est-à-dire tels que $\mathbf{P}(Y=aX+b)=1$.

Démonstration
$|\rho(aX+b,cY+d)|=\left|\frac{\mathbf{Cov}(aX+b,cY+d)}{\sigma(aX+b)\sigma(cY+d)}\right|=\frac{|ac||\mathbf{Cov}(X,Y)|}{|a|\sigma(X)|c|\sigma(Y)}=|\rho(X,Y)|$.
Par ailleurs, en développant $P:t\mapsto\mathbf{V}(X+tY)\geqslant 0$,

$$P(t)=\mathbf{V}(X)+2t\mathbf{Cov}(X,Y)+t^2\mathbf{V}(Y)$$

Donc $\Delta=4|\mathbf{Cov}(X,Y)|^2-4\mathbf{V}(Y)\mathbf{V}(X)\leqslant 0$, i.e. en prenant la racine : $|\mathbf{Cov}(X,Y)|\leqslant\sigma(X)\sigma(Y)$.
(On ne peut pas appliquer CS car ce n'est pas directement un produit scalaire, il faut donc le redémontrer).
Et l'on a

$$|\rho(X,Y)=1|\Longleftrightarrow\Delta=0\Longleftrightarrow\exists\,t_0\mid P(t_0)=0\Longleftrightarrow\exists\,t_0\mid\mathbf{V}(X+t_0Y)=0$$
$$\Longleftrightarrow\exists\,t_0,c\mid X+t_0Y=c\text{p.s.}\Longleftrightarrow\exists\,a,b\mid Y=aX+b\text{ p.s.}$$

□

Savoir faire - Tableau récapitulatif
On considère p un réel de l'intervalle $]0,1[$ et on pose $q=1-p$.

nom	$X(\Omega)$	loi	espérance	variance
v.a constante (certaine)	$\{a\}$	$P(X=a)=1$	a	0
loi uniforme sur $[\![1,n]\!]$ $\mathscr{U}_n$	$[\![1,n]\!]$	$P(X=k)=\frac{1}{n}$	$\frac{n+1}{2}$	$\frac{n^2-1}{12}$
loi de Bernoulli de paramètre p $\mathscr{B}_p$ ou $\mathscr{B}(1,p)$	$\{0,1\}$	$P(X=0)=q$ $P(X=1)=p$	p	pq
loi binomiale de paramètres n,p $\mathscr{B}(n,p)$	$[\![0,n]\!]$	$P(X=k)=\binom{n}{k}p^k(1-p)^{n-k}$	np	npq

6. Bilan

Synthèse

- Une variable aléatoire, issue d'une expérience, prend différentes valeurs numériques en fonction de l'état de l'univers. Il s'agit donc d'une fonction $X:\Omega\to\mathbb{R}$. La connaissance de l'univers est d'ailleurs souvent réduite à l'image donnée par différents $X_i(\Omega)$. Réciproquement, on peut partitionner Ω en fonction de $X^{-1}(k)$, où $k\in X(\Omega)$.
- On associe alors à toute variable, une loi : la suite des valeurs $\mathbf{P}(X=x)$ où $x\in X(\Omega)$. Et comme X est à valeur numérique, on lui associe aussi une espérance $\mathbf{E}(X)=\sum_{x\in X(\omega)}x\mathbf{P}(X=x)$ qui résume, en une valeur toutes les valeurs prises par X. Ce résumé est évidemment pas bon, on lui associe alors $\mathbf{V}(X)$ qui évolue cette erreur.
- Certaines variables aléatoires sont très fréquentes, on apprend donc à les reconnaitre : la variable peut suivre une loi uniforme, ou bien une loi de Bernoulli (comme la variable indicatrice) ou encore une loi binomiale qui compte le nombre de succès lorsqu'on répète n fois et indépendamment une même expérience élémentaire dont la probabilité de succès est p. D'autres lois sont classiques pour des univers dénombrables ou ayant la puissance du continu.
- Plusieurs variables aléatoires peuvent qualifiées d'indépendantes si les événements générés par ces variables sont indépendants. Pour mesurer cela, il faut donc s'intéresser aux événements $(X_1=x_1)\cap(X_2=x_2)\dots$ que l'on étudie à partir de la variable aléatoire du couple (X_1,X_2) (ou n-uplet) : c'est l'événement $[(X_1,X_2)=(x_1,x_2)]$.
  Si ces variables ne sont pas indépendantes, on peut mesurer la corrélation entre ces variables aléatoires.

⇝ Enfin, deux inégalités sont importantes pour contrôler des événements aléatoires, connaissant la variable aléatoire.
L'inégalité de Markov : si $X \geqslant 0$, $\mathbf{P}(X \geqslant a) \leqslant \frac{\mathbf{E}(X)}{a}$ donne une minoration sur la propriété d'absence d'une variable entière.
L'inégalité de Bienaymé-Tchébychev $\mathbf{P}(|X-a| \geqslant \varepsilon) \leqslant \frac{\mathbf{V}(X)}{\varepsilon^2}$ donne une majoration sur la propriété d'absence d'une variable entière.

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Définir la loi d'une variable aléatoire
- Savoir-faire - Exploitation d'indicatrice (1)
- Savoir-faire - Modélisation
- Truc & Astuce pour le calcul - Etude du $\max(X_i)$ où les X_i sont indépendantes
- Savoir-faire - Exploitation d'indicatrice (2)
- Savoir-faire - Exploitation d'indicatrice (3)
- Savoir-faire - Composition avec exp (pour avoir une va positive). Méthode de Chernoff
- Savoir-faire - Formulation calculatoire (transfert) - Moment
- Savoir-faire - Formulation calculatoire (transfert) - Variance
- Savoir-faire - Tableau récapitulatif

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$[X=a]$, $[X \leqslant a]$	Respectivement les événements $X^{-1}(\{a\})$ et $X^{-1}(]-\infty, a])$	$\{\omega \mid X(\omega)=a\}\ldots$	On raisonne ici par image de fonctions $X : \Omega \to R$ ou par classe d'équivalence. .
$\mathbb{1}_A$	Variable aléatoire indicatrice de l'événement A	$\mathbb{1}_A(x)=1$ ssi $x \in A$	$\mathbf{E}(\mathbb{1}_A)=\mathbf{P}(A)$. On s'en sert pour partitionner Ω .
$X \hookrightarrow \mathscr{U}(\llbracket 1,n \rrbracket)$ (ou $\mathscr{U}_n$)	X (v.a.) suit la loi uniforme sur $\llbracket 1,n \rrbracket$	$X(\Omega)=\llbracket 1,n \rrbracket$, $\mathbf{P}(X=k)=\frac{1}{n}$	$\mathbf{E}(X)=\frac{n+1}{2}$ et $\mathbf{V}(X)=\frac{n^2-1}{12}$.
$X \hookrightarrow \mathscr{B}(p)$	X (v.a.) suit la loi de Bernoulli de paramètre p	$X(\Omega)=\{0,1\}$, $\mathbf{P}(X=1)=p$	$\mathbf{E}(X)=p$ et $\mathbf{V}(X)=p(1-p)$.
$X \hookrightarrow \mathscr{B}(n,p)$	X (v.a.) suit la loi binomiale de paramètres n et p Nombre de succès lors d' une répétition de n expériences aléatoires indépendantes	$X(\Omega)=\llbracket 0,n \rrbracket$, $\mathbf{P}(X=k)=\binom{n}{k}p^k(1-p)^{n-k}$ avec probabilité de succès pour chacune égale à p	$\mathbf{E}(X)=np$ et $\mathbf{V}(X)=np(1-p)$.
$X \perp\!\!\!\perp Y$	Les variables X et Y sont indépendantes	$\forall (x,y) \in X(\Omega)\times Y(\Omega)$, $\mathbf{P}([(X=x)\cap(Y=y)])=\mathbf{P}(X=x)\mathbf{P}(Y=y)$	Notation propre à la MPSI3
$X=Y$ p.s.	Les variables X et Y sont égales presque sûrement	$\mathbf{P}\{\omega \in \Omega \mid X(\omega) \neq Y(\omega)\}=0$	
$\mathbf{E}(X)$	Espérance de X	$\mathbf{E}(X)=\sum_{x\in X(\Omega)} x\mathbf{P}(X=x)=\sum_{\omega\in\Omega} X(\omega)\mathbf{P}(\{\omega\})$	Meilleur résumé en un nombre d'une variable aléatoire(...).
$\mathbf{V}(X)$	Variance de X	$\mathbf{V}(X)=\mathbf{E}((X-\mathbf{E}(X))^2)=\sum_{x\in X(\Omega)}(x-\mathbf{E}(X))^2\mathbf{P}(X=x)$	$\mathbf{V}(X)\geqslant 0$.
$\sigma(X)$	Ecart-type de X	$\sigma(X)=\sqrt{\mathbf{V}(X)}$	Meilleur résumé de la dispersion (autour de sa valeur moyenne) d'une variable aléatoire(...).
$\mathrm{Cov}(X,Y)$	Covariance de X et Y.	$\mathrm{Cov}(X,Y)=\mathbf{E}(XY)-\mathbf{E}(X)\mathbf{E}(Y)$ (on exploite la loi du couple)	$\mathrm{Cov}(X,X)=\mathbf{V}(X)$ et $\mathrm{Cov}(X,Y)\leqslant\sqrt{\mathbf{V}(X)}\sqrt{\mathbf{V}(Y)}$.
$\rho(X,Y)$	Corrélation de X et Y.	$\rho(X,Y)=\sqrt{\mathrm{Cov}(X,Y)}$	Entre -1 (cas $X=-Y$) et 1 (cas $X=Y$), elle mesure le commun entre X et Y.
$X \perp Y$	Les v.a. X et Y sont non corrélées	$\mathrm{Cov}(X,Y)=0$	$X \perp\!\!\!\perp Y \Rightarrow X \perp Y$

Retour sur les problèmes

155. Comment répondre mathématiquement à la question : qu'est-ce qui est le plus naturelle? Quelle que soit la réponse intime que se donne le lecteur, le plus important est qu'il soit capable de comprendre l'autre point de vue (fonction image/classe d'équivalence).
156. Cours. Sur un univers fini : lois uniformes, loi de Bernoulli (0 ou 1), loi binomiale, loi hypergéométrique…

157. L'espérance est le bon résumé d'une variable aléatoire, car le nombre m qui annule $\mathbf{E}(X-m)$ est $\mathbf{E}(X)$. Mais cela donne une définition autoréférente. A éviter absolument!
158. Moins on en connait sur un phénomène, plus on peut exploiter le calcul de probabilités. Il est parfois plu simple.
Une autre confirmation de ce point de vue est la méthode de Monte-Carlo proposé par Van Neumann pour calculer l'intégrale d'une fonction compliquée. Pour calculer $\int_a^b f(t)\mathrm{d}t$, on tire au hasard des nombres x_i entre a et b, et on fait la moyenne des $f(x_i)$…
159. On étudie la loi du couple. Finalement, c'est comme si Ω était partitionner en une partiiton plus fine contenant celle induit par la variable X et celle induite par Y…
160. Voir le cours. On retrouve sauf le fait que le produit scalaire soit défini. Sauf à faire évoluer = en = p.s.

Neuvième partie

Analyse (2)

Chapitre 37

Intégrale(s) (sur un segment)

Résumé -

Le but de ce chapitre est de donner une construction de l'intégrale sur un segment d'une fonction continue par morceaux. Cette construction permet d'obtenir :
- *les propriétés classiques (dont celles admises en TS) de l'intégrale,*
- *de déduire des méthodes de calcul approché*

L'intégration est historiquement liée au calcul d'aire et est antérieure au calcul différentiel. La méthode que l'on va utiliser est une version améliorée de celle utilisée par Riemann vers 1850.

D'autres théories de l'intégration ont ensuite été développées (Lebesgue au XXe siècle) permettant de donner un sens à l'intégrale de fonctions encore plus nombreuses, de fonder la théorie de la mesure et les probabilités. Beaucoup de résultats ici sont hors-programme.

Sommaire

1. Problème 740
2. « Construire » l'intégrale. Préalable 741
2.1. Rappels calculatoires 741
2.2. « Vu de loin » 742
2.3. Quelques rappels de topologie sur $\mathbb{R}$ 744
2.4. Subdivision d'un segment de $\mathbb{R}$ 744
3. Construction de l'intégrale 748
3.1. Classes de fonctions à intégrer 748
3.2. Somme de Cauchy/Riemann associée à f sur D . . . 752
3.3. Intégrales d'une fonction 754
4. Espaces et sous-espaces des fonctions intégrables, ou : Qui est intégrable? 761
4.1. Notations 761
4.2. Passage à la limite des propriétés de somme de Riemann 761
4.3. Fermeture par convergence uniforme 762
4.4. Théorèmes fondamentaux de l'analyse 764
4.5. Bilan en termes d'espaces vectoriels croissants . . . 767
5. L'intégrale comme un « outil puissant » de l'analyse . . . 768
5.1. Relation de Chasles 768
5.2. « Contrôle » par intégration 773
5.3. Extension aux fonctions à valeurs complexes 775
5.4. Formules de Taylor 776
6. Bilan 778

1. Problème

Problème 161 - Construction d'une intégrale

Comment « construire » une intégrale puissante, c'est-à-dire souple.
Elle doit en particulier permettre de montrer que si f est dérivable sur I,

alors, pour tout $a,b\in I$, $\displaystyle\int_a^b f'(t)\mathrm{d}t = f(b)-f(a)$.

La construction que nous ferons, répondra positivement à cette question (à l'inverse de l'intégrale proposée dans le programme). En revanche, pour que son utilisation soit plus souple, il faudra en contre-partie un processus de construction plus compliqué…

Problème 162 - Aire sous la courbe

Dans l'histoire, c'est Archimède qui le premier a fait avancer la notion d'intégrale (attention : la notion de fonctions n'existe réellement que depuis Euler…). Son objectif : donner les formules des aires de différentes surfaces.
Et il n'y a qu'une méthode : *« l'aire est une variable extensive »* diraient les physiciens. On coupe en morceaux une surface compliquée, ces morceaux ayant une aire facile à calculer (triangle ou rectangle) et on additionne simplement les aires de ces morceaux.
Comment exploiter cette stratégie naturelle pour mettre en place notre construction d'intégrale, c'est-à-dire « d'aire sous la courbe ».

Problème 163 - Classe des fonctions intégrables

Une fois la construction de l'intégrale mise au point sur l'ensemble $\mathscr{F}(I,\mathbb{R})$ (ou $\mathscr{F}(I,\mathbb{C})$, voire $\mathscr{F}(I,E)$ où E est un espace vectoriel normé comme en seconde année), quelles sont les fonctions qui admettent une intégrale sur I.
Ou dans sa version ensembliste : comment reconnaitre et qualifier l'ensemble des fonctions KH-intégrables?
Dans le chapitre 6 (sur les primitives), nous avons affirmé (sans démonstration) que toute fonction continue sur un intervalle fermé I admettait une primitive. Est-ce vrai?

Problème 164 - Intégrale sur quel type d'intervalle? Fermé ou ouvert?

Nous avons vu que dans $\mathbb{R}$, les intervalles fermés sont des compacts et possèdent des propriétés plus « fortes » : ainsi le théorème de Heine ou de Weierstrass (c'est-à-dire?). La construction de l'intégrale de Riemann ou de Kurzweil-Henstock se fait donc sur ces intervalles.
Que se passe-t-il lorsqu'on considère des intervalles ouverts? En particulier avec ∞ dans une des bornes?

Problème 165 - Etymologie : pourquoi intégrale?

En latin, intégrale dérive du mot entier. Il ne s'agit pas seulement du nombre entier, mais bien de quelque chose considérée *entièrement*, en totalité.
La dérivation regarde très localement l'évolution d'une variable en rap-

port d'une autre.
L'intégration regarde totalement ou globalement une variable en fonction d'une autre.
Un des problèmes des DL est que l'égalité écrite (et réelle) n'est vrai que localement (voire en limite). L'intégration doit permettre d'obtenir un résultat global, nous nous en servirons souvent (et simplement) par un *encadrement moyen*. Quitte à découper l'intégrale en morceaux puisqu'elle est faite pour !

2. « Construire » l'intégrale. Préalable

2.1. Rappels calculatoires

Quelles sont les fonctions intégrables ?. Deux catégories de réponse à la question :

1. une réponse pratique : elle fait le lien avec les résultats vus au premier semestre et rappelés ici. Et elle donne la valeur de l'intégrale.
2. des réponses théoriques : elle permet d'assurer des résultats d'existence pour les fonctions continues (par morceaux) ou plus large… C'est le but de ce chapitre.

Savoir faire - Méthode 1 : primitives

Si on doit calculer $\int_a^b f$, alors si on peut reconnaitre f comme la dérivée d'une fonction F, on a $\int_a^b f = F(b) - F(a)$ notée $[F]_a^b$.
De là un tableau à apprendre !

Savoir faire - Méthode 2 : Fractions rationnelles

Si on doit calculer $\int_a^b f$, où f est une fraction rationnelle alors on commence par décomposer f en éléments simples sur $\mathbb{R}$.
On trouve une combinaison linéaire de fractions du type :
- Polynôme : intégration simple
- $\frac{a}{(t-r)^k}$ de primitive $t \mapsto \frac{-a}{(k-1)(t-r)^{k-1}}$ ou $t \mapsto a\ln(|t-r|)$ $(k=1)$
- $\frac{2t+b}{(t^2+bt+c)^k}$ (avec $b^2-4c<0$) de primitive $t \mapsto \frac{-1}{(k-1)(t^2+bt+c)^{k-1}}$ ou $t \mapsto \ln(t^2+bt+c)$ si $k=1$
- $\frac{d}{(t^2+bt+c)^k} = \frac{d}{(t+\frac{b}{2})^2+\frac{4c-b^2}{4})^k} = \frac{4^k d}{(4c-b^2)^k} \frac{1}{(1+\frac{4}{4c-b^2}(t+\frac{b}{2})^2)^k}$ (avec $b^2-4c<0$), on fait le changement de variable $\tan\theta = \frac{2}{\sqrt{4c-b^2}}(t+\frac{b}{2})$ qui se simplifie bien…

Savoir faire - Méthode 3 : Intégration par parties

Si on doit calculer $\int_a^b f \times g$, alors si on peut reconnaitre f comme la dérivée d'une fonction F et que g est dérivable, on a

$$\int_a^b fg = F(b)g(b) - F(a)g(a) - \int_a^b Fg'$$

Evidemment, cela n'a d'intérêt que si $\int_a^b Fg'$ est plus simple à calculer

Savoir faire - Méthode 4 : Changement de variable

Si on doit calculer $\int_a^b f(t)\mathrm{d}t$, alors si il existe φ de classe $\mathscr{C}^1$-bijective ($\mathscr{C}^1$-difféomorphisme) de $[\alpha,\beta]$ sur $[a,b]$, on peut faire le changement de variable $t=\varphi(u)$. On a

$$\int_a^b f = \int_\alpha^\beta f(\varphi(u))\varphi'(u)\mathrm{d}u$$

Application - Règles de Bioche

En présence d'une intégrale $\int_a^b R(\cos\theta,\sin\theta)\mathrm{d}\theta$ où R est une fraction rationnelle. Alors, si $R(\sin\theta,\cos\theta)\mathrm{d}\theta$ est invariant par le changement de variable :
- $\theta \mapsto -\theta$, on fait le changement de variable $t=\cos\theta$
- $\theta \mapsto \pi-\theta$, on fait le changement de variable $t=\sin\theta$
- $\theta \mapsto \pi+\theta$, on fait le changement de variable $t=\tan\theta$

Sinon, on pose $t=\tan\frac{\theta}{2}$.

Exemple - Primitive de $\frac{\sin^3(x)}{1+\cos^2(x)}$

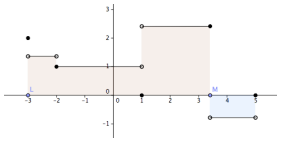
$\frac{\sin^3(-x)}{1+\cos^2(-x)}\mathrm{d}(-x) = \frac{\sin^3(x)}{1+\cos^2(x)}\mathrm{d}x$. On pose donc $t=\cos x$.

$$\int \frac{\sin^3(x)}{1+\cos^2(x)}\mathrm{d}x = \int -\frac{1-t^2}{1+t^2}\mathrm{d}t = \int (-1+\frac{2}{1+t^2})\mathrm{d}t = t - 2\arctan t + K$$

Pour aller plus loin - L'année prochaine : d'autres méthodes
On peut aussi exploiter des séries entières, et plus largement des suites ou séries de fonctions et exploiter les « gros » théorèmes d'interversion de limites. Grand moment du cours de seconde année !

Histoire - Les première années de l'intégration
Bien que l'intégrale a été définie indépendamment par Newton et Leibniz à la fin du XVIIIième siècle, la première version la plus rigoureuse de l'intégrale à été construite par Bernard Riemann (après celle de Cauchy).
Malheureusement, comme on va le voir, cette définition n'était pas suffisamment robuste. Plusieurs versions ont dues être reprise pour élargir la définition…

Représentation - Aire d'une fonction en escalier



2.2. « Vu de loin »

Aire sous la courbe

Analyse - Aire sous la courbe. Rappels de terminale

En terminale, l'intégrale $\int_a^b f(t)\mathrm{d}t$ est définie comme l'aire sous la courbe $y=f(x)$ (avec f continue) et délimitée par $x=a$, $x=b$ et $y=0$.
On admet alors que toute fonction f admet bien une intégrale. Et dans ce cas, on peut définir une application $F : x \mapsto \int_0^x f(t)\mathrm{d}t$, elle vérifie F est de classe $\mathscr{C}^1$ sur I et $F'=f$.
Nous allons essayer de démontrer ce second résultat. Mais il faut d'abord prouver l'existence de cette fonction. On devra commencer par construire l'application intégration de f.
Si tout se passe pour le mieux, tout ce qui a été vu en début d'année lors de l'étude des primitives prendra sens.

Heuristique - Les fonctions en escalier ou les fonctions étagées

Les fonctions en escalier sont celles pour lesquelles le calcul de l'aire « sous » la courbe est la plus simple.
Il s'agit des fonctions constantes sur des intervalles.
Nous serons donc obliger de commencer par définir (ou reprendre) la notion de subdivision d'un segment (ou intervalle). Nous avons définit cela lorsqu'on a vu le lemme de Cousin…

Différentes approches historiques

Les commentaires qui suivent sont pour le moins rapides…

Heuristique - L'approche de Riemann

La construction se passe dans l'ordre suivant :
0. On sait les intégrales de fonctions en escalier.
1. On considère une fonction f continue sur un segment $[a,b]$ pour laquelle on doit calculer $\int_a^b f$.
2. On se donne un qualité d'approximation $\epsilon>0$.
3. La fonction f étant continue sur $[a,b]$, elle est uniformément continue (théorème

de Heine).

$$\exists\,\eta>0,\qquad \forall\,x,x'\in[a,b],|x-x'|<\eta\Longrightarrow|f(x)-f(x')|<\frac{\epsilon}{b-a}$$

4. On découpe $[a,b]$ en n morceaux (subdivision) de taille inférieure à η : $(a=x_0<x_1<x_2\cdots<x_{n-1}=b$
5. On choisit alors (librement) t_i un élément de chaque intervalle $]x_{i-1},x_i[$ et une fonction en escalier définie par :

$$\varphi_{||x_{i-1},x_i[}=f(t_i)$$

6. Enfin, l'intégrale $\int_a^b\varphi=\sum_{i=1}^{n}(x_i-x_{i-1})f(t_i)$, bien définie, approche celle de f à ϵ-près

Attention - Quelque problème

Cette intégrale est bien définie pour les fonctions uniformément continue sur un segment, mais pas très bien lorsque la fonction est plus « *pathologique* ».
Par exemple, la fonction de Dirichlet (indicatrice des rationnels) :

$$\chi_{[0,1]}:t\mapsto\begin{cases}1 & \text{et} \quad t\in\mathbb{Q}\\ 0 & \text{et} \quad t\notin\mathbb{Q}\end{cases}$$

n'est pas Riemann-intégrable sur $[0,1]$. Par ailleurs, comme nous le verrons plus loin, si une fonction est Riemann-intégrable sur $[a,b]$, elle est nécessairement bornée. Et par contraposée…

Heuristique - L'approche de Lebesgue

La stratégie de Lebesgue est très différente. Pour construire cette intégrale, on raisonne non plus sur l'intervalle de départ mais sur l'intervalle image (qui peut contenir l'infini!).

0. On connait les intégrales de fonctions étagées (comme les fonctions en escalier).
1. On découpe alors l'intervalle (image) J en n morceaux : $J=\bigcup_{i=1}^{n}J_n$ et on considère alors les intervalles $I_k=f^{-1}(J_k)$.
2. Toute la difficulté repose alors dans la nature de ces ensembles $I_k=f^{-1}(J_k)$ qui peuvent être « *très pathologiques* ».
3. On calcul alors $\int f=\sum_k|I_k|f(t_k)$

Histoire - Henri Lebesgue



Henri Lebesgue (1875-1941) est l'un des plus grands mathématiciens français du début du XX^e siècle. Il se présentait comme issu de milieu modeste (parents ouvriers) et est surtout connu pour l'intégrale qu'il crée dans sa thèse : Intégrale, longueur, aire

Attention - Quelques problème…

Pour les intégrales de Lebesgue la notion d'intégrale impropre n'existe pas (voir dernière partie de ce chapitre).
Une fonction est intégrable au sens de Lebesgue, si et seulement si sa valeur propre est intégrable (un peu comme les suites sommables).
Donc des fonctions comme

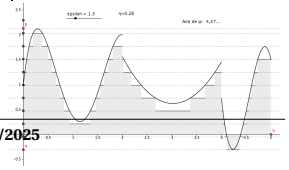
$$\int_0^{+\infty}\frac{\sin t}{t}\mathrm{d}t$$

qui sont intégrables (au sens de Riemann) mais pas intégrable en valeur absolue ne sont pas intégrable au sens de Lebesgue…

Heuristique - L'approche de Kurzweil-Henstock

Le cours qui suit présente l'intégrale definie indépendamment par Kurzweil et Henstock. Le principe repose sur une généralisation de l'intégration de Riemann. Elle permet d'obtenir de nombreux résultats de la théorie de Lebesgue. Mais elle reste assez peu connue… Une raison : elle nécessite au démarrage le lemme de Cousin. Mais nous le connaissons bien…

Représentation - Aire d'une fonction étagée



Histoire - Mathématiciens moins connus…

Jaroslav Kurzweil (né en 1926) est un mathématicien tchèque mort l'an dernier, le 17 mars 2022. Il dirigeait l'équipe de recherche en Mathématiques de l'Académie Tchèque des Sciences.
Ralph Henstock (né le 2 juin 1923 et mort le 17 janvier 2007) était un mathématicien anglais. Il a développé l'intégrale KH en 1957, indépendamment de Kurzweil (et la même année).

2.3. Quelques rappels de topologie sur $\mathbb{R}$

Il n'y a rien de nouveau dans cette partie, mais cela vaut le coup de revoir certains points.
Nous nous souvenons que nous avons défini $\mathbb{R}$ comme l'ensemble des points x, obtenu par coupure :
$x=(A,B)$, où $A\uplus B=\mathbb{Q}$, $\forall\,(a,b)\in A\times B$, $a<_{\mathbb{Q}}b$. On a alors $a\leqslant_{\mathbb{R}}x<_{\mathbb{R}}b$.

Analyse - Schéma des principaux résultats topologiques

$\mathbb{R}$ vérifie le théorème de la borne supérieure $\forall A\subset\mathbb{R}$, borné, $\exists\,x\in\mathbb{R}$ tel que $x=\sup A$ $\Longleftrightarrow$ Toute suite croissante majorée converge $\Longleftrightarrow$ Les suites adjacentes convergent	Propriétés essentielles (de construction de $\mathbb{R}$)
Théorème des segments emboités Si (I_n) tel que $I_{n+1}\subset I_n$ et $\ell(I_n)\to 0$ alors $\exists\,a\in\mathbb{R}$ tel que $\{a\}=\bigcap_{n\in\mathbb{N}}I_n$ Et principe de dichotomie Si f est fonction d'intervalles sous additive sur $[a,b]$ et que $f(a,b)=1$, $\Rightarrow\exists\,(a_n)(b_n)\in\mathbb{R}^{\mathbb{N}}$, adjacentes telle que pour tout $n\in\mathbb{N}$ $f(a_n,b_n)=1$ $\Longleftrightarrow$ Théorème de Bolzano Weierstrass Toute suite bornée admet une suite extraite convergente $\Longleftrightarrow$ Lemme de Cousin Soit $[a,b]\subset\mathbb{R}$ et δ, jauge (>0) alors $[a,b]$ admet une subdivision δ fine.	Bloc de la COMPACITE
Toute suite de Cauchy converge (et réciproquement) Suite de Cauchy : $\forall\,\epsilon>0,\exists\,N$ tel que $\forall\,p>q\geqslant N,\|u_p-u_q\|\leqslant\epsilon$ Toute série absolument convergente est convergente	Bloc de la COMPLETUDE

Dans $\mathbb{R}$ ces blocs sont équivalents (ce n'est pas toujours le cas).

Analyse - Et pour les fonctions continues…

Avec des fonctions continues :
- Le bloc de la construction de $\mathbb{R}$ ⇒ le théorème des valeurs intermédiaires
- Le bloc de la compacité ⇒ le théorème de Weierstrass
- Le bloc de la compacité ⇒ le théorème de Heine

Exercice
Rappelez l'énoncé de ces trois théorèmes. Quelle différence entre les deux premiers ?

Correction
Dans tous les cas f est continue
TVI : $\forall\,a,b\in\mathscr{D}_f$, $f([a,b])$ est un intervalle
TW : $\forall\,a,b\in$ intérieur$(\mathscr{D}_f)$, $f([a,b])$ est un segment
TH : f est continue sur $[a,b]$ si et seulement si f est uniformément continue sur $[a,b]$
La question de la forme de l'intervalle (compact) est très importante et change beaucoup de chose (que cela soit au départ ou à l'arrivée)…

2.4. Subdivision d'un segment de $\mathbb{R}$

Relation d'ordre sur les subdivisions

On commence par un rappel. Les résultats qui suivent immédiatement n'ont pas vraiment été vus.

Définition - Subdivision
Soit $[a,b]$ un segment de $\mathbb{R}$.
On appelle **subdivision** de $[a,b]$ toute famille finie $\sigma=(x_i)_{0\leqslant i\leqslant n}$ de points

de $[a,b]$ telle que

$$a = x_0 < x_1 < \cdots < x_n = b.$$

On appelle **pas** de la subdivision $\sigma = (x_i)_{0\leqslant i\leqslant m}$ de $[a,b]$ le réel $\delta(\sigma) = \max_{1\leqslant i\leqslant n}(x_i - x_{i-1})$.

Exemple - Cas particuliers : subdivision à pas constant

• en posant $x_i = a + i\dfrac{b-a}{n}$ pour $n \in \mathbb{N}^*$, on définit une subdivision de $[a,b]$ telle que

$$\forall i \in [\![1,n]\!], \quad x_i - x_{i-1} = \frac{b-a}{n}.$$

On dit que c'est une subdivision de $[a,b]$ de **pas constant** $\dfrac{b-a}{n}$ (que l'on peut prendre aussi petit que l'on veut en augmentant n, nombre de points de la subdivision).
Cela rappelle la commande `linspace` du module `numpy` de Python.

Définition - Relation d'ordre sur la subdivision
La subdivision $\sigma = (x_i)_{0\leqslant i\leqslant n}$ de $[a,b]$ est dite **plus fine** que la subdivision $\sigma' = (x'_i)_{0\leqslant i\leqslant m}$ de $[a,b]$ si

$$\{x'_0,\dots,x'_m\} \subset \{x_0,\dots,x_n\}.$$

Comme la relation « contenant » noté $\supset$, il s'agit d'une relation d'ordre.

Remarque - Plus fine : relation d'ordre, non totale
On peut montrer que la relation *« est plus fine »* est une relation d'ordre sur l'ensemble des subdivisions de $[a,b]$.
Elle est réflexive, antisymétrique et transitive.
Mais elle n'est pas totale (comme la relation sur $\mathbb{Z}$: *« est divisible par »*).
Mais on peut opérer sur les subdivision (comme pour les ensembles).

Définition - Affinement des subdivisions
Soient σ et σ' deux subdivisions de $[a,b]$,
la subdivision obtenue en réunissant les points de σ et de σ' est plus fine que σ et que σ'.
C'est la moins fine des subdivisions plus fines que σ et σ', on la note $\sigma \vee \sigma'$.
On a $\sigma \vee \sigma' = \sup_{\supset}(\sigma,\sigma')$

Remarque - $\sigma \wedge \sigma'$
On peut également définir la plus fine des subdivisions moins fines que σ et σ'

Des subdivisions pointés

Définition - Subdivision pointée
Soit $I = [a,b]$, un segment de $\mathbb{R}$.
On appelle subdivision pointée de I la donnée
— d'une subdivision $\sigma = (x_0,x_1,\dots x_n)$ de $[a,b]$,
— un pointage de cette subdivision $t_1,t_2,\dots t_n \in I$ tels que
$\forall\, i \in \mathbb{N}_n,\ t_i \in [x_{i-1},x_i]$.
On note $\sigma_p = \big(([x_0,x_1],t_1),([x_1,x_2],t_2),\dots([x_{n-1},x_n],t_n)\big)$, les nombres (t_i) sont appelés les points de marquage de σ_p.

Définition - Subdivision pointée adaptée à un jauge
Un pas ou une jauge est une application $\delta : [a,b] \to \mathbb{R}_+^*$.
Une subdvision pointée $\sigma_p = \big(([x_0,x_1],t_1),([x_1,x_2],t_2),\dots([x_{n-1},x_n],t_n)\big)$ est

dite adaptée au pas δ ou δ-fine, si

$$\forall\, k \in \mathbb{N}_n, \qquad [x_{k-1},x_k] \subset \left[t_k - \frac{\delta(t_k)}{2}, t_k + \frac{\delta(t_k)}{2}\right]$$

On remarquera que $0 \leqslant x_k - x_{k-1} \leqslant \delta(t_k)$.
Pour une jauge δ donnée, on note $\delta - \mathfrak{S}([a,b])$ (simplifiée en $\delta - \mathfrak{S}$ si cela ne conduit à aucune ambiguïté), l'ensemble des subdivisions pointés de $[a,b]$ δ-fine. Si δ est constante, on notera la notera δ^*. Dans ce cas $\delta(\sigma_p) \leqslant \delta^*$.

Proposition - Amélioration de la finesse de la subdivision
Soient δ_1 et δ_2 deux jauges.
Soit $\delta = \min(\delta_1,\delta_2)$, i.e. $\forall\ t \in [a,b],\ \delta(t) = \min(\delta_1(t),\delta_2(t)) > 0$.
Alors si σ_p est une subdivision pointée de $[a,b]$, δ-fine,
nécessairement, σ_p est également δ_1-fine et δ_2-fine.
Autrement écrit : $\delta - \mathfrak{S} \subset \delta_1 - \mathfrak{S} \cap \delta_2 - \mathfrak{S}$.

Démonstration
La subdivision $(x_0,x_1,\dots x_n)$ reste la même.
Puis comme $\delta_1(t_k) \geqslant \delta(t_k)$, on a bien

$$[x_{k-1},x_k] \subset \left[t_k - \frac{\delta(t_k)}{2}, t_k + \frac{\delta(t_k)}{2}\right] \subset \left[t_k - \frac{\delta_1(t_k)}{2}, t_k + \frac{\delta_1(t_k)}{2}\right]$$

De même pour δ_2. □

Exercice
On note $\mathfrak{S}_\delta = \{\sigma_p$, subdivison pointée δ-fine de $[a,b]\}$.
Montrer que si $\delta_1 \leqslant \delta_2$, alors $\mathfrak{S}_{\delta_1} \subset \mathfrak{S}_{\delta_2}$.

Correction

Réunion de subdivisions

Les résultats suivants nous serons utiles autour du théorème de Chasles et le lemme de Henstock.

Proposition - Extraction
Soit δ une jauge définie sur $[a,b]$.
Si $\sigma_p = \big(([x_0,x_1],t_1),([x_1,x_2],t_2),\dots([x_{n-1},x_n],t_n)\big)$ est une subdivision pointée δ-fine de $[a,b]$,
alors pour tout $0 \leqslant i < j \leqslant n$, $\big(([x_k,x_{k+1}],t_{k+1}), i \leqslant k < j\big)$ est une subdivision pointée de $[x_i,x_j]$, $\delta_{|[x_i,x_j]}$ fine.

Par la suite, nous définirons la notion de sous-subdivision en réunion d'extraction.

Démonstration
Le résultats est évident, puisque pour tout $k \in [\![i,j-1]\!]$,

$$t_{k+1} - \frac{\delta_{|[x_i,x_j]}(t_{k+1})}{2} = t_{k+1} - \frac{\delta(t_{k+1})}{2} \leqslant x_k \leqslant t_{k+1} \leqslant x_{k+1} \leqslant t_{k+1} + \frac{\delta(t_{k+1})}{2} \leqslant t_{k+1} - \frac{\delta_{|[x_i,x_j]}(t_{k+1})}{2}$$

□

Réciproquement,

Proposition - Réunion
Soient $a < b < c \in \mathbb{R}$ et δ_1 une jauge sur $[a,b]$, δ_2 une jauge sur $[b,c]$.
Soit $(\sigma_p)_1$ une subdivision pointée δ_1 fine sur $[a,b]$.
Soit $(\sigma_p)_2$ une subdivision pointée δ_2 fine sur $[b,c]$.

On note $\delta : [a,c] \to \mathbb{R}_+^*,\ t \mapsto \begin{cases} \delta_1(t) & \text{si } t \in [a,b[\\ \max(\delta_1(b),\delta_2(b)) & \text{si } t = b \\ \delta_2(t) & \text{si } t \in]b,c] \end{cases}$.
Alors la réunion (concaténation) $(\sigma_p)_1 \cup (\sigma_p)_2$ est une subdivision pointée δ-fine de $[a,c]$

Démonstration
Soit $t_k \in [a,c]$, point de marquage de $\sigma_p = (\sigma_p)_1 \cup (\sigma_p)_2$.
Si $t_k < b$, c'est un point de marquage de $(\sigma_p)_1$ et l'on trouve bien

$$t_k - \frac{\delta(t_k)}{2} = t_k - \frac{\delta_1(t_k)}{2} \leqslant x_{k-1} \leqslant t_k \leqslant x_k \leqslant t_k + \frac{\delta_1(t_k)}{2} \leqslant t_k - \frac{\delta(t_k)}{2}$$

Si $t_k > b$, c'est un point de marquage de $(\sigma_p)_2$ et l'on trouve bien

$$t_k - \frac{\delta(t_k)}{2} = t_k - \frac{\delta_2(t_k)}{2} \leqslant x_{k-1} \leqslant t_k \leqslant x_k \leqslant t_k + \frac{\delta_2(t_k)}{2} \leqslant t_k - \frac{\delta(t_k)}{2}$$

Enfin, si $t = b$. Alors, il peut être associée à $[x_k, b]$ sur $[a,b]$ ou à $[b, x_j]$ sur $[b,c]$.
Dans les deux cas, on trouve

$$t_k - \frac{\delta(t_k)}{2} \leqslant x_{k-1} \leqslant t_k \leqslant x_k \leqslant t_k + \frac{\delta(t_k)}{2}$$

car $\delta(t_k) = \delta(b) = \max(\delta_1(b),\delta_2(b))$ □

Forçage

Par la suite, on aura besoin d'exploiter des jauges particulières

Proposition - Forçage
Soit $c \in [a,b] \subset \mathbb{R}$ et $\alpha > 0$.
Considérons la jauge $\delta : [a,b] \to \mathbb{R}_+^*,\ t \mapsto \begin{cases} |t-c| & \text{si} \quad t \neq c \\ \alpha & \text{si} \quad t = c \end{cases} = |t - c|\mathbb{1}_{[a,b]\setminus\{c\}} + \alpha\mathbb{1}_{\{c\}}(t)$.
Si σ_p une subdivision pointé δ-fine de $[a,b]$, alors c est nécessairement un point de marquage de σ_p.

Démonstration
• δ est bien une jauge (toujours strictement positive).
• Soit σ_p une subdivision pointée δ-fine.
Alors $\forall\ k \in \mathbb{N}_n, \quad [x_{k-1}, x_k] \subset \left[t_k - \frac{\delta(t_k)}{2}, t_k + \frac{\delta(t_k)}{2}\right]$.
Nécessairement, il existe k_c tel que $c \in [x_{k_c-1}, x_{k_c}]$.
On a alors

$$c \in [x_{k_c-1}, x_{k_c}] \subset \left[t_{k_c} - \frac{\delta(t_{k_c})}{2}, t_{k_c} + \frac{\delta(t_{k_c})}{2}\right]$$

Donc $|c - t_{k_c}| \leqslant \frac{\delta(t_{k_c})}{2} = \frac{|t_{k_c} - c|}{2}$, donc $\frac{|t_{k_c} - c|}{2} \leqslant 0$.
Ceci n'est possible que si $t_{k_c} = c$. Donc c est un point de marquage de σ_p. □

Lemme de Cousin

Le lemme de Cousin énonce alors :

Théorème - Lemme de Cousin
Pour tout δ, jauge sur $[a,b]$, il existe une subdivision pointée $\sigma_p = \big(([x_0,x_1],t_1),([x_1,x_2],t_2),\dots([x_{n-1},x_n],t_n)\big)$, adaptée à δ (δ-fine).
Autrement écrit, pour tout δ jauge de $[a,b]$, $\delta - \mathfrak{S}([a,b]) \neq \emptyset$

La démonstration du lemme de Cousin été vu en début d'année. On peut par exemple, exploiter le principe de dichotomie ou ce qui revient au même : une suite de segments emboîtés.
Petit rappel :

Démonstration
Soit δ jauge sur $[a,b]$.
On note, pour tout $\alpha,\beta \in [a,b]$, $f(\alpha,\beta) = 0$ ssi il existe une subdivision sur $[\alpha,\beta]$, $\delta_{|[\alpha,\beta]}$-fine.
Soient $\alpha < \beta < \gamma \in [a,b]$ tels que $f(\alpha,\beta) = f(\beta,\gamma) = 0$.
En concaténant les deux subdivisons $\delta_{|[\alpha,\beta]}$ et $\delta_{|[\alpha,\beta]}$-fines respectivement,
On obtient une subdivision $\delta_{|[\alpha,\gamma]}$-fine. Donc $f(\alpha,\gamma) = 0$.
Donc f est sous-additive.
Supposons que $f(a,b) = 1$.
Alors il existe (a_n) et (b_n) adjacentes tels que pour tout $n \in \mathbb{N}$, $f(a_n,b_n) = 1$.
On note $\ell = \lim(a_n) = \lim(b_n)$ et $T = \delta(\ell) > 0$.
Il existe $N \in \mathbb{N}$ tel que $[a_N,b_N] \subset [\ell - \frac{T}{2}, \ell + \frac{T}{2}]$, donc $([a_N,b_N],\ell)$ est $\delta_{|[a_N,b_N]}$-fine et donc $f(a_N,b_N) = 0$. Contradiction.
Ainsi, $f(a,b) = 0$ □

3. Construction de l'intégrale

3.1. Classes de fonctions à intégrer

Heuristique - Principe
L'intégrale est facile à mettre en place pour une famille de fonctions simples : les fonctions en escalier (cf partie suivante).
Donc ici :

1. On se concentre sur l'ensemble des fonctions en escalier, c'est une algèbre.
2. On voit comment on peut *par densité* généraliser les propriétés obtenues en passant sur un ensemble *adhérant* : l'ensemble des fonctions continues par morceaux.
3. On définit donc, en amont, cet ensemble.

Fonctions en escalier

Représentation - Fonctions en escalier
Dans la première partie de ce chapitre, nous avons représenté des fonctions en escalier. Vous pouvez vous y reporter

Définition - Fonction en escalier
$\phi : [a,b] \to \mathbb{R}$ est dite **en escalier** s'il existe une subdivision $\sigma = (x_i)_{0\leqslant i\leqslant n}$ de $[a,b]$ telle que pour tout $i \in [\![1,n]\!]$, $\quad \phi_{|]x_{i-1},x_i[}$ est constante (notée λ_i).
Une telle subdivision est dite **subordonnée** (ou **adaptée**) à ϕ.
On a $\phi = \sum_{i=1}^{n} \lambda_i \mathbf{1}_{]x_{i-1},x_i[} + \sum_{i=0}^{n} \phi(x_i)\mathbf{1}_{\{x_i\}}$.

Proposition - Sur les subdivisions
• Toute subdivision plus fine qu'une subdivision subordonnée à ϕ est encore subordonnée à ϕ.
• Une fonction constante sur $[a,b]$ est une fonction en escalier.
• Une fonction en escalier est bornée.

Démonstration
Soit φ en escalier et $\sigma = (x_i)_{0\leqslant i\leqslant n}$ une subdivision adaptée.
Soit $\sigma' = (y_j)_{0\leqslant j\leqslant p}$, plus fine que σ.
Pour tout $i \in [\![0,n]\!]$, $x_i \in \sigma'$, donc pour tout $j \in \mathbb{N}_{p-1}$,
on ne peut avoir : $\exists\ i \in \mathbb{N}_n$ tel que $y_{j-1} < x_i < y_j$, donc $\varphi_{|]y_{j-1},y_j[}$ est bien constante. Et donc σ' est adaptée à φ.
Si $\varphi = K$, alors $\sigma = (a,b)$ est une subdivision qui convient : φ est en escalier.
Si φ est en escalier et que $\sigma = (x_i)_{0\leqslant i\leqslant n}$ une subdivision adaptée,
alors φ ne prend qu'un nombre fini de valeurs,
les éléments de $\{f(x_i), i \in [\![0,n]\!]\} \cup \{f_{|[x_{i-1},x_i]}, i \in \mathbb{N}_n\}$.
donc φ est nécessairement bornée. □

Exemple - Fonction en escalier. Définition algébrique

La fonction $\begin{cases} [a,b] & \to \mathbb{R} \\ x & \mapsto \lfloor x \rfloor \end{cases}$ est en escalier.

On note $n = \lfloor a \rfloor$. Une subdivision subordonnée est alors

$$\sigma = (a, n+1, n+2, n+3, \dots \lfloor b \rfloor, b)$$

Exercice

Que vaut $\mathbf{1}_{[a,b]} + \mathbf{1}_{[c,d]}$ et $\mathbf{1}_{[a,b]} \times \mathbf{1}_{[c,d]}$?

Correction

$\mathbf{1}_{[a,b]} + \mathbf{1}_{[c,d]} = 2\mathbf{1}_{[a,b]\cap[c,d]} + \mathbf{1}_{[a,b]\setminus[c,d]} + \mathbf{1}_{[c,d]\setminus[a,b]}$.
$\mathbf{1}_{[a,b]} \times \mathbf{1}_{[c,d]} = \mathbf{1}_{[a,b]\cap[c,d]}$

Théorème - Algèbre

On note $\mathscr{E}([a,b],\mathbb{R})$ l'ensemble des fonctions en escalier à valeurs réelles (ou plus simplement $\mathscr{E}([a,b])$ s'il n'y a pas d'ambigüité sur l'ensemble d'arrivée).
$\mathscr{E}([a,b],\mathbb{R})$ est un sous-espace vectoriel de $\mathscr{F}([a,b],\mathbb{R})$.
Et $(\mathscr{E}([a,b],\mathbb{R}),+,\times)$ est un sous-anneau de $(\mathscr{F}([a,b],\mathbb{R}),+,\times)$.
Donc $\left(\mathscr{E}([a,b],\mathbb{R}),+,\times,\cdot\right)$ est une algèbre.

Démonstration

- $\mathscr{E}([a,b],\mathbb{R}) \subset \mathscr{F}([a,b],\mathbb{R})$,
- la fonction nulle sur $[a,b]$ est en escalier sur $[a,b]$,
- pour ϕ,ψ en escalier sur $[a,b]$, et λ,μ réels,
  en prenant $\sigma = (x_i)_{0\leqslant i\leqslant n} = \sigma_\phi \vee \sigma_\psi$, on obtient une subdivision plus fine que σ_ϕ et σ_ψ, et donc $\lambda\phi + \mu\psi$ est constante sur chacun des $]a_{i-1}, a_i[$, pour $i \in [\![1,n]\!]$.
  D'où $\lambda\phi + \mu\psi \in \mathscr{E}([a,b],\mathbb{R})$ et $\mathscr{E}([a,b],\mathbb{R})$ est un s.e.v de $\mathscr{F}([a,b],\mathbb{R})$.
- $(\mathscr{E}([a,b],\mathbb{R}),+,\times,\cdot)$ est une sous-algèbre de $\mathscr{F}([a,b],\mathbb{R})$ car la fonction constante sur $[a,b]$ égale à 1 appartient à $\mathscr{E}([a,b],\mathbb{R})$, et le produit de deux fonctions en escalier est en escalier (subdivision $\sigma_f \vee \sigma_g$ que pour la combinaison linéaire).

□

Pour aller plus loin - Comparaison à l'addition de fractions

C'est comme lorsqu'on met deux fractions aux même dénominateur avant de faire l'addition

Fonctions continues par morceaux

Définition - Continuité par morceaux sur un segment

Soit $f : [a,b] \to \mathbb{R}$. On dit que f est **continue par morceaux** sur le segment $[a,b]$ s'il existe une subdivision $\sigma = (x_i)_{0\leqslant i\leqslant n}$ de $[a,b]$ telle que
- f est continue sur chacun des intervalles $]x_{i-1}, x_i[$
- pour $i \in [\![1,n]\!]$, f admet une limite finie à droite en x_{i-1} et une limite finie à gauche en x_i.

La subdivision est dite subordonnée ou adaptée à f.

Exemple - Quelques exemples

- une fonction en escalier est continue par morceaux ;
- une fonction continue est continue par morceaux ;
- $f : \begin{matrix} x & \mapsto e^{1/x} \text{ si } x \in [-1,1], x \neq 0 \\ 0 & \mapsto 0 \end{matrix}$ n'est pas continue par morceau, car elle n'admet pas de limite finie à droite en 0.

Proposition - Bornée

Une fonction continue par morceaux sur $[a,b]$ est bornée sur $[a,b]$.

Démonstration

On considère $\sigma = (x_0, x_1, \dots x_n)$ une subdivision adaptée à f.
Soit $i \in [\![1,n]\!]$.
Comme $f_{|]x_{i-1},x_i[}$ se prolonge par continuité à droite en x_{i-1} et à gauche en x_i.
On peut considérer $\tilde{f}_i$, la fonction prolongée. Elle est continue sur le segment $[x_{i-1}, x_i]$, donc d'après le théorème de Weierstrass, elle est bornée (et atteint ses bornes).
il existe M_i tel que $\forall\ t \in [x_{i-1}, x_i],\ |\tilde{f}_i(t)| \leqslant M_i$.
$\forall\ t \in]x_{i-1}, x_i[,\ |f(t)| \leqslant M_i$.
Notons enfin $M = \max(M_1, \dots M_n, |f(x_0)|, \dots |f(x_n)|)$.
Alors pour tout $t \in [a,b]$, $|f(t)| \leqslant M$. □

Proposition - Algèbre

L'ensemble des fonctions continues par morceaux sur $[a,b]$ à valeurs réelles, que l'on pourra noter $\mathscr{C}_{\mathscr{M}}([a,b],\mathbb{R})$, est un s.e.v, et même une sous-algèbre de $\mathscr{B}([a,b],\mathbb{R})$, algèbre des fonctions bornées, lui-même sous algèbre de $\mathscr{F}([a,b],\mathbb{R})$.

Démonstration

Montrons que c'est un sous-espace.
- $\mathscr{C}_{\mathscr{M}}([a,b],\mathbb{R}) \subset \mathscr{F}([a,b],\mathbb{R})$,
- la fonction nulle sur $[a,b]$ est en escalier sur $[a,b]$, ainsi que la fonction constante égale à 1,
- pour f, g continues par morceaux sur $[a,b]$, λ,μ réels, en prenant $\sigma = (x_i)_{0\leqslant i\leqslant n}$ subdivision obtenue par réunion des points de deux subdivisions σ_f et σ_g subordonnées respectivement à f et g, on obtient, par les opérations sur les fonctions continues et sur les limites, que $\lambda f + \mu g, fg \in \mathscr{C}_{\mathscr{M}}([a,b],\mathbb{R})$ donc $\mathscr{C}_{\mathscr{M}}([a,b],\mathbb{R})$ est une sous-algèbre de $\mathscr{F}([a,b],\mathbb{R})$.

□

Approximation (uniforme) des fonctions continues par morceaux par des fonctions en escalier

Théorème - Approximation uniforme par des fonctions en escalier

Soit f continue par morceaux sur $[a,b]$. Soit $\epsilon > 0$.
Alors il existe une fonction ϕ en escalier sur $[a,b]$ telle que

$$\sup_{x\in[a,b]} |f(x) - \phi(x)| \leqslant \epsilon$$

On commence par démontrer (de deux façons) le cas particulier suivant :

Proposition - Approximation uniforme de fonctions continues par des fonctions en escalier

Soit f continue sur $[a,b]$. Soit $\epsilon > 0$.
Alors il existe une fonction ϕ en escalier sur $[a,b]$ telle que

$$\sup_{x\in[a,b]} |f(x) - \phi(x)| \leqslant \epsilon$$

Puis on généralisera

Démonstration

On suppose donc ici que f est continue sur $[a,b]$. *Méthode classique : en exploitant l'uniforme continuité finie (et donc une jauge δ^* constante).*
Soit $\epsilon > 0$.
f est continue, donc (Heine) elle est uniformément continue sur $[a,b]$.
Ainsi, il existe δ^* tel que

$$\forall\ x, y \in [a,b] \qquad |x-y| \leqslant \delta^* \Longrightarrow |f(x) - f(y)| \leqslant \epsilon$$

On note $N = \lfloor \frac{b-a}{\delta^*} \rfloor$, donc $N\delta^* \leqslant b-a < (N+1)\delta^*$, i.e $a + N\delta^* \leqslant b < a + (N+1)\delta^*$.
Soit pour tout $k \in \mathbb{N}_N$, $x_k = a + k\delta^*$ et $x_0 = a$ et $x_{N+1} = b$,

donc $x_{k+1}-x_k \leqslant \delta^*$.
Notons $\sigma=(x_k)_{0\leqslant k\leqslant N+1}$ et φ tel que $\forall\ i\in[\![0,N]\!]$, $\phi_{|]x_i,x_{i+1}[}=f(x_i)$ et $\varphi(b)=f(b)$.
Alors φ est en escalier.
Et pour tout $y\in[a,b[$, supposons que $y\in[x_i,x_{i+1}]$:

$$|f(y)-\varphi(y)|=|f(y)-f(x_i)|\leqslant\epsilon$$

car $|y-x_i|\leqslant\delta^*$. Donc $\sup|f-\varphi|\leqslant\epsilon$.
Plus efficace : en exploitant le lemme de Cousin (et sans l'uniforme continuité - Heine).
Soit $\epsilon>0$.
f est continue, donc il existe $\delta:[a,b]\to\mathbb{R}^+$, jauge telle que (continuité en tout x) :

$$\forall\ y\in[a,b],\ |x-y|\leqslant\delta(x)\Rightarrow|f(x)-f(y)|\leqslant\epsilon$$

D'après le lemme de Cousin, il existe σ_p, une subdivision pointée δ-fine de $[a,b]$.
Supposons que $\sigma_p=\big(([x_0,x_1],t_1),\dots([x_{m-1},x_m],t_m)\big)$.
Soit φ, fonction en escalier définie par $\phi_{|]x_{k-1},x_k[}=f(t_k)$ et $\varphi(b)=f(b)$.
Alors pour tout $y\in[a,b[$, supposons que $y\in[x_i,x_{i+1}]$:

$$|f(y)-\varphi(y)|=|f(y)-f(t_i)|\leqslant\epsilon$$

car $|y-t_i|\leqslant\delta(t_i)$. Donc $\sup|f-\varphi|\leqslant\epsilon$.
□

Pour les fonctions continues par morceaux maintenant.

Démonstration
Soit $\epsilon>0$. Soit f continue par morceaux. Notons $\sigma=(x_0,x_1,\dots x_n)$, une subdivision adaptée.
Alors, pour tout $k\in\mathbb{N}_n$, $f_{|]x_{k-1},x_k[}$ est continue, prolongeable en $\tilde{f}_k$ continue sur $[x_{k-1},x_k]$.
Donc il existe φ_k, escalier sur $[x_{k-1},x_k]$, tel que $\sup_{x\in]x_{k-1},x_k[}|\tilde{f}(x)-\varphi_k(x)|\leqslant\epsilon$.
Prenons alors φ en escalier tel que pour $t\in[a,b]$:

$$\varphi(t)=f(t)\text{ si }t\in\sigma\qquad\varphi(t)=\varphi_k(t)\text{ si }t\in[x_{k-1},x_k]$$

Alors $\sup_{x\in[a,b]}|f(x)-\phi(x)|\leqslant\epsilon$ □

Corollaire - Approximation uniforme par des suites de fonctions
Soit f continue par morceaux sur $[a,b]$. Alors il existe une suite $(\phi_n)_{n\in\mathbb{N}^*}$ d'éléments de $\mathscr{E}([a,b],\mathbb{R})$ telle que $\lim\limits_{n\to+\infty}\sup\limits_{[a,b]}|f-\phi_n|=0$.

Remarque - Convergence « uniforme »
Dans ce cas, on dit que la suite $(\phi_n)_n$ converge uniformément vers la fonction f.

Démonstration
On prend $\epsilon=\dfrac{1}{n}$ puis on a ϕ_n ainsi définie qui vérifie les hypothèses du corollaire. □

Corollaire - Encadrement uniforme
Soit f continue par morceaux sur $[a,b]$. Soit $\epsilon>0$.
Alors il existe deux fonctions en escalier sur $[a,b]$, ϕ et ψ, telles que

$$\phi\leqslant f\leqslant\psi\text{ et }\psi-\phi\leqslant\epsilon.$$

Démonstration
Soit $\epsilon>0$.
Il existe Φ en escalier telle que $\forall\ x\in[a,b]$, $-\frac{\epsilon}{3}\leqslant f(x)-\Phi(x)\leqslant\frac{\epsilon}{3}$ Notons $\phi=\Phi-\frac{\epsilon}{2}$ et $\psi=\Phi+\frac{\epsilon}{2}$.
Alors

$$\phi(x)=\Phi-\frac{\epsilon}{2}\leqslant\Phi-\frac{\epsilon}{3}\leqslant f(x)\leqslant\Phi+\frac{\epsilon}{3}\leqslant\Phi+\frac{\epsilon}{2}=\psi(x)$$

Et $\psi-\phi=\epsilon$. □

Pour aller plus loin - Convergence de fonctions…
La convergence de fonctions est une partie essentielle du cours de seconde année.
La convergence la plus naturelle est la convergence simple :
$(f_n)\overset{c.s.}{\to}f$

$\forall\ x\in I,\forall\ \epsilon>0\exists\ N\mid\forall\ n\geqslant N,|f_n(x)-f(x)|\leqslant\epsilon$

(Ici, chaque N dépend de x)

Mais il y a une convergence plus forte : la convergence uniforme
$(f_n)\overset{c.u.}{\to}f$

$\forall\ \epsilon>0\exists\ N\mid\forall\ x\in I,\forall\ n\geqslant N,|f_n(x)-f(x)|\leqslant\epsilon$

(c'est maintenant le même N pour tout x)

Fonctions continues par morceaux sur un intervalle

Définition - Continuité par morceaux sur un intervalle
Soit $f:I\to\mathbb{R}$. On dit que f est **continue par morceaux** sur l'intervalle I, si pour tout segment $[a,b]\subset I$, $f_{|[a,b]}$ est continue par morceaux sur le segment $[a,b]$.

Exemple - La fonction $f:x\mapsto e^{1/x}$ sur $]0,1]$
Cette fonction est continue par morceaux sur l'intervalle $]0,1]$.
Mais elle n'est pas continue sur $[0,1]$.
On notera qu'elle n'est pas bornée :

$$\forall\ M>1,\exists\ x_0\left(=\frac{1}{2\ln M}\right)\mid f(x)>M$$

Elle n'est pas limite uniforme d'une suite de fonctions en escalier.
Toute fonction en escalier est nécessairement bornée, donc $f-\varphi_k$ n'est pas bornée…

Heuristique - Situation courante dans l'étude de fonctions numériques
L'année prochaine à de nombreuses reprises, il faudra faire cette différence :
— L'étude sur l'intervalle I n'est pas possible,
— Mais celle sur tout segment inclus dans I est possible.
Incroyable mais vrai : les propriétés passeront alors en tout x de I (puisque tout x de I est dans un segment $[a,b]\subset I$).

3.2. Somme de Cauchy/Riemann associée à f sur D

Somme de Cauchy d'une fonction en escalier

On commence par une construction simple : l'intégrale de fonctions en escalier.

Analyse - Intégrale d'une fonction en escalier
On considère :
— $\phi\in\mathscr{E}([a,b],\mathbb{R})$,
— $\sigma=(a_i)_{0\leqslant i\leqslant n}$ une subdivision subordonnée à ϕ telle $\forall\ i\in[\![1,n]\!],\phi_{|]a_{i-1},a_i[}=\lambda_i$.
On a envie de prendre pour intégrale le nombre

$$I(\phi,\sigma)=\sum_{i=1}^{n}(a_i-a_{i-1})\lambda_i$$

en remarquant que $I(\phi,\sigma)$ est indépendant du choix de la subdivision subordonnée σ.
Exercice
Montrer que si σ et σ' sont deux subdivisions subordonnées à ϕ, alors $I(\phi,\sigma)=I(\phi,\sigma')$.

Correction
• Supposons tout d'abord que σ' est plus fine que σ.
σ' étant obtenue en rajoutant un nombre fini de points à σ, il suffit de le montrer lorsque σ' a un point de plus que σ.
On pose $\sigma=(a_i)_{0\leqslant i\leqslant n}$ et $\sigma'=(a_0,\dots,a_{k-1},c,a_k,\dots,a_n)$ avec $c\in]a_{k-1},a_k[$, $k\in[\![1,n]\!]$.

$$I(\phi,\sigma')=\sum_{i=1}^{k-1}\lambda_i(a_i-a_{i-1})+\lambda_k(c-a_{k-1})+\lambda_k(a_k-c)+\sum_{i=k+1}^{n}\lambda_i(a_i-a_{i-1})=\sum_{i=1}^{n}\lambda_i(a_i-a_{i-1})=I(\phi,\sigma).$$

• Supposons maintenant que σ et σ' soient deux subdivisions quelconques subordonnées à ϕ. On a vu que l'on pouvait trouver σ'' plus fine que σ et σ', et on a alors $I(\phi,\sigma)=I(\phi,\sigma'')=I(\phi,\sigma')$.

Somme de Cauchy selon une subdivision pointée

Suivant cet exemple, on définit

Définition - Somme de Cauchy de f selon σ_p
Soit f une fonction numérique défini sur le segment $[a,b]$.
Soit $\sigma_p = \big(([x_0,x_1],t_1),([x_1,x_2],t_2)\dots([x_{n-1},x_n],t_n)\big)$ une subdivision pointée de $[a,b]$.
On appelle **somme de Cauchy de f associée à σ_p** ou **selon σ_p** le nombre réel

$$S(f,\sigma_p)=\sum_{k=1}^{n}(x_k-x_{k-1})\times f(t_k)$$

On a noté nombre réel, mais si f est à valeur dans un espace vectoriel, ce nombre existe toujours (combinaison linéaire).

Remarque - Une somme de Cauchy est une intégrale

On notera que si $S(f,\mathscr{P})=\sum_{k=1}^{n}(x_k-x_{k-1})\times f(t_k)$, alors en fait, on a

$$S(f,\mathscr{P})=I(\overline{f},\sigma)$$

où $\sigma=(x_0,x_1,\dots x_n)$ (même subdivision que $\mathscr{P}$, mais non pointée) et

$$\overline{f}:x\mapsto f(t_k) \text{ si } x\in[x_{k-1},x_k[\qquad \overline{f}=\sum_{k=1}^{n}f(t_k)\mathbb{1}_{[x_{k-1},x_k[}$$

avec $\overline{f}(x_n)=f(t_n)$.

Cas d'une subdivision à pas constant

Remarque - Cas fréquents

On rencontre souvent le cas d'une subdivision σ à pas constant $\delta^*=\dfrac{b-a}{n}$:

$x_i=a+i\dfrac{b-a}{n}$ (donc $x_i-x_{i-1}=\frac{b-a}{n}$) et $t_k=x_{k-1}$ ou $t_k=x_k$, ce qui donne respectivement :

Définition - Somme de Riemann (Cauchy à pas constant)
A toute fonction $f\in\mathscr{F}([a,b],\mathbb{R})$, on associe les sommes dites de Riemann

$$R_n(f)=\frac{b-a}{n}\sum_{k=0}^{n-1}f(a+k\tfrac{b-a}{n}) \text{ ou } S_n(f)=\frac{b-a}{n}\sum_{i=1}^{n}f(a+i\tfrac{b-a}{n})$$

Remarque - Appellation uniforme
Sans précision, une somme de Riemann est une somme de Cauchy à pas constant.
Ces subdivisions apparaissent dans la « méthode des rectangles » pour obtenir des valeurs approchées de $\displaystyle\int_a^b f(t)\mathrm{d}t$.

Exemple - Calcul de $R_n(f)$ et $S_n(f)$ avec $f:x\mapsto x$ sur $[0,1]$
On considère donc la subdivision pointée à pas constant $\frac{1}{n}$: $x_0=0,\dots\ x_k=\frac{k}{n}\dots$ et $x_n=1$.

$$R_n(f)=\frac{1}{n}\sum_{k=0}^{n-1}\frac{k}{n}=\frac{1}{n^2}\frac{n(n-1)}{2}=\frac{1}{2}\frac{n-1}{n}$$

$$S_n(f)=\frac{1}{n}\sum_{k=1}^{n}\frac{k}{n}=\frac{1}{n^2}\frac{n(n+1)}{2}=\frac{1}{2}\frac{n+1}{n}$$

Puis, pour toute subdivision $\mathscr{P}$ de pas constant $\frac{1}{n}$ (mais pointée autrement), par croissance de f :

$$R_n(f)\leqslant S(f,\mathscr{P})\leqslant S_n(f)$$

Elles ont une limite commune : $\frac{1}{2}$.

Propriétés des sommes de Cauchy

Théorème - Propriétés des sommes de Cauchy (selon σ_p)
Soit $\sigma_p=\big(([x_0,x_1],t_0),\dots([x_{n-1},x_n],t_n)\big)$ une subdivision pointée de $[a,b]$.
- $f\mapsto S(f,\sigma_p)$ est une forme linéaire sur $\mathscr{F}([a,b],\mathbb{R})$.
- Si f est positive sur $[a,b]$ alors $S(f,\sigma_p)\geqslant 0$.
  Si $f\geqslant g$ sur $[a,b]$ alors $S(f,\sigma_p)\geqslant S(g,\sigma_p)$.
- Si $f\in\mathscr{F}([a,b],\mathbb{R})$, alors on a pour tout $k\in\mathbb{N}_{n-1}$,
  en notant $\sigma_p^k=\big(([x_0,x_1],t_1),\dots([x_{k-1},x_k],t_k)\big)$
  et ${}^k\sigma_p=\big(([x_k,x_{k+1}],t_{k+1}),\dots([x_{n-1},x_n],t_n)\big)$

$$S(f,\sigma_p)=S(f,\sigma_p^k)+S(f,{}^k\sigma_p) \qquad \text{relation de Chasles}$$

Démonstration
D'abord la linéarité :

$$\begin{aligned}S(\lambda f+\mu g,\sigma_p) &= \sum_{k=1}^{n}(x_k-x_{k-1})\times(\lambda f+\mu g)(t_k)=\lambda\sum_{k=1}^{n}(x_k-x_{k-1})f(t_k)+\mu\sum_{k=1}^{n}(x_k-x_{k-1})g(t_k)\\ &= \lambda S(f,\sigma_p)+\mu S(g,\sigma_p)\end{aligned}$$

Puis la positivité : Si $f\geqslant 0$, $S(f,\sigma_p)=\sum_{k=1}^{n}(x_k-x_{k-1})f(t_k)\geqslant 0$ (somme de nombres positifs).
La croissance découle de la linéarité et positivité : Si $f\geqslant g$, $S(f,\sigma_p)-S(g,\sigma_p)=S(f-g,\sigma_p)\geqslant 0$.
Enfin la relation de Chasles découle d'un découpage de la somme en 2.

$$S(f,\sigma_p)=\sum_{h=1}^{n}(x_h-x_{h-1})f(t_h)=\sum_{h=1}^{k}(x_h-x_{h-1})f(t_h)+\sum_{h=k+1}^{n}(x_h-x_{h-1})f(t_h)=S(f,\sigma_p^k)+S(f,{}^k\sigma_p)$$

□

3.3. Intégrales d'une fonction

Intégrale de Riemann : pas constant

Définition - Intégrale de f, au sens de Riemann
Soit f une fonction numérique définie sur le segment $[a,b]$.
La fonction f est dite **intégrable sur** $[a,b]$ **au sens de Riemann** ou **R-intégrable sur** $[a,b]$ s'il existe un nombre réel S tel que

$$\forall\,\epsilon>0,\exists\,\delta^*>0 \text{ telle que } \forall\ \sigma_p \text{ subdivision pointée } \delta-\text{fine},|S(f,\sigma_p)-S|<\epsilon$$

On notera $\mathscr{I}_R([a,b])$ **l'ensemble des fonctions intégrables sur** $[a,b]$ **au sens de Riemann**.
Le nombre S ci-dessus est appelé l'intégrale de la fonction f sur $[a,b]$ et est noté

$$\int_{[a,b]}f(x)\mathrm{d}x \quad \text{ou} \quad \int_a^b f(x)\mathrm{d}x \quad \text{voire} \quad \int_{[a,b]}f \quad \text{ou} \quad \int_a^b f$$

***Pour aller plus loin - Intégrale de* Stieljes**
Dans le DS9 de la saison 2018-2019, nous avions défini « l'intégrale de Stieljes de f contre g » comme :

$$\lim_{\delta(\sigma_p)\to 0}St(f,\sigma_p)=S$$

où $St(f,\sigma_p)=\sum_{k=0}^{n-1}f(t_k)(g(x_{k+1})-g(x_k))$.
Cela donne naturellement la formule d'intégration par parties dans un cas très générale (même si g n'est pas dérivable, seulement croissante).
Et dans le cas où g est dérivable, on trouve que $S=\int_a^b f(t)g'(t)\mathrm{d}t$.
Cette intégrale sert en théorie des nombres et aussi en probabilités. Elle permet de faire un lien assez naturellement entre les objets continues et les objets discrets.

On admet à ce stade que le nombre S est unique, nous le démontrerons dans le cadre plus large des fonctions intégrables au sens de Kurzweil-Henstock.

Remarque - Ecriture en fonction de n
En prenant δ de la forme $\frac{1}{n}$, comme $\delta\to 0\iff n\to+\infty$, on a la définition équivalente :

$$\forall\,\epsilon>0,\exists\,N\in\mathbb{N} \text{ telle que } \forall\ \sigma_p(N) \text{ subdivision pointée } -\frac{1}{N}\text{ fine},|S(f,\sigma_p(N))-S|<\epsilon$$

Heuristique - C'est bien une limite

On note (u_n) converge :

$$\exists\, \ell\in\mathbb{R} \quad \text{tel que} \quad \forall\, \epsilon>0,\ \exists\, N\in\mathbb{N} \quad \text{tel que} \quad \forall\, n\in\mathbb{N}, n\geqslant N,\quad |u_n-\ell|\leqslant\epsilon$$
$$\exists\, S\in\mathbb{R} \quad \text{tel que} \quad \forall\, \epsilon>0,\ \exists\, \delta^*>0 \quad \text{tel que} \quad \forall\, \sigma_p,\delta^*\text{-fine},\quad |S(f,\sigma_p)-S|\leqslant\epsilon$$

Souvenons nous que nous avions également écrit cela en terme de réunion ($\exists$), d'intersection ($\forall$), de réunion d'intersection d'ensemble.
On notera donc

$$\lim_{\delta^*(\sigma_p)\to 0} S(f,\sigma_p)=S$$

Remarque - Le sens du $\mathrm{d}x$

Si $\int f(x)\mathrm{d}x=\lim\sum_{k=0}^{n} f(t_k)(x_{k+1}-x_k)$, alors on voit que le $\mathrm{d}x$ est la limite de $(x_{k+1}-x_k)$.
Cela donne à la fois à $\mathrm{d}x$ une rôle d'infinitésimal (selon Newton), mais aussi celui d'une homogénéité à x, ce qui explique la formule du changement de variable x en $y=\varphi(x)$, alors $\mathrm{d}y=\varphi'(x)\mathrm{d}x$.
On a une condition nécessaire d'intégrabilité au sens de Riemann. C'est une *faiblesse*.

Proposition - $\mathscr{I}_R([a,b])\subset\mathscr{B}([a,b])$
Si f est intégrable sur $[a,b]$ au sens de Riemann, alors f est bornée

Démonstration
Soit f, intégrable au sens de Riemann. On note S, la valeur (finie) de son intégrale
Soit $\epsilon=1$. Il existe $\delta^*>0$ telle que pour tout subdivision pointée δ^*-fine, $|S(f,\sigma_p)-S|<\epsilon$.
Définissons une subdivision pointée σ_p particulière δ-fine :
$x_0=a$, $x_1=x_0+\frac{\delta}{2}\dots x_{k+1}=x_k+\frac{\delta}{2}=a+(k+1)\frac{\delta}{2}\dots x_n=b$, où n est tel que $a+(n-1)\frac{\delta}{2}<b\leqslant a+n\frac{\delta}{2}$, i.e. $n=\lceil\frac{2(b-a)}{\delta}\rceil$,
Soit $x\in[a,b]$, il existe $k_x\in\mathbb{N}_n$ tel que $x\in[x_{k_x-1},x_{k_x}]$.
Prenons alors pour tout $k\neq k_x$, $t_k=x_k$ et $t_{k_x}=x$.

$$\begin{aligned}|S(f,\sigma_p)-S|\leqslant 1 \quad&\Longrightarrow\quad S-1\leqslant S(f,\sigma_p)\leqslant S+1\\ &\Longrightarrow\quad \frac{2}{\delta}(S-1)-\sum_{k=1}^{n} f(a+k\tfrac{\delta}{2})\leqslant f(x)\leqslant\frac{2}{\delta}(S+1)-\sum_{k=1}^{n} f(a+k\tfrac{\delta}{2})\end{aligned}$$

Et donc $f(x)$ est borné. Ceci est vraie pour tout x, donc f est bornée. □

Exemple - $f:x\mapsto\frac{1}{\sqrt{x}}$ **et** $f(0)=0$

Cette fonction f n'est pas bornée, elle n'est donc pas intégrable au sens de Riemann
En gardant la notation générique $\sigma_p=\big(([x_{k-1},x_k],t_k),k\in\mathbb{N}_n\big)$, on a

Proposition - Contrôle sur la subdivision pointée δ^*-fine (et réciproquement)
Soit $\delta^*>0$. Si σ_p est une subdivision pointée δ^*-fine, alors $\forall\, k\in\mathbb{N}_n$ $0\leqslant x_k-x_{k-1}\leqslant\delta^*$.
Réciproquement, si σ_p est une subdivision pointée vérifiant : $\forall\, k\in\mathbb{N}_n$ $0\leqslant x_k-x_{k-1}\leqslant\delta^*$,
alors σ_p est $2\delta^*$-fine.

Remarque - Liens entre intégrale
On exploitera en particulier la réciproque pour montrer que toute fonction R-intégrable est KH-intégrable.

Démonstration
Pour le sens direct. On a les inégalités (pour tout $k\in\mathbb{N}_n$) :

$$t_k-\frac{\delta^*}{2}\leqslant x_{k-1}\leqslant t_k\leqslant x_k\leqslant t_k+\frac{\delta^*}{2}$$

Donc $0\leqslant x_k-x_{k-1}\leqslant(t_k+\frac{\delta^*}{2})-(t_k-\frac{\delta^*}{2})=\delta^*$.
Réciproquement, si $\forall\, k\in\mathbb{N}_n$ $0\leqslant x_{k+1}-x_k\leqslant\delta^*$,
alors pour tout $k\in\mathbb{N}_n$, tout $t\in[x_{k-1},x_k]$, $t-x_{k-1}\leqslant x_k-x_{k-1}\leqslant\delta^*$, donc $t_k-\frac{2\delta^*}{2}=t-\delta^*\leqslant x_{k-1}$.
De même $x_k-t_k\leqslant x_k-x_{k-1}\leqslant\delta^*$, donc $x_k\leqslant t_k+\delta^*=t_k+\frac{2\delta^*}{2}$.
Ainsi, quel que soit le pointage considéré, σ_k est $2\delta^*$ fine. □

Sommes « classiques » de Riemann

Là, on fait un petit détour sur un savoir-faire classique. On reprend les sommes à pas constant vues plus haut.

Théorème - Méthode des rectangles
Soit $f:[a,b]\to\mathbb{R}$ intégrable au sens de Riemann.
On rappelle que :

$$R_n(f)=\frac{b-a}{n}\sum_{i=0}^{n-1} f(x_i) \text{ et } S_n(f)=\frac{b-a}{n}\sum_{i=1}^{n} f(x_i) \text{ où } x_i=a+i\frac{b-a}{n}.$$

Alors

$$\lim_{n\to+\infty} R_n(f)=\lim_{n\to+\infty} S_n(f)=\int_a^b f(t)\mathrm{d}t$$

(méthode de calcul approché de $\int_a^b f(t)\mathrm{d}t$, dite méthode des rectangles).
Si f est de classe C^1 sur $[a,b]$, la vitesse de convergence est en $\frac{1}{n}$.

Pour aller plus loin - Taylor-Lagrange

Soit F de classe $\mathscr{C}^1$, deux fois dérivable sur $[a,b]$.
Soit $\psi:t\mapsto F(t)-F(b)+(b-t)F'(t)-\frac{M}{2}(b-t)^2$ tel que $\psi(a)=0$.
C'est possible avec

$$M=\frac{2(F(a)-F(b)-(b-a)F'(a))}{(b-a)^2}.$$

Alors $\psi(a)=\psi(b)=0$.
Donc il existe c tel que $\psi'(c)=0$.
Or $\psi'(t)=F'(t)-F'(t)+(b-t)F''(t)-M(b-t)$
Or $\psi'(c)=0$ et donc $M=F''(c)$.
Et donc $\psi(a)=0=F(a)-F(b)+(b-a)F'(a)-\frac{(b-a)^2}{2}F''(c)$.
$F(a)=F(b)+(a-b)F'(b)+\frac{1}{2}(a-b)^2F''(c)$.

Démonstration
On suppose que f est intégrable au sens de Riemann.
Soit $\epsilon>0$, alors, on a vu qu'il existe δ^* tel que, pour tout σ_p δ^*-fine, $|S(f,\sigma_p)-\int_a^b f|\leqslant\epsilon$.
Alors en notant pour tout $n\in\mathbb{N}$, $x_i=a+i\frac{b-a}{n}$,
$\sigma_p^1(n)=\big(([x_0,x_1],x_0),([x_1,x_2],x_1),\dots,([x_{n-1},x_n],x_{n-1})\big)$ et $\sigma_p^2(n)=\big(([x_0,x_1],x_1),([x_1,x_2],x_2),\dots,([x_{n-1},x_n],x_n)\big)$ ont un pas égal à $\frac{b-a}{n}$.
Si $n\geqslant N=\lceil\frac{b-a}{\delta^*}\rceil$, alors $\delta(\sigma_p^1(n))=\delta(\sigma_p^2(n))=\frac{b-a}{n}\leqslant\delta^*$.
Donc, $|S(f,\sigma_p^1(n))-\int_a^b f|\leqslant\epsilon$ et $|S(f,\sigma_p^2(n))-\int_a^b f|\leqslant\epsilon$.
Ainsi,

$$\lim_{n\to+\infty} S(f,\sigma_p^1(n))=\lim_{n\to+\infty}\frac{b-a}{n}\sum_{i=0}^{n-1} f(x_i)=\int_a^b f(t)\mathrm{d}t$$
$$\lim_{n\to+\infty} S(f,\sigma_p^2(n))=\lim_{n\to+\infty}\frac{b-a}{n}\sum_{i=1}^{n} f(x_i)=\int_a^b f(t)\mathrm{d}t$$

□

Démontrons maintenant l'ordre de grandeur de la vitesse de convergence lorsque f est de classe $\mathscr{C}^1$.
On exploite ici un résultat non encore démontré mais largement exploité depuis le début de l'année : le théorème de Taylor-Lagrange.
On notera que ce qui compte vraiment, c'est que f' soit R-intégrable plutôt que f de classe $\mathscr{C}^1$…

Démonstration
Dans le cas où f est en outre de classe $\mathscr{C}^1$. Notons F une primitive de f, on a donc, par télescopage :

$$\int_a^b f(t)\mathrm{d}t-R_n(f)=F(b)-F(a)-\sum_{k=0}^{n-1}\frac{b-a}{n}f(x_k)=\sum_{k=0}^{n-1}\Big(F(x_{k+1})-F(x_k)-\frac{b-a}{n}f(x_k)\Big)$$

F est de classe $\mathscr{C}^2$, on peut appliquer le théorème de Taylor-Lagrange (marge)

$$\exists\, t_k\in[x_k,x_{k+1}],\qquad F(x_{k+1})=F(x_k)+(x_{k+1}-x_k)F'(x_k)+\frac{(x_{k+1}-x_k)^2}{2}F''(t_k)$$

Ce qui signifie exactement :

$$\exists\, t_k\in[x_k,x_{k+1}],\qquad F(x_{k+1})=F(x_k)+\frac{b-a}{n}f(x_k)+\frac{(b-a)^2}{2n^2}f'(t_k)$$

Donc

$$\frac{2n}{b-a}\times\int_a^b f(t)\mathrm{d}t-R_n(f)=\frac{2n}{b-a}\times\Big(\sum_{k=0}^{n-1}\Big(F(x_{k+1})-F(x_k)-\frac{b-a}{n}f(x_k)\Big)\Big)=\frac{(b-a)}{n}\sum_{k=0}^{n-1}f'(t_k)=S(f',\sigma_p)$$

où σ_p est la subdivision pointée : $\{([x_0,x_1],t_0),\dots([x_{n-1},x_n],t_n)\}$,
Comme f' est continue (f est de classe $\mathscr{C}^1$) : $S(f',\mathscr{P}_n)\to\int_a^b f'(t)\mathrm{d}t=f(b)-f(a)$.
On a donc

$$\int_a^b f(t)\mathrm{d}t-R_n(f)\underset{n\to+\infty}{\sim}\frac{b-a}{2n}(f(b)-f(a))$$

□

Si f est suffisamment régulière, on pourrait prolonger ce calcul pour avoir un DL plus précis...

Exemple - Cas particulier courant

Dans le cas particulier (très courant) où $a=0, b=1$, on a donc

$$\lim_{n\to+\infty}\frac{1}{n}\sum_{i=0}^{n-1}f\left(\frac{i}{n}\right)=\lim_{n\to+\infty}\frac{1}{n}\sum_{i=1}^{n}f\left(\frac{i}{n}\right)=\int_0^1 f(t)\mathrm{d}t.$$

Savoir faire - Reconnaitre les sommes de Riemann à pas constant : limite

Si l'on doit chercher la limite pour $n\to+\infty$ d'une somme k de a_n à b_n dont le terme général dépend de k ET de n, c'est très probablement une somme de Riemann à pas constant !

1. On commence par tout factoriser par n afin de transformer tous les k en $\frac{k}{n}$.
2. On écrit sur un brouillon la formule de Riemann pour mieux identifier.
3. Le facteur devant $\frac{k}{n}$ vaut $b-a$ (premier terme reconnu), le nombre additionné à $\frac{k}{n}(b-a)$ vaut a (second terme reconnu)
4. On en déduit la valeur de b. Puis on identifie pour trouver f
5. Si besoin on factorise pour faire apparaitre devant la somme $\frac{b-a}{n}$

On exploite les relations avec les primitives, démontrées plus tard mais largement utilisées depuis le début de l'année (et la relation de Chasles directe).

Savoir faire - Reconnaitre les sommes de Riemann à pas constant : vitesse de convergence

On a reconnu la formule avec le savoir-faire précédent. Il s'agit de calculer la vitesse de convergence.

1. On remplace la limite $\ell=\int_a^b f(t)\mathrm{d}t$ par $F(b)-F(a)=\sum_{k=0}^{n-1}F(x_{k+1})-F(x_k)$
2. Il s'agit d'évaluer la différence : $\sum_{k=0}^{n-1}[(x_{k+1}-x_k)f(x_k)-(F(x_{k+1})-F(x_k))]$.
3. La formule de Taylor-Lagrange donne l'existence d'un c_k tel que $(x_{k+1}-x_k)f(x_k)-(F(x_{k+1})-F(x_k))=\frac{1}{2}(x_{k+1}-x_k)^2f'(c_k)$
4. On remplace par leur valeur les x_k :

$$R_n-\ell=\frac{b-a}{2n}\times\frac{b-a}{n}\sum_{k=0}^{n-1}f'(c_k)\sim\frac{(b-a)}{2n}(f(b)-f(a))$$

Attention - Il ne s'agit pas de série !!

Bien que cela y ressemble fortement, les suites R_n ou S_n ne sont pas les sommes partielles de série.
En effet, dans la cas des séries, le terme général ne dépend que de k (et pas de n).
Ici il y a bien un mélange des deux variables : n et k compris entre 0 et n...
Il faut prendre le coup d'oeil pour bien différencier ces deux objets (par

, ailleurs il ne faut pas non plus confondre série et somme de Riemann)

Exercice

Déterminer la limite quand n tend vers $+\infty$ de $\sum_{k=1}^{n}\frac{1}{n+k}$.

Quelle est la vitesse de convergence ? (Savoir-faire)

Correction

Notons $f:x\mapsto\frac{1}{1+x}$, $a=0$, $b=1$, alors

$$S_n(f)=\frac{1}{n}\sum_{k=1}^{n}\frac{1}{1+\frac{k}{n}}=\sum_{k=1}^{n}\frac{1}{n+k}\xrightarrow[n\to\infty]{}\int_0^1 f(t)\mathrm{d}t=\int_0^1\frac{1}{1+t}\mathrm{d}t=\ln 2$$

Pour la vitesse de convergence, il s'agit de donner un équivalent de $S_n(f)-\ln(2)$.

On note $f:x\mapsto\ln(1+x)$. Rappelons que $S_n(f)=\frac{1}{n}\sum_{k=1}^{n}f'(x_k)$.

Donc

$$\ln 2-S_n(f)=\sum_{k=1}^{n}f(x_k)-f(x_{k-1})-\frac{1}{n}f'(x_k)$$

Donc il existe $t_k\in[x_{k-1},x_k]$ tel que

$$f(x_k)-f(x_{k-1})-\frac{1}{n}f'(x_k)=\frac{1}{2n^2}f''(t_k)$$

Et donc, on reconnait une somme de Riemann :

$$\ln 2=S_n(f)+\frac{1}{2n}\left(f'(1)-f'(0)\right)+o\left(\frac{1}{n}\right)=S_n(f)-\frac{1}{4n}+o\left(\frac{1}{n}\right)$$

Corollaire - Méthode des trapèzes

Soit $f:[a,b]\to\mathbb{R}$ continue. Alors

$$\frac{R_n(f)+S_n(f)}{2}=\frac{b-a}{n}\sum_{i=0}^{n-1}\frac{f(a_i)+f(a_{i+1})}{2}\xrightarrow[n\to+\infty]{}\int_a^b f(t)\,dt$$

Intégrale de Kurzweil-Henstock : le pas est défini par une jauge

Pour aller plus loin - Ecriture de la convergence

Certains auteurs écrivent :

$$\int_a^b f(x)\mathrm{d}x:\lim_{\delta(\sigma_p)\to 0}S(f,\sigma_p)=S$$

ou encore

$$\int_a^b f(x)\mathrm{d}x:=\lim_{KH,\sigma_p}S(f,\sigma_p)$$

nous verrons que cela a du sens, et que c'est bien pratique

Définition - Intégrale de f

Soit f une fonction numérique définie sur le segment $[a,b]$.
La fonction f est dite **intégrable sur** $[a,b]$**, au sens de Kurzweil-Henstock** ou **KH-intégrable sur** $[a,b]$ s'il existe un nombre réel S tel que

$$\forall\,\epsilon>0,\exists\,\delta:[a,b]\to\mathbb{R}_+^*\text{ tq }\forall\,\sigma_p\in\delta-\mathfrak{S},\ |S(f,\sigma_p)-S|<\epsilon$$

On notera $\mathscr{I}([a,b])$ **l'ensemble des fonctions intégrables sur** $[a,b]$.
Le nombre S ci-dessus est appelé l'intégrale de la fonction f sur $[a,b]$ et est noté

$$\int_{[a,b]}f(x)\mathrm{d}x\quad\text{ou}\quad\int_a^b f(x)\mathrm{d}x\quad\text{voire}\quad\int_{[a,b]}f\quad\text{ou}\quad\int_a^b f$$

On dit que δ est ϵ-adaptée à f. On note $D_{KH}(f,\epsilon)$, l'ensemble des jauges ϵ-adaptée à f.
On notera que si $\delta\in D_{KH}(f,\epsilon)$, $\quad\forall\,\delta'\leqslant\delta,\delta'\in D_{KH}(f,\epsilon)$
$\forall\,\epsilon'>\epsilon,\delta\in D_{KH}(f,\epsilon')$.

Evidemment, la jauge δ dépend de ϵ fixé a priori.
Il nous faudrait donc maintenant préciser ce qu'est l'ensemble $\mathscr{I}([a,b])$.

Remarque - Existence d'une subdivision δ-fine

Cette définition serait problématique si pour une jauge δ, il n'existait pas de subdivision δ-fine.
Heureusement, le lemme de COUSIN nous montre que ceci est impossible. Notre définition semble donc opérante.

Ce serait le même problème pour la question de $\lim_{n\to+\infty}$ ie $\exists N\in\mathbb{N}$ tel que $\forall\, n\geqslant N$ si l'ensemble $\{n\in\mathbb{N}\mid n\geqslant N\}$ était vide. Ce qui n'est pas le cas grâce au lemme d'Archimède.

Exemple - Intégrale d'une fonction nulle sauf en un nombre fini de points

On considère une fonction f définie sur $[a,b]$.
On suppose qu'il existe $(y_i)_{i\in\mathbb{N}_p}$ tel que $a<y_i<y_{i+1}<b$ et $f(y_i)\neq 0$, alors que $f(t)=0$ si $t\notin\{y_i\}$.

Soit $\epsilon>0$ et $\delta: t\mapsto\begin{cases}\frac{1}{2}\min\{y_{i+1}-y_i, i\in\mathbb{N}_{p-1}\} & \text{si } t\notin\{y_i\}\\ \frac{\epsilon}{p}\frac{1}{f(y_i)} & \text{si } t=y_i\end{cases}$

Si σ_p est δ-fine, on a vu que $x_k-x_{k-1}\leqslant\delta(t_k)$.
Et donc si σ_p est δ-fine, à r éléments, alors dans le pire des cas (tous les y_i sont des t_k, sinon $f(t_k)=0$) :

$$S(f,\mathscr{P})=\sum_{k=1}^{r}(x_k-x_{k-1})\times f(t_k)\leqslant\sum_{i=1}^{p}\delta(y_i)f(y_i)=\epsilon$$

Exercice

Si le nombre de points (y_i) est infini mais dénombrable. Montrer qu'on a encore $\int_a^b f(t)\mathrm{d}t=0$

Correction

On a de même pour tout subdivision σ_p, δ fine et à r éléments dont p sont des y_i :

$$S(f,\sigma_p)=\sum_{k=1}^{r}(x_k-x_{k-1})\times f(t_k)\leqslant\sum_{i=1}^{p}\delta(y_i)f(y_i)$$

En prenant

$$\delta: t\mapsto\begin{cases}\frac{1}{2}\min\{y_{i+1}-y_i, i\in\mathbb{N}_{p-1}\} & \text{si } t\notin\{y_i\}\\ \frac{\epsilon}{2^i}\frac{1}{f(y_i)} & \text{si } t=y_i\end{cases}$$

On alors

$$S(f,\sigma_p)\leqslant\sum_{i=1}^{p}\frac{\epsilon}{2^i f(y_i)}f(y_i)\leqslant\epsilon\sum_{i=1}^{+\infty}\frac{1}{2^i}=\epsilon$$

Proposition - Unicité de l'intégrale
Si f est R-intégrable sur $[a,b]$, alors f est KH-intégrable.
Si f est intégrable, son intégrale est unique (définie de l'une ou l'autre des façons).

Démonstration
Si f est R-intégrable, il existe S telle que :
pour tout $\epsilon>0$, il existe $\delta^*>0$, tel que $\forall\,\mathscr{P}$ δ^*-fine $|S(f,\mathscr{P})-S|\leqslant\epsilon$.
On prend alors la jauge $\delta: t\mapsto\delta^*$, constante.
Toute subdivision pointée σ_p δ-fine et alors δ^*-fine.
On a donc $|S(f,\sigma_p)-S|\leqslant\epsilon$ et f est KH-intégrable.
Montrons l'unicité :
Soit $\epsilon>0$, deux jauges δ_1 et δ_2, et deux nombres S_1 et S_2
telles que $\forall\,(\sigma_p)_1$ δ_1-fine et $\forall\,(\sigma_p)_2$ δ_2-fine $|S(f,(\sigma_p)_1)-S_1|\leqslant\epsilon$ et $|S(f,(\sigma_p)_2)-S_2|\leqslant\epsilon$.
Considérons alors la jauge $\delta=\min(\delta_1,\delta_2)$ (pour tout $t\in[a,b]$, $\delta(t)=\min(\delta_1(t),\delta_2(t))$.
Soit alors une subdivision pointée $(\sigma_p)_3$ adaptée à δ.
Alors, on a vu, $(\sigma_p)_3$ est à la fois δ_1-fine et δ_2-fine, donc :

$$|S_1-S_2|\leqslant|S_1-S(f,(\sigma_p)_3)|+|S(f,(\sigma_p)_3)-S_2|\leqslant 2\epsilon$$

Cette inégalité est vraie pour tout $\epsilon>0$, donc $S_1=S_2$. □

L'exemple qui suit, montre qu'il n'est pas nécessaire que la fonction soit bornée pour être KH-intégrable.
Il donne aussi une méthode pour savoir comment choisir δ, adaptée à f.

Exemple - $x\mapsto\frac{1}{\sqrt{x}}$ sur $]0,1]$

On considère $f:[0,1]\to\mathbb{R}_+$, $x\mapsto\begin{cases}0 & \text{si } x=0\\ \frac{1}{\sqrt{x}} & \text{sinon}\end{cases}$

Pour aller plus loin - Cas d'un nombre dénombrable de points non nuls
Le résultat marche aussi pour un nombre dénombrable de points.
Pour δ, on considère $\frac{\epsilon}{2^i}$ au lieu de $\frac{\epsilon}{p}$.
Comme $\mathbb{Q}$ est dénombrable alors $\mathbb{1}_{\mathbb{Q}\cap[0,1]}$ est KH-intégrable, d'intégrale nulle.

Pour aller plus loin - Ecriture de la convergence (2)
On peut résumer en :

$$\int_a^b f(x)\mathrm{d}x:=\lim_{\delta^*(\sigma_p)\to 0}S(f,\sigma_p)$$

$$\Longrightarrow\int_a^b f(x)\mathrm{d}x:=\lim_{\delta(\sigma_p)\to 0}S(f,\sigma_p)$$

Ceci est dû au fait que
$\{\mathscr{P}$ subdivisions pointées δ-fine, $\forall\,\delta>0\}$
$\subset\{\mathscr{P}$ subdivisions pointées δ-fine, $\forall\,\delta$ jauge$\}$.

Pour aller plus loin - Fonction à valeurs vectorielles
En seconde année, on étudie les fonctions de $\mathbb{R}\to E$, où E est un espace vectoriel normé (on parle de fonction vectorielle). Pour ces fonctions, tout se passe de la même façon…

On a vu que pour la subdivision à n points telle que pour tout $k\in\{0,1,\dots n\}$, $x_k=\frac{k^2}{n^2}$, alors pour toute famille (t_k) tel que $t_k\in[x_{k-1},x_k]$ et $\mathscr{P}=(([x_{k-1},x_k],t_k))_{k\in\mathbb{N}_n}$:

$$S(f,\mathscr{P})-\frac{1}{n^2\sqrt{t_1}}\xrightarrow[n\to\infty]{}2$$

Mais il nous fallait maîtriser ce terme : $\frac{1}{n^2\sqrt{t_1}}$ avec t_1 non bornée…
Il nous faudrait FORCER la subdivision pointée δ-fine à prendre $t_1=0$, dans ce cas $f(t_1)=0$ et nous n'aurions plus ce problème…
Soit $\epsilon>0$.

1. On prend $\delta_1: t\mapsto\begin{cases}1 & \text{si } t=0\\ \frac{t}{2} & \text{sinon}\end{cases}$. Il s'agit bien d'une jauge définie sur $]0,1]$
   Toute subdivision pointée δ_1-fine prendra $t=0$ comme point de marquage nécessairement.
2. Ensuite, on s'occupe du calcul $\sum_{k=2}^{n}(x_k-x_{k-1})f(t_k)$.
   On commence avec $k=2$, car la jauge δ_1 force t_1 à valoir 0 et donc $f(t_1)=0$.
   Il s'agit d'encadrer $(x_k-x_{k-1})f(t_k)$; cela ressemble beaucoup à l'égalité des accroissements finis.
   Notons $F: x\mapsto 2\sqrt{x}$, de dérivée f sur $]0,1]$.
   Alors, il existe $c_k\in]x_{k-1},x_k[$ tel que $F(x_k)-F(x_{k-1})=(x_k-x_{k-1})F'(c_k)=(x_k-x_{k-1})f(c_k)$

   $$(x_k-x_{k-1})f(t_k)-\big(F(x_k)-F(x_{k-1})\big)=(x_k-x_{k-1})\times\big(f(t_k)-f(c_k)\big)$$

   Par téléscopage :

   $$\begin{aligned}\sum_{k=1}^{n}(x_k-x_{k-1})f(t_k)-2 &=\sum_{k=1}^{n}(x_k-x_{k-1})f(t_k)-(F(1)-F(0))\\ &=\sum_{k=1}^{n}\big((x_k-x_{k-1})f(t_k)-F(x_k)-F(x_{k-1})\big)\\ &=\sum_{k=1}^{n}\big((x_k-x_{k-1})\times\big(f(t_k)-f(c_k)\big)\big)\end{aligned}$$

   Par inégalité triangulaire :

   $$\left|\sum_{k=1}^{n}(x_k-x_{k-1})f(t_k)-2\right|\leqslant\sum_{k=1}^{n}\big((x_k-x_{k-1})\times|f(t_k)-f(c_k)|\big)$$

   Or $c_k\in]x_{k-1},x_k[\subset\left]t_k-\frac{\delta(t_k)}{2},t_k+\frac{\delta(t_k)}{2}\right[$; comment assurer que $|f(c_k)-f(t_k)|<\epsilon$, sachant que $|c_k-t_k|\leqslant\frac{\delta(t_k)}{2}$?
   Avec la continuité tout simplement ! f est continue sur $]0,1]$, donc

   $$\forall\, t\in]0,1],\exists\,\delta_2(t)>0\qquad\text{tel que}\qquad|c-t|<\frac{\delta_2(t)}{2}\Rightarrow|f(c)-f(t)|<\epsilon$$

   On prend donc ainsi δ_2, en ajoutant $\delta_2(0)=1$.
   On a alors pour tout subdivision de $[0,1]$, $\mathscr{P}=\big(([x_{k-1},x_k],t_k)_{k\in\mathbb{N}_n}\big)$ δ_2-fine :

   $$\left|\sum_{k=1}^{n}(x_k-x_{k-1})f(t_k)-2\right|\leqslant\sum_{k=1}^{n}\big((x_k-x_{k-1})\times\epsilon\big)=\epsilon(x_n-x_1)=\epsilon(1-x_1)<\epsilon$$

Ainsi, avec $\delta=\min(\delta_1,\delta_2)$, on a pour tout subdivision de $[0,1]$, $\mathscr{P}=\big(([x_{k-1},x_k],t_k)_{k\in\mathbb{N}_n}\big)$

$$\left|\sum_{k=0}^{n}(x_k-x_{k-1})f(t_k)-2\right|\leqslant(x_1-x_0)f(0)+\sum_{k=1}^{n}\big((x_k-x_{k-1}\epsilon\big)\leqslant\epsilon$$

Pour aller plus loin - Fonction intégrable au sens de Lebesgue
*f est intégrable au sens de Lebesgue si f **ET** $|f|$ sont toutes deux intégrables au sens de Kurzweil-Henstock.*
Mais la démarche est différente, c'est une raison qu'il fait qu'il s'agit de l'intégrale souvent privilégiée dans le second cycle (école d'ingénieur ou université).

Savoir faire - A chaque problème sa jauge!
Vous aurez peu d'exercices où il faudra montrer à la main, la KH-intégrabilité.
Une idée (parmi d'autres) : pour chaque problème de la fonction f, on crée une jauge qui contient une solution à ce problème (pointage…).
Puis, on prend la jauge minimale, qui contient la solution à tous les pro-

blèmes

4. Espaces et sous-espaces des fonctions intégrables, ou : Qui est intégrable?

Si la jauge peut être choisie constante, alors la fonction est R-intégrable et donc KH-intégrable, sinon elle est KH-intégrable (ou rien).
Nous le verrons sur différents exemples

4.1. Notations

Définition - Ensemble
On note $\mathscr{I}_{\mathscr{R}}([a,b])$ l'ensemble des fonctions R-intégrables sur $[a,b]$.
On note $\mathscr{I}_{\mathscr{KH}}([a,b])$ l'ensemble des fonctions KH-intégrables sur $[a,b]$.
Si on ne précise pas : $\mathscr{I}([a,b])$ est un abus de notation de $\mathscr{I}_{\mathscr{KH}}([a,b])$.
Par abus, on peut aussi oublier de noter $([a,b])$, si le contexte est assez clair.
On rappelle que $\mathscr{C}_M([a,b],\mathbb{R})$ est l'ensemble des fonctions continues par morceaux définies sur $[a,b]$ est à valeurs dans $\mathbb{R}$.

Un des buts de ce chapitre est de caractériser ces ensembles, donner des exemples…

4.2. Passage à la limite des propriétés de somme de Riemann

Les propriétés suivantes découlent des résultats sur les sommes de Riemann. Plus précisément : par continuité et croissance du passage à la limite

$$\lim_{\delta(\sigma_p)\to 0} S(f,\sigma_p) = \int_a^b f$$

Théorème - Extensions des propriétés de l'intégrale

- $\mathscr{I}([a,b])$ et $\mathscr{C}_M([a,b],\mathbb{R})$ sont des espaces vectoriels et $f \mapsto \int_{|a,b|} f$ est une forme linéaire sur $\mathscr{I}([a,b])$ et sur $\mathscr{C}_M([a,b],\mathbb{R})$
- positivité : $f \in \mathscr{I}([a,b])$, $f \geqslant 0 \Rightarrow \int_{|a,b|} f \geqslant 0$
- croissance : $f,g \in \mathscr{I}([a,b])$, $f \geqslant g \Rightarrow \int_{|a,b|} f \geqslant \int_{|a,b|} g$
- majoration en valeur absolue : $f \in \mathscr{C}_M([a,b]) \Rightarrow |f| \in \mathscr{C}_M(\mathbb{R})$ et

$$\left|\int_{|a,b|} f\right| \leqslant \int_{|a,b|} |f|$$

En revanche, on n'a pas nécessairement : $f \in \mathscr{I} \Rightarrow |f| \in \mathscr{I}$.
mais, si f et $|f| \in \mathscr{I}([a,b])$, alors $\left|\int_{|a,b|} f\right| \leqslant \int_{|a,b|} |f|$.

Démonstration

- Soient $(\lambda,\mu) \in \mathbb{R}^2$, $(f,g) \in \mathscr{I}([a,b])^2$. Soit $\epsilon > 0$, $\exists\, \delta_f, \delta_g$ tel que :
  $\forall\, \sigma_p$ δ_f-fine, $|S(f,\sigma_p) - \int_a^b f| \leqslant \frac{\epsilon}{2\lambda}$
  $\forall\, \sigma_p$ δ_g-fine, $|S(g,\sigma_p) - \int_a^b g| \leqslant \frac{\epsilon}{2\mu}$ On prend $\delta = \min(\delta_f,\delta_g)$, c'est une jauge.
  $\forall\, \sigma_p$ δ-fine, alors σ_p est δ_f-fine et δ_g-fine, donc par linéarité des sommes de Riemann, puis inégalité triangulaire :

$$\left|S(\lambda f+\mu g\sigma_p) - \left(\lambda\int_a^b f + \mu\int_a^b g\right)\right| \leqslant \left|S(f,\sigma_p) - \int_a^b f\right| + \left|S(g,\sigma_p) - \int_a^b g\right| \leqslant \epsilon$$

Pour aller plus loin - Structure d'algèbre
Si f et $g \in \mathscr{I}([a,b])$, on ne peut pas espérer grand chose de $f \times g$.
Souvenons-nous qu'il n'y a pas de relation simple entre $\int f\times g$ et $\int f$ et $\int g$.

Concernant la composition, on peut montrer que si $f \in \mathscr{I}([a,b])$ et $\varphi : [c,d] \to [a,b]$ dérivable à dérivée bornée, alors $f\circ\varphi \times |\varphi'| \in \mathscr{I}([c,d])$. De même si f dérivable sur $[a,b]$ et φ sur $[c,d]$ avec $\varphi([c,d]) \subset [a,b]$, alors $f'\circ\varphi \times \varphi' \in \mathscr{I}([c,d])$.

Pour aller plus loin - Linéarité de $\lim_{KH}$
On notera que la première propriété signifie $\mathscr{I}([a,b])$ est bien un espace vectoriel et que $\int_a^b \cdot$ est une forme linéaire sur cet espace car $\lim_{\delta(\sigma_p)\to 0} \cdot$ est linéaire.

- Si f est positive, alors pour tout σ_p, $S(f,\sigma_p) \geqslant 0$.
  Pour tout $\epsilon > 0$, $\exists\, \sigma_p$ tel que $\int_a^b f \geqslant S(f,\sigma_p) - \epsilon \geqslant -\epsilon$.
  Ainsi , pour tout $\epsilon > 0$, $\int_a^b f \geqslant -\epsilon$, cela impose : $\int_a^b f \geqslant 0$.
- $f - g \geqslant 0$, la linéarité et la positivité donnent alors le résultat.
- Une subdivision adaptée à f l'est également pour $|f|$.
  Puis, comme $|f| - f \geqslant 0$ et $|f| + f \geqslant 0$, on applique la linéarité
  et on trouve le résultat $\int_a^b |f| \geqslant \max\left(\int_a^b f, -\int_a^b f\right) = \left|\int_a^b f\right|$.

□

4.3. Fermeture par convergence uniforme

Avant de faire la liste des fonctions intégrables au sens de Riemann ou au sens de Kurzweil-Henstock, nous avons besoin d'un théorème de stabilité.

Cas simple des fonctions en escalier

Remarque - Fonction intégrable au sens de Riemann
f est intégrable au sens de Riemann si dans la définition précédente la jauge δ est nécessairement constante.
On a vu que c'est le même passage de l'uniforme continuité (jauge constante comme l'intégrale de Riemann) à la continuité plus souple (jauge adaptée comme pour l'intégrale de Kurzweil-Henstock).
Pour démontrer que les fonctions en escalier sont KH-intégrables, on exploitera une jauge constante. On en déduit qu'elles sont en fait R-intégrable.

Analyse - Fonction créneau et fonction en escalier
Considérons la fonction créneau générique $f = \mathbb{1}_{[c,d]}$. Le candidat d'intégration est $(d-c)$.
Soit $\epsilon > 0$, fixé quelconque. Soit $\delta > 0$ avec $\delta \leqslant \frac{\epsilon}{2}$.
Considérons une subdivision pointée δ-fine : $\big(([x_0,x_1],t_1),\dots([x_{n-1},x_n],t_n)\big)$.
Il existe $1 \leqslant i \leqslant j \leqslant n$ tel que $c \in [x_{i-1},x_i]$ et $d \in [x_{j-1},x_j]$.
On a alors pour tout $k < i$ et $k > j$, $f(t_k) = 0$; puis pour $k \in [i+1,j-1] \subset [c,d]$, $f(t_k) = 1$.
Ainsi, on a :

$$S(f,\sigma_p) = \sum_{k=1}^{n}(x_k - x_{k-1})f(t_k) = \sum_{k=i}^{j}(x_k - x_{k-1})f(t_k) = (x_i - x_{i-1})f(t_i) + (x_j - x_{j-1})f(t_j) + (x_{j-1} - x_i)$$

Et donc on a la majoration (puisque $f(t_i) = 0$ ou $f(t_i) = 1$:

$$|S(f,\sigma_p - (d-c)| = |(c - x_{i-1})f(t_i) + (x_i - c)(f(t_i)-1) + (d - x_{j-1})(f(t_j)-1) + (x_j - d)f(t_j)| \leqslant |\alpha|(x_i - x_{i-1}) + (x_j$$

Donc f est Riemann-intégrable, d'intégrale égale à $(d-c)$. Considérons maintenant une fonction ϕ en escalier et $\tau = (a_0,a_1,\dots a_n)$ subordonnée à ϕ.
Supposons donc que $\phi = \sum_{i=1}^{n} \lambda_i \mathbb{1}_{[a_{i-1},a_i]}$. On applique alors la linéarité, vu plus haut :

$$\int_a^b \phi = \sum_{i=1}^{n} \lambda_i \int_a^b \mathbb{1}_{[a_{i-1},a_i]} = \sum_{i=1} n\lambda_i(a_i - a_{i-1})$$

Les fonctions en escalier sur un segment sont donc R-intégrables et donc KH-intégrables.

Proposition - Intégration des fonction en escalier
Les fonctions en escalier sur un segment sont donc R-intégrables et KH-intégrables.
Et plus précisément si $f \in \mathscr{E}([a,b])$,

$$\int_a^b f(t)\mathrm{d}t = I(f,\sigma) = \sum_{i=1}^{n}(a_i - a_{i-1})\lambda_i$$

où $\sigma = (a_0, a_1, \dots, a_n)$ est une subdivision quelconque subordonnée à f.

Stabilité uniforme

Théorème - Encadrement
Une fonction f est KH-intégrable sur $[a,b]$ si et seulement si,
pour tout $\epsilon > 0$, il existe deux fonctions $f_{-\epsilon}$ et $f_{+\epsilon}$ KH-intégrables tq :

$$f_{-\epsilon} \leqslant f \leqslant f_{+\epsilon} \quad \text{et} \quad \left| \int_a^b f_{+\epsilon} - \int_a^b f_{-\epsilon} \right| \leqslant \epsilon$$

On a le même résultat de fermeture d'espace des fonctions R-intégrables par convergence uniforme :

Proposition - Encadrement
Une fonction f est R-intégrable sur $[a,b]$ si et seulement si,
pour tout $\epsilon > 0$, il existe deux fonctions $f_{-\epsilon}$ et $f_{+\epsilon}$ R-intégrables tq :

$$f_{-\epsilon} \leqslant f \leqslant f_{+\epsilon} \quad \text{et} \quad \left| \int_a^b f_{+\epsilon} - \int_a^b f_{-\epsilon} \right| \leqslant \epsilon$$

Il s'agit de la même structure de démonstration, mais la jauge est restreinte à l'ensemble des jauges constantes dans le second cas.

Démonstration
• Si f est intégrable, elle vérifie l'implication en prenant $f_{-\epsilon} = f_{+\epsilon} = f$.
• Réciproquement, supposons que f vérifie la condition du théorème.
Il faut commencer par trouver un candidat pour I.
Notons $I_+ = \inf\{\int_a^b f_+ \mid f_+ \geqslant f \text{ et } f_+ \in \mathscr{I}([a,b])\}$.
I_+ existe bien car
l'ensemble considéré est un sous-ensemble de $\mathbb{R}$, non vide
et minorée par $\int_{[a,b]} f_{-1}$.
Notons $I_- = \sup\{\int_a^b f_- \mid f_- \leqslant f \text{ et } f_- \in \mathscr{I}([a,b])\}$.
I_- existe bien car
l'ensemble considéré est un sous-ensemble de $\mathbb{R}$, non vide
et majorée par $\int_{[a,b]} f_{+1}$.
Par ailleurs d'après l'énoncé, pour tout $\epsilon > 0$,

$$0 \leqslant I_+ - I_- \leqslant \int_a^b f_{+\epsilon} - \int_a^b f_{-\epsilon} \leqslant \epsilon$$

Ce qui permet d'affirmer que $I_+ = I_-$.
Notons cette valeur I et montrer que f est intégrable d'intégrale égale à I.
Soit $\epsilon > 0$, Il existe δ_+ et δ_- telles que pour toutes sub. pointées σ_p^+ δ_+-fine et σ_p^- δ_--fine,

$$\left| S(f_{+\epsilon}, \sigma_p^+) - \int_a^b f_{+\epsilon} \right| \leqslant \epsilon \qquad \left| S(f_{-\epsilon}, \sigma_p^-) - \int_a^b f_{-\epsilon} \right| \leqslant \epsilon$$

Comme plus haut, on considère $\delta = \min(\delta_+, \delta_-)$. δ est plus fine.
Soit σ_p, une subdivision pointé δ-fine, donc également δ_+-fine et δ_--fine .

$$S(f,\sigma_p) - I \leqslant S(f_{+\epsilon}) - \int_a^b f_{-\epsilon} \leqslant \int_a^b f_{+\epsilon} - \int_a^b f_{-\epsilon} + \epsilon$$

Et

$$S(f,\sigma_p) - I \geqslant S(f_{-\epsilon}) - \int_a^b f_{+\epsilon} \leqslant \int_a^b f_{-\epsilon} - \int_a^b f_{-\epsilon} - \epsilon$$

Donc

$$|S(f,\sigma_p) - I| \leqslant 2\epsilon$$

□

Pour aller plus loin - $\mathscr{I}([a,b])$
En fait, on peut démontrer mieux : $\mathscr{I}([a,b])$ est un espace vectoriel ordonné…
Il semble qu'ils vérifient une certaine propriété de continuité

Fonctions continues par morceaux

Pour l'étude des fonctions continues (par morceaux).
Nous savons que les fonctions en escalier sur $[a,b]$ sont intégrables, donc avec le théorème de stabilité vue plus haut :

Proposition - $\mathscr{C}_{\mathscr{M}}([a,b]) \subset \mathscr{I}([a,b])$
Toute fonction continue par morceaux sur $[a,b]$ est R-intégrable et KH-intégrable sur $[a,b]$.

Corollaire - Fonction continue
Soit f continue sur $[a,b]$, alors f est R-intégrable KH-intégrable sur $[a,b]$

Démonstration
On applique le théorème d'encadrement avec deux fonctions en escaliers qui encadrent f et sont donc intégrables. □

Remarque - Changement de valeurs en quelques points
Lorsque l'on change la valeur de f continue par morceaux en un nombre fini de points, on ne change pas la valeur de l'intégrale.
On peut le voir avec f_1 comme fonction nulle sauf en un nombre fini de points (fonction en escalier).
Puis on exploiter la linéarité pour une fonction f quelconque.

Remarque - Calcul d'aire
Si $f \geqslant 0$, $\int_{[a,b]} f$ représente, en unité d'aire, l'aire comprise entre la courbe, l'axe Ox et les droites d'équations $x = a$ et $x = b$.

4.4. Théorèmes fondamentaux de l'analyse

A ce stade, on n'a pas besoin de faire la différence entre les deux intégrales. Cela change avec la partie qui suit.

Histoire - La clé
Ce résultat a été trouvé indépendamment par Newton et Leibniz (bien avant que l'intégrale soit réellement définie de manière satisfaisante).
Une grande tension entre les mathématiciens britanniques et ceux du continent s'est alors produite suite à une querelle de priorité…

Fonction dérivable

Théorème - Théorème fondamental du calcul différentiel (version forte)
Soit $F : [a,b] \to \mathbb{R}$ une fonction continue sur $[a,b]$, dérivable sur $]a,b[$ et admettant une dérivée à droite en a et à gauche en b.
Notons f la dérivée de F. Alors f est KH-intégrable ($f \in \mathscr{I}([a,b])$) et :

$$\int_a^b f(t)\,\mathrm{d}t = F(b) - F(a)$$

Remarque - Jauge adaptée, inégalité des accroissements finis et réciproque
Il faut trouver une jauge bien adaptée. Comme le montre la démonstration, cette jauge nous est fourni par le théorème des accroissements finis.
D'une certaine façon, l'utilisation de la jauge pour définir l'intégration est une sorte de réciproque du théorème des accroissements finis.

Démonstration
Soit $\epsilon > 0$.
On cherche donc à trouver une jauge δ sur $[a,b]$ telle que :

$$\forall\, \mathscr{P} \text{ subdivision } \delta - \text{fine}, \quad |S(f,\mathscr{P}) - (F(b) - F(a))| < \epsilon$$

Si $\mathscr{P} = \{([x_0,x_1],t_1),([x_1,x_2],t_2)\dots([x_{n-1},x_n],t_n)\}$, alors $S(f,\mathscr{P}) = \sum_{k=1}^{n} f(t_k)\times(x_k-x_{k-1})$.

et (par téléscopage) : $F(b)-F(a) = F(x_n)-F(x_0) = \sum_{k=1}^{n}(F(x_k)-F(x_{k-1}))$.

Donc, avec l'inégalité triangulaire

$$|S(f,\mathscr{P})-(F(b)-F(a))| = \left|\sum_{k=1}^{n} f(t_k)\times(x_k-x_{k-1})-(F(x_k)-F(x_{k-1}))\right| \leqslant \sum_{k=1}^{n}\left|f(t_k)\times(x_k-x_{k-1})-(F(x_k)-F(x_{k-1}))\right|$$

Reste à trouver la jauge puis la subdivision pointée.
Soit ϵ'. Soit $x\in]a,b[$. F est dérivable en x, de dérivée f :

$$\exists\,\delta(x)\mid\forall\, y\in]a,b[,|y-x|\leqslant\delta(x)\Longrightarrow\left|\frac{F(y)-F(x)}{y-x}-f(x)\right|\leqslant\epsilon\Longrightarrow\left|(F(y)-F(x))-f(x)(y-x)\right|\leqslant\epsilon'|y-x|$$

Nous avons ainsi défini une jauge δ. Si $\mathscr{P}$ est δ-fine,
alors en prenant $x=t_k$, $y=x_{k-1}$ (comme $x_{k-1}\in[t_k-\delta(t_k);t_k+\delta(t_k)]$) :

$$|F(x_{k-1}-F(t_k))-f(t_k)(x_{k-1}-t_k)|\leqslant\epsilon'|x_{k-1}-t_k|=\epsilon'(t_k-x_{k-1})$$

et en prenant $x=t_k$, $y=x_k$ (comme $x_k\in[t_k-\delta(t_k);t_k+\delta(t_k)]$) :

$$|F(x_k-F(t_k))-f(t_k)(x_k-t_k)|\leqslant\epsilon'|x_k-t_k|=\epsilon'(x_k-t_k)$$

Enfin par inégalité triangulaire :

$$\begin{aligned}\left|f(t_k)\times(x_k-x_{k-1})-(F(x_k)-F(x_{k-1}))\right| &= |f(t_k)\times(x_k-t_k+t_k-x_{k-1})-(F(x_k)-F(t_k)+F(t_k)-F(x_{k-1})|\\ &= ||[F(x_{k-1}-F(t_k))-f(t_k)(x_{k-1}-t_k)]-[F(x_k-F(t_k))-f(t_k)(x_k-t_k)]|\\ &\leqslant |F(x_{k-1}-F(t_k))-f(t_k)(x_{k-1}-t_k)|+|F(x_k-F(t_k))-f(t_k)(x_k-t_k)|\end{aligned}$$

Donc

$$\left|f(t_k)\times(x_k-x_{k-1})-(F(x_k)-F(x_{k-1}))\right|\leqslant\epsilon'(x_k-t_k)+\epsilon'(t_k-x_{k-1})=\epsilon'(x_k-x_{k-1})$$

En sommant, il vient :

$$|S(f,\mathscr{P})-(F(b)-F(a))|\leqslant\sum_{k=1}^{n}\epsilon'(x_k-x_{k-1})=\epsilon'(b-a)$$

En prenant $\epsilon'=\dfrac{\epsilon}{b-a}$, on trouve le résultat recherché □

Remarque - Retour sur le choix de la jauge

La jauge δ est définie ici en fonction du contrôle des variations de la dérivée (ou de la dérivée seconde). Si $f=F'$ varie beaucoup au voisinage de x, alors la jauge $\delta(x)$ est relativement petite.

Savoir faire - Trouver la jauge pour une fonction f admettant une primitive F

Si f admet une primitive F, i.e. $F'=f$, alors on a une jauge naturelle : celle de la la dérivation de F.

$$\forall\,\epsilon>0,\exists\,\delta:[a,b]\to\mathbb{R}_+^*,\forall\, x,y\in[a,b],\ |y-x|\leqslant\delta(x)\Rightarrow\left|\frac{F(y)-F(x)}{y-x}-f'(x)\right|\leqslant\epsilon$$

Alors si σ_p est δ-fine :

$$\int_a^b f(t)\mathrm{d}t-(F(b)-F(a))=\sum_{k=1}^{r}[(x_{k+1}-x_k)f(t_k)-(F(x_{k+1})-F(t_k))-(F(t_k)-F(x_k))]$$

$$\int_a^b f(t)\mathrm{d}t-(F(b)-F(a))\leqslant\epsilon(b-a)$$

en respectant la croissance : $x_k<t_k<x_{k+1}$

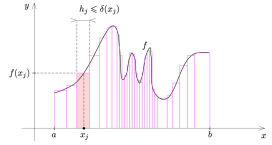
Primitives

Remarque - Rappels. Revoir le chapitre 6

Les résultats qui suivent justifient le cours du chapitre 6 (calcul de primitives) vu en début d'année.
Il est bon de retravailler ce cours, en particulier :

- Revoir les primitives usuelles
- Revoir la méthode du changement de variable pour le calcul d'intégrale
- Revoir la méthode de l'intégration par parties pour le calcul d'intégrale

Représentation - Choix de la jauge



(illustration extraite de l'excellent cours de Jean-Pierre Demailly)

Théorème - Théorème fondamental du calcul différentiel (version faible)

Soit f continue sur I, intervalle de $\mathbb{R}$, à valeurs dans $\mathbb{K}$ (=$\mathbb{R}$ ou $\mathbb{C}$). Soit $a\in I$.
Alors la fonction

$$\begin{array}{rccc}F: & I & \to\mathbb{K}\\ & x & \mapsto\displaystyle\int_a^x f(t)\,dt\end{array}$$

est de classe C^1 sur I et $F'=f$.
C'est de plus l'unique primitive de f nulle en $a\in I$.

Pour aller plus loin - Et si f n'est pas continue...

Ce n'est pas grave, si f est KH-intégrable sur I, alors la fonction F définie de la même façon est dérivable et de dérivée $F'=f$ presque partout. C'est à dire si $A=\{x\in I\mid F'(x)-f(x)\neq 0\}$, alors $\int_I \mathbb{1}_A=0$.
La théorie de la mesure de Lebesgue se cache derrière cette porte...

Démonstration
D'après la partie précédente, cette fonction F est bien définie.
Pour faire cette démonstration, nous exploitons les propriétés de l'intégration d'une fonction : relation de Chasles (directe), et positivité.
Nous les démontrerons plus tard, mais sans exploiter cette partie. Il n'y a donc pas d'auto-référence démonstrative
. On évalue son taux de variations ($h>0$) :

$$\frac{F(x+h)-F(x)}{h}=\frac{1}{h}\int_x^{x+h} f(t)\mathrm{d}t$$

Or f est continue sur $[x,x+h]$, donc il existe $m_h,M_h\in[x,x+h]$ tel que : pour tout $x\in[x,x+h]$, $f(m_h)\leqslant f(x)\leqslant f(M_h)$ On n'a par positivité de l'intégrale

$$f(m_h)\leqslant\frac{f(m_h)}{h}\int_x^{x+h}1\mathrm{d}t\leqslant\frac{1}{h}\int_x^{x+h}f(t)\mathrm{d}t\leqslant\frac{f(M_h)}{h}\int_x^{x+h}1\mathrm{d}t=f(M_h)$$

Et comme $M_h,m_h\to x$ lorsque h tend vers 0 et f est continue en x :
$\frac{F(x+h)-F(x)}{h}\to f(x)$ lorsque h tend vers 0, par valeurs supérieures.
Le cas $h\to 0^-$ est identique (une inversion de signe près) □

Corollaire - Primitive pour une fonction continue

Toute fonction continue sur I admet une primitive sur I.

Ce résultat se démontre également en restant dans le cadre des fonctions au sens de Riemann. Car toute fonction continue sur une segment est uniformément continue, elle est donc intégrable au sens de Riemman (on peut prendre une jauge constante).

Attention - Pas toutes les primitives

On n'obtient pas toutes les primitives ainsi.
Un contre-exemple : pour $f(x)=\cos x$, la primitive $F(x)=\sin x+2$ ne peut s'obtenir ainsi.

Et on retrouve le résultat largement exploité depuis le début d'année :

Théorème - Expression en fonction d'une primitive

Soit f continue sur I intervalle de $\mathbb{R}$ contenant a et b. Soit F une primitive de f. Alors

$$\int_a^b f(t)\mathrm{d}t=F(b)-F(a)=\Big[F(t)\Big]_a^b.$$

Démonstration
Soit $F_a:x\mapsto\int_a^x f(t)\,dt$ et F une autre primitive, on a $F=F_a+C$ avec C une constante et

$$\int_a^b f(t)\,dt=F_a(b)=F(b)-C=F(b)-F(a).$$

□

Remarque - Cas des fonctions continues par morceaux

• Si une fonction f, continue par morceaux, admet une primitive, alors f est continue. En effet, soit F telle que $F' = f$, F' admet des limites à droite et à gauche en tout point, or si F est dérivable (donc continue) et $F'_{/I\cap]-\infty,a[}$ admet une limite ℓ_1 alors $F'(a) = \ell_1$ (de même à droite avec ℓ_2, par théorème de prolongement des fonctions dérivables) et donc $\ell_1 = \ell_2 = f(a)$, c'est-à-dire que $f = F'$ est continue en a.

• Si f est continue par morceaux, $x \mapsto \int_a^x f(t)\,dt$ est continue sur I, dérivable en tout point x_0 en lequel f est continue avec $F'(x_0) = f(x_0)$ et sinon $F'_g(x_0) = \lim\limits_{a_i^-} f$ et $F'_d(x_0) = \lim\limits_{a_i^+} f$.

Attention - Dérivation

Si f est continue et que $G : x \mapsto \int_{x_0}^x f(t)\mathrm{d}t$, alors G est dérivable et $G'(x) = f(x)$ et non : $f(x) - f(x_0)$, comme lu souvent!

Savoir faire - Etudier $x \mapsto \int_{h_1(x)}^{h_2(x)} f(t)\mathrm{d}t$

Supposons f est continue, h_1 et h_2 dérivable. Notons F une primitive de f,

$$G : x \mapsto \int_{h_1(x)}^{h_2(x)} f(t)\mathrm{d}t = F(h_2(x)) - F(h_1(x))$$

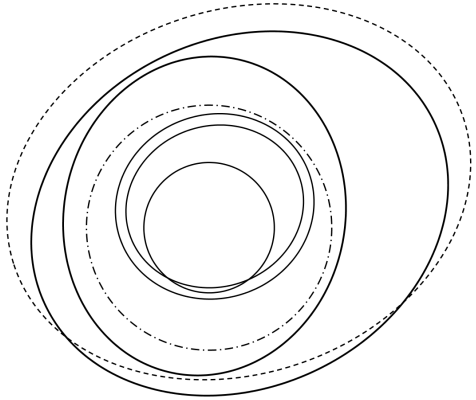
dérivable par composition (et soustraction) de dérivée :

$$G'(x) = h_2'(x)\times F'(h_2(x)) - h_1'(x)\times F'(h_1(x)) = h_2'(x)\times f(h_2(x)) - h_1'(x)\times f(h_1(x))$$

4.5. Bilan en termes d'espaces vectoriels croissants

Afin de visualiser les résultats en termes d'ensemble, on peut faire un diagramme de Wenn.
Notons que ces ensembles sont toujours **des espaces vectoriels** et que la forme naturelle d'un espace vectoriel n'est pas celle d'une « patate » (mais plutôt celle d'un plan dans un espace euclidien...).
Ecrire sur le diagramme suivant où se trouve les espaces vectoriels :

— $\mathscr{B}([a,b])$
— $\mathscr{C}([a,b])$
— $\mathscr{C}_M([a,b])$
— $\mathscr{E}([a,b])$
— $\overline{\mathscr{E}([a,b])}^u$, l'ensemble des limites uniformes des fonctions en escalier
— $\mathscr{R}([a,b])$
— $\mathscr{R}_R([a,b])$



5. L'intégrale comme un « outil puissant » de l'analyse

5.1. Relation de CHASLES

Une première implication

Théorème - Relation de Chasles

Soient $f \in \mathscr{F}([a,b],\mathbb{R})$ et $c \in]a,b[$.
Si les restrictions de f à $[a,c]$ et à $[c,b]$ sont intégrables, alors f est intégrable sur $[a,b]$.
Dans ce cas :

$$\int_{[a,b]} f = \int_{[a,c]} f + \int_{[c,b]} f$$

L'idée : faire des extractions de subdivisions et un forçage en c.

Démonstration

Soit c tel $f_1 = f_{|[a,c]} \in \mathscr{I}([a,c])$ et $f_2 = f_{||c,b]} \in \mathscr{I}([c,b])$.
Soit $\epsilon > 0$ et δ_1 et δ_2 tel que

$\forall\,(\sigma_p)_1 - \delta_1$ adaptée $|S(f_1,(\sigma_p)_1) - \int_a^c f_1(t)\mathrm{d}t| < \frac{\epsilon}{2}$.

$\forall\,(\sigma_p)_2 - \delta_2$ adaptée $|S(f_2,(\sigma_p)_2) - \int_c^b f_2(t)\mathrm{d}t| < \frac{\epsilon}{2}$.

Soit

$$\delta : t \mapsto \begin{cases} \min(\delta_1(t), \frac{c-t}{2}) & \text{si } t < c \\ \min(\delta_2(t), \frac{t-c}{2}) & \text{si } t > c \\ \min(\delta_1(c),\delta_2(c)) & \text{si } t = c \end{cases}$$

Soit σ_p une subdivision δ-adaptée, elle est forcée, donc c est un point de marquage.
Notons k tel que $c = t_k$. Alors $\{x_0,x_1,\dots x_{k-1}\} \subset [a,c]$ et $\{x_k,x_{k+1},\dots x_n\} \in [c,b]$.

$$\left|S(f,\sigma_p) - \left(\int_a^c f + \int_c^b f\right)\right| = \left|\sum_{j=1}^{k-1}(x_j - x_{j-1})f(t_j) + \underbrace{(x_{k+1}-x_k)f(c)}_{(c-x_k)f(c)+(x_{k+1}-c)f(c)} + \sum_{j=k+1}^{n}(x_j - x_{j-1})f(t_j) - \left(\int_a^c f + \int_c^b f\right)\right|$$

Donc si l'on considère les subdivision ${}^k\sigma_p = \left(([x_0,x_1],t_1),\dots([x_{k-1},c],c)\right)$ et $\sigma_p^k = \left(([c,x_k],c),([x_k,x_{k+1}],t_{k+1},\dots([x_{n-1},x_n],t_n)\right)$ de $[a,c]$ et $[b,c]$.
Elles sont respectivement δ_1 et δ_2 adaptée, donc :

$$\left|S(f,\sigma_p) - \left(\int_a^c f + \int_c^b f\right)\right| \leqslant \left|S(f_1,{}^k\sigma_p) - \int_a^c f_1\right| + \left|S(f_2,\sigma_p^k) - \int_c^b f_2\right| \leqslant \epsilon$$

Donc f est bien intégrable et $\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_c^b f(t)\mathrm{d}t$ □

Remarque - Retour sur la démonstration de la version faible du théorème fondamentale

Pour la version faible, on suppose f continue sur I, donc nécessairement intégrable sur $[a,x]$ (ou $[x,a]$ respectivement), mais aussi sur $[a,x+h]$ et $[x,x+h]$ (resp. $[x+h,a]$ et $[x,x+h]$).

On peut appliquer ce théorème de Chasles direct. Donc $F(x+h)-F(x) = \int_a^{x+h} f(t)\mathrm{d}t - \int_a^x f(t)\mathrm{d}t = \int_x^{x+h} f(t)\mathrm{d}t$.

Une réciproque? Critère de Cauchy pour l'intégrale

Il y a bien une réciproque, si l'on se concentre sur les segments (intervalles compacts).

Analyse - $f \in \mathscr{I}([a,b]) \Rightarrow f \in \mathscr{I}([a',b'])$?

On suppose que $a < a' < b' < b$ et f définie sur $[a,b]$, intégrable sur $[a,b]$.

Est-ce que f est intégrable sur $[a',b']$?

Il faut être capable de proposer un candidat à $\int_{a'}^{b'} f(t)\mathrm{d}t$.

C'est comme pour les suites, pour montrer leur convergence, on a besoin de donner ℓ, afin de montrer que $|u_n - \ell| < \epsilon$.

A l'époque dans le cours sur les suites, nous avions trouver une méthode pour démontrer la convergence d'une suite sans définir ℓ : l'utilisation du critère de Cauchy.

Rappel :

Proposition - Critère de Cauchy-Suite

Soit (u_n) telle que

$$\forall\, \epsilon > 0, \exists\, N \mid \forall\, p,q \geqslant N, |u_p - u_q| \leqslant \epsilon$$

Alors (u_n) est convergente (et réciproquement)

Remarque - Démonstration

Pour la démonstration, on a :

1. Montrer que (u_n) étaient bornée ($\epsilon = 1$, puis N, puis $\forall\, p \geqslant N$, $u_p \in [u_N - 1, u_N + 1]$)
2. Montrer que $(u_{\varphi(n)})$ était convergente (BW) vers ℓ.
3. Puis que (u_n) (en entier) converge vers ℓ

On a la proposition suivante :

Proposition - Critère de Cauchy-Intégrale

Soit $f : [a,b] \to \mathbb{R}$ telle que

$$\forall\, \epsilon > 0, \exists\, \delta : [a,b] \to \mathbb{R}_+^* \mid \forall\, (\sigma_p)_1, (\sigma_p)_2, \delta\text{-fine}, |S(f,(\sigma_p)_1) - S(f,(\sigma_p)_2)| \leqslant \epsilon$$

Alors f est intégrable sur $[a,b]$.

La réciproque est vraie : si f est intégrable, alors elle vérifie le critère Cauchy

Démonstration

Commençons par le sens indirect.

Soit $\epsilon > 0$, il existe $\delta : [a,b] \to \mathbb{R}_+^*$ tel que $\forall\, \sigma_p, \delta$-fine $\left| \int_a^b f(t)\mathrm{d}t - S(f,\sigma_p)\right| \leqslant \frac{\epsilon}{2}$.

Alors $\forall\, (\sigma_p)_1, (\sigma_p)_1, \delta$-fine,

$$|S(f,(\sigma_p)_1) - S(f,(\sigma_p)_2)| \leqslant |S(f,(\sigma_p)_1) - \int_a^b f(t)\mathrm{d}t - | + | \int_a^b f(t)\mathrm{d}t - S(f,(\sigma_p)_2| \leqslant 2\frac{\epsilon}{2} \leqslant \epsilon$$

d'après l'inégalité triangulaire.

Réciproquement, prenons $\epsilon = \frac{1}{n}$.

Pour aller plus loin - Limitesup

Prenons $\epsilon = 1$, et donc il existe N tel que $\forall\, p \geqslant N$, $u_p \in [u_N - 1, u_N + 1]$.

Donc (u_p) est bornée (à partir d'un certaine raing)

On note $v_q = \sup\{u_p, p \geqslant q\}$. (v_q) est décroissante et minorée donc convergente vers ℓ.

On montre ensuite que (u_n) converge vers ℓ.

Il existe $\delta_n : [a,b] \to \mathbb{R}_+^*$, tel que $\forall\, (\sigma_p)_1, (\sigma_p)_2$ δ_n-fine, $|S(f,(\sigma_p)_1) - S(f,(\sigma_p)_2)| \leqslant \frac{1}{n}$.

Libérons n et notons, pour tout $n \in \mathbb{N}$ $\Delta_n : t \mapsto \min(\delta_k(t), k \leqslant n)$.

Ainsi Δ_n est décroissante, et si (σ_p) est Δ_n-fine, elle est δ_n-fine.

Considérons, pour tout $n \in \mathbb{N}$, $(\tau_p)_n$, une subdivision pointée Δ_n fine.

Notons, pour tout $n \in \mathbb{N}$, $u_n = S(f,(\tau_p)n)$.

Soit $\epsilon > 0$, alors il existe $N \in \mathbb{N}$ tel que $\frac{1}{N} < \epsilon$.

Puis, pour tout $r \geqslant q \geqslant N$, alors $(\tau_p)_r$ est Δ_q fine (par décroissance) :

$$|u_q - u_r| = |S(f,(\tau_p)_q) - S(f,(\tau_p)_r)| \leqslant \frac{1}{q} \leqslant \frac{1}{N} \leqslant \epsilon$$

Ainsi, la suite (u_r) est de Cauchy donc convergente. On note $S = \lim(u_r)$.

Soit $\epsilon > 0$ et $N \in]\frac{1}{\epsilon}, +\infty[\cap \mathbb{N}$.

Soit σ_p une subdivision pointée Δ_N-fine et $r > N$ ($(\tau_p)_r$ est Δ_n-fine) :

$$|S(f,\sigma_p) - S(f,(\tau_p)_r)| \leqslant \frac{1}{N} \leqslant \epsilon$$

Reste à passer à la limite pour $r \to +\infty$: $|S(f,\sigma_p) - S| \leqslant \epsilon$.

Donc f est intégrable sur $[a,b]$ □

Application - Théorème d'encadrement

Il est possible de démontrer de nouveau le théorème d'encadrement avec le théorème de Cauchy.

Vous pouvez le faire comme exercice.

Appliquons ce résultat à la réciproque du théorème de Chasles

Proposition - Diminution du segment d'intégration

Si f est intégrable sur $[a,b]$, alors pour tout $a', b' \in]a,b[$, $f_{|[a',b']}$ est intégrable sur $[a',b']$

Démonstration

Soit $\epsilon > 0$. Soit $\delta : [a,b] \to \mathbb{R}_+^*$ tel que $\forall\, (\sigma_p)_1, (\sigma_p)_2, \delta$-fine, $|S(f,(\sigma_p)_1) - S(f,(\sigma_p)_2)| \leqslant \epsilon$.

On applique ici le critère réciproque de Cauchy pour f intégrable. Soit $\delta' = \delta_{|[a',b']}$, il s'agit bien d'une jauge sur $[a',b']$.

On note également $f' = f_{|[a',b']}$.

Soient $(\sigma_p)'_1$ et $(\sigma_p)'_2$ deux subdivisions pointées δ'-fine.

On les complète sur $[a,b]$ en deux subdivisions $(\sigma_p)_1$ et $(\sigma_p)_2$ deux subdivisions pointées δ-fine, en ajoutant exactement les mêmes points.

Donc

$$|S(f',(\sigma_p)'_1) - S(f',(\sigma_p)'_2)| = |S(f',(\sigma_p)_1) - S(f',(\sigma_p)_2)| < \epsilon$$

car on ajoute les mêmes termes pour les calculs de $S(f',(\sigma_p)_1)$ et de $S(f',(\sigma_p)_2)$

Donc d'après le critère direct de Cauchy pour que f' soit intégrable :

f' est intégrable sur $[a',b']$. □

Corollaire - Réciproque de Chasles

Si f est intégrable sur $[a,b]$ et $c \in]a,b[$.

Alors les restrictions de f sont intégrable sur $[a,c]$ et sur $[c,b]$ respectivement et $\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_c^b f(t)\mathrm{d}t$

Démonstration

Pour démontrer ce résultat, on démontre d'abord les intégrabilités sur $[a,c]$ et sur $[c,b]$ avec la proposition précédentes.

Puis on applique le théorème de Chasles direct. □

Généralisation (notation)

Définition - Notations
Soient I un segment, f intégrable sur I, $(a,b)\in I^2$. On pose :

$$\text{si } a<b,\quad \int_a^b f(t)\,dt=\int_{[a,b]} f$$
$$\text{si } a>b,\quad \int_a^b f(t)\,dt=-\int_{[b,a]} f$$
$$\text{si } a=b,\quad \int_a^b f(t)\,dt=0.$$

Proposition - Relation de Chasles
Avec ces notations, la relation de Chasles s'écrit, pour tout $(a,b,c)\in\mathbb{R}^3$,

$$\int_a^b f(t)\mathrm{d}t=\int_a^c f(t)\mathrm{d}t+\int_c^b f(t)\mathrm{d}t.$$

Démonstration
Il suffit d'envisager les différentes positions possibles de a,b,c. □

Lemme de Henstock et sous-subdivision

Heuristique - Sous-subdivisions

Considérons une subdivision pointé $\sigma_p=\big(([x_0,x_1],t_1),\dots([x_{n-1},x_n],t_n)$ de $[a,b]$. On est amené à évaluer

$$\int_a^b f(t)\mathrm{d}t-S(f,\sigma_p)=\sum_{k=1}^n\int_{x_{k-1}}^{x_k} f(t)\mathrm{d}t-(x_k-x_{k-1})f(t_k)=\sum_{k=1}^n\int_{x_{k-1}}^{x_k}\big(f(t)-f(t_k)\big)\mathrm{d}t$$

d'après la relation de Chasles (et intégration d'une constante).
Lorsque cette différence est comprise entre $-\epsilon$ et $+\epsilon$, est-ce qu'on est assuré que chaque terme $\int_{x_{k-1}}^{x_k}\big(f(t)-f(t_k)\big)\mathrm{d}t$ est également en valeur absolue plus petite que ϵ? Et une somme quelconque de ces termes : $\sum_{k\in J\subset\mathbb{N}_n}\int_{x_{k-1}}^{x_k}\big(f(t)-f(t_k)\big)\mathrm{d}t$?

Définition - Sous-subdivision
Soit $\sigma_p=\big(([x_0,x_1],t_1),\dots([x_{n-1},x_n],t_n)$ une subdivision pointée d'un segment $[a,b]$.
On dit que s_p est une sous-subdivision de σ_p, s'il existe $I\subset\mathbb{N}_n$ tel que $s_p=\big([x_{k-1},x_k],t_k\big),k\in I\big)$.
L'ensemble I est appelé ensemble d'appui de la sous-subdivision s_p à partir de σ_p.
On appelle domaine de s_p, l'ensemble $\mathscr{D}(s_p)=\bigcup_{k\in I}[x_{k-1},x_k]$.

Exemple - Cas simple

$\sigma_p=\big(([0,1],0),([1,\frac{3}{2}],\frac{5}{4}),([\frac{3}{2},3],2),([3,4],4)\big)$.
Alors $s_p=\big(([1,\frac{3}{2}],\frac{5}{4}),([3,4],4)\big)$ est une sous-subdivision de σ_p d'appui $I=\{2,4\}$.
On notera également que s_p n'est **pas** une subdivision de $[0,4]$; ce n'est pas une subdivision d'un intervalle (mais d'une réunion)

Théorème - Lemme de Henstock
Soient $f\in\mathscr{I}([a,b])$ et $\epsilon>0$.
Soit δ, une jauge ϵ-adaptée à f, i.e. $\delta\in D_{KH}(f,\epsilon)$.
(Donc $\forall\ \sigma_p$, δ-fine, $|S(f,\sigma_p)-\int_a^b f(t)\mathrm{d}t|\leqslant\epsilon$).
Alors pour toute sous-subdivision s_p d'une subdivision σ_p, δ-fine et d'appui I

$$\left|S(f,s_p)-\int_{\mathscr{D}(s_p)}f(t)\mathrm{d}t\right|=\left|\sum_{k\in I}\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t\right|\leqslant\epsilon$$

Pour aller plus loin - Subdivision ?
On peut aussi dire que s_p est une subdivision pointée de $\mathscr{D}(s_p)$ qui la plupart du temps n'est pas un intervalle…

Pour aller plus loin - Intégrales impropres (1)
Dans le cadre de l'intégrale de Riemann, il n'est pas possible de donner du sens à des intégrales comme $I=\int_0^1\frac{1}{\sqrt{t}}\mathrm{d}t$ car l'intégrant n'est pas borné. L'astuce, vue en seconde année, consiste à définir ce nombre I comme la limite : $\int_0^1\frac{1}{\sqrt{t}}\mathrm{d}t:=\lim_{x\to0}(2\sqrt{1}-2\sqrt{x})$.
Pour l'intégrale KH, ceci n'est en règle pas générale grâce au théorème de Hacke qui découle du lemme de Henstock : f est KH-intégrable sur $[a,b]$ ssi $\forall\ c\in[a,b]$, f est KH-intégrable sur $[a,c]$ et $F(c):=\int_a^c f(t)\mathrm{d}t$ admet une limite finie en b.
Dans ce cas $\lim_{c\to b}F(c)=\int_a^b f(t)\mathrm{d}t$.

Remarque - Une jauge adaptée à f, sur toute la longueur

Ce « lemme » signifie que, pour toute partie de $[a,b]$ que vous regardez, la sous-subdivision donne une somme de Riemann ϵ-ment proche de l'intégrale.
Cette proximité se retrouve uniformément tout au long de la fonction.
Autrement écrit : si la somme de Cauchy calculée globalement est proche de la valeur de l'intégrale, ce n'est pas avec des compensations entre quantités positives et quantités négatives, mais bien parce que toutes les différences sont plus petites qu'ϵ (au plus).

Démonstration
On va commencer par une extraction de subdivision. Puis on développera l'argument pour une sous-subdivision.
Soient $f\in\mathscr{I}([a,b])$ et $\epsilon>0$.
Soit δ, une jauge tel que $\forall\ \sigma_p$, δ-fine, $|S(f,\sigma_p)-\int_a^b f(t)\mathrm{d}t|\leqslant\epsilon$.
Considérons la sous-subdivision (extraction ici) : $\sigma_k=([x_{k-1},x_k],t_k)$.
Notons $\alpha>0$ (on le fera tendre vers 0).
f est intégrable sur $[a,b]$, f est intégrable sur $[a,x_{k-1}]$, sur $[x_k,b]$.
Donc il existe une jauge δ_1 sur $[a,x_{k-1}]$ et une jauge δ_2 sur $[x_k,b]$ telles que,
pour toute subdivision $(\tau_p)_1$, δ_1-fine et toute subdivision $(\tau_p)_2$, δ_2-fine,

$$\left|S(f_1,(\tau_p)_1)-\int_a^{x_{k-1}}f_1(t)\mathrm{d}t\right|\leqslant\alpha\text{ et }\left|S(f_2,(\tau_p)_2)-\int_{x_k}^b f_2(t)\mathrm{d}t\right|\leqslant\alpha$$

où l'on a noté $f_1=f_{|[a,x_{k-1}]}$ et $f_2=f_{|[x_k,b]}$.
Soit $(\rho_p)_1$ une subdivision pointée $\min(\delta_1,\delta_{|[a,x_{k-1}]})$-fine sur $[a,x_{k-1}]$.
Soit $(\rho_p)_2$ une subdivision pointée $\min(\delta_2,\delta_{|[x_k,b]})$-fine sur $[x_k,b]$.
Soit $(\rho_p)=(\rho_p)_1\oplus\sigma_k\oplus(\rho_p)_2$ (c'est plus une concaténation qu'une réunion, puisque ce sont des listes et non des ensembles.) Alors (ρ_p) est δ-fine, donc $\left|S(f,\rho_p)-\int_a^b f(t)\mathrm{d}t\right|\leqslant\epsilon$.
En découpant les sommes et intégrales (Chasles) :

$$\left|S(f_1,(\rho_p)_1)-\int_a^{x_{k-1}}f(t)\mathrm{d}t+S(f_{|[x_{k-1},x_k]},\sigma_k)-\int_{x_{k-1}}^{x_k}f(t)\mathrm{d}t+S(f_2,(\rho_p)_2)-\int_{x_k}^b f(t)\mathrm{d}t\right|\leqslant\epsilon$$

Donc, par inégalité triangulaire renversée :

$$\left|S(f_{|[x_{k-1},x_k]},\sigma_k)-\int_{x_{k-1}}^{x_k}f(t)\mathrm{d}t\right|\leqslant\epsilon+\left|S(f_1,(\rho_p)_1)-\int_a^{x_{k-1}}f_1(t)\mathrm{d}t\right|+\left|S(f_2,(\rho_p)_2)-\int_{x_k}^b f_2(t)\mathrm{d}t\right|$$

Or $(\rho_p)_1$ est également δ_1-fine et $(\rho_p)_2$ est également δ_2-fine, donc

$$\left|S(f_{|[x_{k-1},x_k]},\sigma_k)-\int_{x_{k-1}}^{x_k}f(t)\mathrm{d}t\right|\leqslant\epsilon+2\alpha$$

Ce résultat étant vraie pour tout $\alpha>0$:

$$\left|S(f_{|[x_{k-1},x_k]},\sigma_k)-\int_{x_{k-1}}^{x_k}f(t)\mathrm{d}t\right|\leqslant\epsilon$$

Cette démonstration se généralise sans problème, en coupant en r-morceaux la subdivision pointée σ_p initiale pour donner s_p et en considérant des subdivisions δ_i-fine (associée à α et avec $\epsilon\leftarrow\frac{\epsilon}{5}$) sur le complémentaire de $\mathscr{D}(s_p)$ dans $[a,b]$… □

Pour aller plus loin - Intégrales impropres (2)
Il reste également à définir une intégrale sur un intervalle non bornée.
Pour la KH-intégrale sur $\mathbb{R}$, on doit préciser adapter la notion de jauge adaptée.
On dit que $\sigma_p=\big([x_{i-1},x_i],t_i),i\in\mathbb{N}_n\big)$ est une subdivision de $[a,+\infty[$ δ_∞-fine si :
- *$x_n=+\infty$ (et $t_n=+\infty$)*
- *$\forall\ k\in\mathbb{N}_{n-1}$: $t_k-\frac{\delta(t_k)}{2}\leqslant x_{k-1}\leqslant t_k\leqslant x_k\leqslant t_k+\frac{\delta(t_k)}{2}$*
- *$\frac{1}{\delta(t_n)}\leqslant x_{n-1}$ (rappel : $t_n=+\infty$)*

Le théorème de Hacke peut s'appliquer également, et on retrouve les intégrales impropres de seconde année.

Application - Majoration de la somme des valeurs absolues

Soit $f\in\mathscr{I}([a,b])$. On considère $\epsilon>0$, et δ, jauge ϵ-adaptée à f.
Soit $\sigma_p=\big(([x_0,x_1],t_1),\dots([x_{n-1},x_n],t_n)$ une subdivision pointée δ-fine.
Sur tous les intervalles $[x_{k-1},x_k]$, f est intégrable (Chasles).
Puis, on note $K^+=\{k\in\mathbb{N}_n\mid(x_k-x_{k-1})f(t_k)-\int_{x_{k-1}}^{x_k}f(t)\mathrm{d}t>0\}$ et $K^-=\mathbb{N}_n\setminus K^+$.
D'après le lemme de Henstock

$$\sum_{k\in K^+}\left|\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t\right|=\sum_{k\in K^+}\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t=\left|\sum_{k\in K^+}\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t\right|\leqslant\epsilon$$

$$\sum_{k\in K^-}\left|\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t\right|=-\sum_{k\in K^-}\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t=\left|\sum_{k\in K^-}\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t\right|\leqslant\epsilon$$

Et donc

$$\sum_{k=1}^n\left|\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t\right|=\sum_{k\in K^+}\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t+\sum_{k\in K^-}\left|\int_{x_{k-1}}^{x_k}\big(f(t_k)-f(t)\big)\mathrm{d}t\right|\leqslant2\epsilon$$

Exercice

Soit $f \in \mathscr{I}([a,b])$. Soit $F : x \mapsto \int_a^x f(t)\mathrm{d}t$.

Montrer que F est continue en tout $c \in [a,b]$.

Correction

Démontré plus loin

5.2. « Contrôle » par intégration

Théorème(s) de la moyenne

Remarque - Le théorème de la mouche

M. Gissot, professeur en PC* (et anciennement en MPSI3) parle du théorème de la mouche pour dire que :

- si l'on sait qu'une mouche se déplace dans une pièce, on ne sait rien de sa vitesse
- si on contrôle la vitesse de la mouche, alors on contrôle (sur un temps relativement court) son déplacement.

Proposition - Inégalité de la moyenne

Soit f continue par morceaux sur $[a,b]$. Alors :

$$\left|\int_{[a,b]} f\right| \leqslant (b-a)\sup_{[a,b]}|f|.$$

Démonstration

$\forall\ t \in [a,b]$, $f(t) \leqslant \sup|f|$.

Ensuite on intègre (positivité) :

$$\int_{[a,b]} f \leqslant \int_{[a,b]} \sup|f|(b-a)\sup_{[a,b]}|f|.$$

De même pour $-f$. Comme $\left|\int_{[a,b]} f\right| = \max(\int_{[a,b]} f, -\int_{[a,b]} f)$, on trouve l'inégalité recherchée.

□

Définition - Valeur moyenne de f

Soit f continue par morceaux sur $[a,b]$.

Alors $\frac{1}{b-a}\int_{[a,b]} f$ s'appelle la valeur moyenne de f sur $[a,b]$.

Exercice

Montrer que si f est continue sur $[a,b]$ alors il existe $c \in [a,b]$ tel que $f(c) = \frac{1}{b-a}\int_{[a,b]} f$.

Correction

La fonction $F : x \mapsto \int_a^x f(t)\mathrm{d}t$ est de classe $\mathscr{C}^1$.

On applique le théorème des accroissements finis :

$$\exists\ c \in]a,b[\ |\ (b-a)F'(c) = F(b) - F(a)$$

Comme $F' = f$, le résultat est immédiat.

Exercice

Montrer les théorèmes suivants :

1. Soit $f : [a,b] \to \mathbb{R}$, continue et $g : [a,b] \to \mathbb{R}_+$, positive et intégrable.
   Alors il existe $c \in [a,b]$ tel que $\int_a^b f(x)g(x)\mathrm{d}x = f(c)\int_a^b g(x)\mathrm{d}x$.
2. Soit $f : [a,b] \to \mathbb{R}$, postive, de classe $\mathscr{C}^1$ et décroissante et $g : [a,b] \to \mathbb{R}_+$ continue.
   Alors il existe $c \in [a,b]$ tel que $\int_a^b f(x)g(x)\mathrm{d}x = f(a)\int_a^c g(x)\mathrm{d}x$.

Correction

Pour aller plus loin - Théorème de convergence uniforme

Les théorèmes de convergence uniforme où ceux qui en découlent (théorème des intégrales à paramètres $F(x) = \int_I f(x,t)\mathrm{d}t$ avec suffisamment de régularité pour $x \mapsto f(x,t)$) se démontrent de la même façon (en seconde année) pour l'intégrale de Riemann que pour l'intégrale de Kurzweil-Henstock.

Pour aller plus loin - Théorème de convergence dominée (convergence simple)

Les théorèmes de convergence monotone et convergence dominée énoncés en seconde année pour l'intégrale de Riemann sont identiques pour l'intégrale de Kurzweil-Henstock.

On peut ajouter même comme étape intermédiaire le théorème de convergence encadrée :

Si (f_n) est une suite de fonctions KH-intégrables sur I qui converge simplement vers une fonction $f : I \to \mathbb{R}$ telle qu'il existe g, h KH-intégables sur I avec $g \leqslant f_n \leqslant h$ sur I, pour tout $n \in \mathbb{N}$.

Alors f est KH-intégrable sur I et $\int_I f = \lim_{n\to+\infty}\int_I f_n$.

Pour aller plus loin - Règles d'or de l'analyse

La <u>première règle d'or</u> en analyse : pour contrôler une fonction (transformation, distribution…), il faut contrôler sa dérivée puis intégrer.

La <u>seconde règle d'or de l'analyse</u> (qui lui est équivalente) : si l'on veut comprendre une variable erratique, il faut en faire la moyenne (intégration…). C'est ce qui est fait avec le calcul de l'espérance d'une variable aléatoire, par exemple.

1. f est continue sur le segment $[a,b]$, donc il existe m, M tel que $f([a,b]) = [m,M]$.
   Donc $m\int_a^b g(x)\mathrm{d}x \leqslant \int_a^b f(x)g(x)\mathrm{d}x \leqslant M\int_a^b g(x)\mathrm{d}x$ (g positive).
   Par le TVI il existe $c \in [a,b]$ tel que $\int_a^b f(x)g(x)\mathrm{d}x = f(c)\int_a^b g(x)\mathrm{d}x$.
2. Soit $G : t \mapsto \int_a^t g(x)\mathrm{d}x$, primitive de g, de classe $\mathscr{C}^1$. On note $G([a,b]) = [m,M]$.
   $$\int_a^b f(x)g(x)\mathrm{d}x = [G(x)f(x)]_a^b - \int_a^b G(t)f'(t)\mathrm{d}t = G(b)f(b) - \int_a^b G(t)f'(t)\mathrm{d}t$$
   Or $mf(b) \leqslant G(b)f(b) \leqslant Mf(b)$,
   et $m(f(b)-f(a)) \geqslant \int_a^b G(t)f'(t)\mathrm{d}t \geqslant M(f(b)-f(a))$ (f décroissante, donc $f' \leqslant 0$)
   Donc
   $$mf(a) \leqslant \int_a^b f(x)g(x)\mathrm{d}x \leqslant Mf(a)$$
   On conclue avec le TVI

Positivité et continuité

Proposition - Intégrale d'une fonction positive et continue

Soit $f : [a,b] \to \mathbb{R}$ **continue, positive**.

Si f n'est pas la fonction nulle sur $[a,b]$ alors $\int_a^b f(t)\,dt > 0$.

Démonstration

f n'est pas nulle. Il existe x_0 tel que $f(x_0) > 0$.

Et par continuité en x_0, il existe $\eta > 0$ tel que $\forall\ x \in [x_0-\eta, x_0+\eta]$, $f(x) > \frac{f(x_0)}{2}$ (on prend $\epsilon = \frac{f(x_0)}{2}$).

Puis, d'après la relation de Chasles et la positivité :

$$\int_a^b f(t)\mathrm{d}t \geqslant \int_{x_0-\eta}^{x_0+\eta} f(t)\mathrm{d}t \geqslant \frac{f(x_0)}{2}\times 2\eta > 0$$

□

Exercice

Autre démonstration : On note $F : x \mapsto \int_a^x f(t)\mathrm{d}t$. Montrer que F est de classe $\mathscr{C}^1$, croissante. Conclure par contraposition.

Correction

Alors F est dérivable, de dérivée f continue, donc F est de classe $\mathscr{C}^2$ et $F' \geqslant 0$, donc F croissante.

Ainsi $F(b) \geqslant F(a)$. Si on n'a pas $F(b) > F(a)$, alors $F(b) = F(a) = 0$. Ainsi pour tout $x \in [a,b]$, $0 = F(a) \leqslant F(x) \leqslant F(b) = 0$ et donc $f(x) = F'(x) = 0$.

Le théorème suivant nous sert souvent (en particulier pour montrer que certaines formes bilinéaires sont définies) :

Corollaire - Intégrale nulle d'une fonction continue, de signe constant

Soit f **continue, de signe constant** sur $[a,b]$ telle que $\int_a^b f(t)\,dt = 0$.

Alors f est nulle sur $[a,b]$.

Démonstration

Il s'agit de la contraposée de la proposition précédente □

Attention - Toutes les hypothèses sont importantes

S'il manque l'une des deux hypothèses, le résultat est faux.

- Donner un contre-exemple pour une fonction continue, non nulle, d'intégrale nulle :
- Donner un contre-exemple pour une fonction continue par morceaux mais non continue, positive, non nulle, d'intégrale nulle.

5.3. Extension aux fonctions à valeurs complexes

Soit $f : [a,b] \to \mathbb{C}$ où $[a,b]$ est un intervalle de $\mathbb{R}$.

Définition - Continuité par morceaux
On dit que f est continue par morceaux sur $[a,b]$ s'il existe une subdivision $\sigma = (a_i)_{0\leqslant i\leqslant n}$ de $[a,b]$ telle que $\forall i \in [\![1,n]\!]$, $f_{|]a_{i-1},a_i[}$ soit continue, f admette des limites dans $\mathbb{C}$ à droite en a_{i-1}, à gauche en a_i.
Cela revient à dire que $\mathrm{Re}f$ et $\mathrm{Im}f$ sont continues par morceaux.

On se contente ici de l'intégrabilité pour des fonctions continues par morceaux :

Définition - Intégrale complexe
Si f est continue par morceaux sur $[a,b]$, on appelle intégrale de f sur $[a,b]$ le complexe

$$\int_{[a,b]} f = \int_{[a,b]} \mathrm{Re}f + i\int_{[a,b]} \mathrm{Im}f$$

et on utilise les mêmes conventions pour $\displaystyle\int_a^b f(t)\,dt$.

Mais on a mieux :

Définition - Intégrale KH complexe
On dit que $f : [a,b] \to \mathbb{C}$ est (KH)-intégrable sur $[a,b]$ si $\mathrm{Re}f$ et $\mathrm{Im}f$ sont intégrables sur $[a,b]$.
On a alors $\displaystyle\int_{[a,b]} f = \int_{[a,b]} \mathrm{Re}f + i\int_{[a,b]} \mathrm{Im}f$.

Remarque - Plusieurs définitions?
En fait, la définition :

$$\exists\, S, \text{tel que } \forall\, \epsilon > 0, \exists\, \delta \in D(f,\epsilon) \text{ telle que } \forall\, \sigma_p \in \delta - \mathfrak{S}, \quad \left|S(f,\sigma_p) - S\right| \leqslant \epsilon$$

est toujours valable, en lisant des modules au lieu de valeurs absolues.
Elle est équivalente à la définition par parties réelles et imaginaires, en se souvenant que $|z| \leqslant \mathrm{Re}(z)+\mathrm{Im}(z)$ et $|\mathrm{Re}(z)| \leqslant |z|$, $|\mathrm{Im}(z)| \leqslant |z|$, puis en exploitant $\min(\delta_1,\delta_2) - \mathfrak{S} \subset \delta_1 - \mathfrak{S} \cap \delta_2 - \mathfrak{S}$.

Théorème - Propriétés
On a les propriétés suivantes

- linéarité : $f \mapsto \displaystyle\int_a^b f(t)\mathrm{d}t$ est une forme linéaire sur $\mathscr{C}_{\mathscr{M}}([a,b],\mathbb{C})$ $(K = \mathbb{C})$
- relation de Chasles : $f \in \mathscr{C}_{\mathscr{M}}(I,\mathbb{C})$, pour tout $(a,b,c) \in I^3$,

$$\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_c^b f(t)\mathrm{d}t.$$

- module : $f \in \mathscr{C}_{\mathscr{M}}([a,b],\mathbb{C}) \Rightarrow |f| \in \mathscr{C}_{\mathscr{M}}([a,b],\mathbb{R})$ et

$$\left|\int_a^b f(t)\mathrm{d}t\right| \leqslant \int_a^b |f(t)|\mathrm{d}t$$

- sommes de Riemann : si $f : [a,b] \to \mathbb{C}$ est continue alors

$$\lim_{n\to+\infty} \frac{b-a}{n}\sum_{k=0}^{n-1} f\left(a + k\frac{b-a}{n}\right) = \int_a^b f(t)\mathrm{d}t$$

Démonstration
Elles se démontrent toutes à partir des relations pour les fonctions à valeurs réelles, en prenant partie imaginaire et partie réelle.
Démontrons, néanmoins, le résultat sur les module (autre méthode).
Il existe $\theta \in [0,2\pi[$ tel que $\displaystyle\int_a^b f(t)\mathrm{d}t = \left|\int_a^b f(t)\mathrm{d}t\right| e^{i\theta}$.
Donc

$$\left|\int_a^b f(t)\mathrm{d}t\right| = \int_a^b f(t)e^{-i\theta}\mathrm{d}t$$

Si on prend la partie réelle (ces nombres sont réels) :

$$\left|\int_a^b f(t)\mathrm{d}t\right| = \mathrm{Re}\left(\left|\int_a^b f(t)\mathrm{d}t\right|\right) = \mathrm{Re}\left(\int_a^b f(t)e^{-i\theta}\mathrm{d}t\right) = \int_a^b \mathrm{Re}\left(f(t)e^{-i\theta}\right)\mathrm{d}t$$

Enfin, comme pour tout $z \in \mathbb{C}$, $\mathrm{Re}(z) \leqslant |z|$, on a donc :

$$\left|\int_a^b f(t)\mathrm{d}t\right| \leqslant \int_a^b \left|f(t)e^{-i\theta}\right|\mathrm{d}t$$

□

5.4. Formules de Taylor

Remarque - Rappels de notation
Soit $f : I \to \mathbb{R}$ ou $\mathbb{C}$, $a \in I$. On suppose que f est n fois dérivable en a.
Le développement de Taylor à l'ordre n de f en a est l'expression :

$$T_n(x) = f(a) + f'(a)(x-a) + \cdots + f^{(n)}(a)\frac{(x-a)^n}{n!} = \sum_{k=0}^{n} \frac{(x-a)^k}{k!} f^{(k)}(a)$$

On pose $R_n(x) = f(x) - T_n(x)$. R_n est le reste de Taylor à l'ordre n de f en a.
L'idée est de considérer T_n comme une approximation polynomiale de f en a, R_n mesurant l'erreur commise.

Pour aller plus loin - Alléger les hypothèses
On peut supposer juste que f est dérivable $n+1$, la KH-intégration de $f^{(n+1)}$ existera donc…

Théorème - Formule de Taylor avec reste intégral
Soient f une application de I dans $\mathbb{R}$ (ou $\mathbb{C}$) de classe C^{n+1}, $a,b \in I$. Alors

$$f(b) = f(a) + \sum_{k=1}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\mathrm{d}t.$$

Ou de même $\displaystyle R_n(b) = \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\mathrm{d}t$.

Démonstration
On peut faire une récurrence. Ou mieux, comme Lagrange, changer de variable.
On considère : $\phi : t \mapsto f(b) - f(t) - \displaystyle\sum_{k=1}^{n} \frac{(b-t)^k}{k!} f^{(k)}(t)$.
Elle est de classe $\mathscr{C}^1$ sur I et pour tout $t \in I$,

$$\phi'(t) = -f'(t) + \sum_{k=1}^{n} \frac{(b-t)^{k-1}}{(k-1)!} f^{(k)}(t) - \sum_{k=1}^{n} \frac{(b-t)^k}{k!} f^{(k+1)}(t) = -\frac{(b-t)^k}{k!} f^{(k+1)}(t)$$

On a donc

$$0 - f(b) + f(a) + \sum_{k=1}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) = \phi(b) - \phi(a) = \int_a^b \phi'(t)\mathrm{d}t = -\int_a^b \frac{(b-t)^k}{k!} f^{(k+1)}(t)\mathrm{d}t$$

□

Théorème - Inégalité de Taylor-Lagrange
Soient f une application de I dans $\mathbb{R}$ (ou $\mathbb{C}$) de classe C^{n+1}, $a,b \in I$. Alors

$$|f(b) - f(a) - \sum_{k=1}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a)| \leqslant \frac{|b-a|^{n+1}}{(n+1)!} \sup_{t\in[a,b]} |f^{(n+1)}(t)|$$

Ou de même $|R_n(b)| \leqslant \frac{|b-a|^{n+1}}{(n+1)!} \sup_{t\in[a,b]} |f^{(n+1)}(t)|$.

Si $b<a$ il faut remplacer $[a,b]$ par $[b,a]$.

Démonstration
Il suffit d'utiliser l'inégalité de l'intégration puis de majorer $f^{(n+1)}$, continue sur $[a,b]$,

$$\left|f(b)-f(a)-\sum_{k=1}^{n}\frac{(b-a)^k}{k!}f^{(k)}(a)\right|\leqslant\int_a^b\left|\frac{(b-t)^n}{n!}f^{(n+1)}(t)\right|\mathrm{d}t\leqslant\sup_{t\in[a,b]}|f^{(n+1)}(t)|\times\int_a^b\frac{(b-t)^k}{k!}$$

$$\left|f(b)-f(a)-\sum_{k=1}^{n}\frac{(b-a)^k}{k!}f^{(k)}(a)\right|\leqslant=\frac{|b-a|^{n+1}}{(n+1)!}\sup_{t\in[a,b]}|f^{(n+1)}(t)|$$

Le résultat reste vraie si $b<a$… □

La formule suivante découle des précédente (et avait déjà été rencontrée)

Théorème - Formule de Taylor-Young
Soient I un intervalle de $\mathbb{R}$, f une application de I dans $\mathbb{R}$ (ou dans $\mathbb{C}$), n fois dérivable en $a\in I$. Alors pour tout $x\in I$ on a

$$f(x)=\sum_{k=0}^{n}\frac{(x-a)^k}{k!}f^{(k)}(a)+(x-a)^n\epsilon(x)\text{ avec }\lim_{x\to a}\epsilon(x)=0.$$

Ou de même $R_n(x)=o((x-a)^n)$.

Savoir faire - Utilisation des différentes formules (de Taylor)
- L'inégalité de Taylor-Lagrange donne un résultat global (sur tout l'intervalle I) et permet de majorer $|R_n|$.
- La formule de Taylor avec reste intégral donne également un résultat global, c'est de plus une expression exacte que l'on utilise lorsque la majoration du reste n'est pas suffisante, par exemple si on veut en étudier le signe.
- La formule de Taylor-Young donne uniquement un résultat local, elle sert donc à préciser la fonction f au voisinage de a.

On fait la démonstration grâce à l'exercice suivant :
Exercice
Taylor-Young avec les hypothèses les plus générales :
Soit $n\in\mathbb{N}^*$. Soit f une fonction de I dans $\mathbb{R}$, où I intervalle de $\mathbb{R}$, $a\in I$ tels que f soit $n-1$ fois dérivable sur I et admette une dérivée n-ième en a. On veut montrer qu'il existe une fonction $\epsilon: I\to\mathbb{R}$ telle que

$$\forall x\in I,\ f(x)=\sum_{k=0}^{n}\frac{(x-a)^k}{k!}f^{(k)}(a)+\frac{(x-a)^n}{n!}\epsilon(x)\text{ avec }\lim_{x\to a}\epsilon(x)=0$$

1. On suppose f réelle.
   On considère ϵ définie par : $\epsilon(a)=0$ et pour $x\neq a$,
   $$\epsilon(x)=\frac{n!}{(x-a)^n}\left(f(x)-\sum_{k=0}^{n}\frac{(x-a)^k}{k!}f^{(k)}(a)\right)$$
   On fixe un réel $x\neq a$ et $A(x)=f^{(n)}(a)+\epsilon(x)$.
   Et enfin on considère la fonction ϕ définie sur I par
   $$\phi(t)=f(t)-\sum_{k=0}^{n-1}\frac{(t-a)^k}{k!}f^{(k)}(a)-\frac{(t-a)^n}{n!}A(x).$$
   Calculer $\phi^{(k)}(a)$, pour tout $k\leqslant n-2$.
2. Montrer que pour tout $i\leqslant n-1$, il existe $x_i\in]a,x[$ tel que $\phi^{(i)}(x_i)=0$.
3. En déduire la limite de $A(x)$ pour $x\to a$, puis celle de $\epsilon(x)$.
4. Faire le cas d'une fonction complexe.

Correction

1. On a pour $i\leqslant n-1$,
   $$\phi^{(i)}(t)=f^{(i)}(t)-\sum_{k=i}^{n-1}\frac{(t-a)^{k-i}}{(k-i)!}f^{(k)}(a)-\frac{(t-a)^{n-i}}{(n-i)!}A(x)$$
   On a $\phi(a)=\phi'(a)=\ldots=\phi^{(n-2)}(a)=0$.
2. On a $\phi(a)=0=\phi(x)$, ϕ est continue sur $[a,x]$ (si $x>a$, sinon sur $[x,a]$), dérivable sur $]a,x[$, donc il existe $x_1\in]a,x[$ tel que $\phi'(x_1)=0$.
   Une nouvelle application du théorème de Rolle permet d'obtenir $x_2\in]a,x_1[$ tel que $\phi''(x_2)=0$, et ainsi, tant que la fonction $f^{(i)}$ est encore dérivable, on obtient $x_i\in]a,x_{i-1}[$ tel que $\phi^{(i+1)}(x_{i+1})=0$.
   Et donc il existe $x_{n-1}\in]a,x[$ tel que $\phi^{(n-1)}(x_{n-1})=0$.
   On a alors $0=f^{(n-1)}(x_{n-1})-f^{(n-1)}(a)-(x_{n-1}-a)A(x)$.
3. $A(x)=\dfrac{f^{(n-1)}(x_{n-1})-f^{(n-1)}(a)}{x_{n-1}-a}$ qui tend vers $f^{(n)}(a)$ quand x tend vers a car $f^{(n-1)}$ est dérivable en a, $x_{n-1}\in]a,x[$ tend vers a quand x tend vers a, d'où $\epsilon(x)$ tend vers 0 quand x tend vers a.
4. Pour une fonction à valeurs complexes, on sépare partie réelle et partie imaginaire.

6. Bilan

Synthèse

⇝ Avant même de définir précisément ce qu'est une fonction (prémices : Euler), les mathématiciens savaient ce qu'était en gros une intégrale (avec la notion d'aire). Puis au fur et à mesure des besoins la définitions s'est élargie, précisée. Ainsi Riemann complète la construction de Cauchy au milieu du XIXe siècle afin de rendre cohérent la théorie de Fourier. Cette construction de Riemann est satisfaisante en MPSI elle permet de montrer que toute fonction continue sur un intervalle bornée admet une primitive. Mais la quête, par les mathématiciens, d'une définition robuste ne s'arrête pas là. Ainsi Lebesgue (début du XXe) propose une définition plus large encore puisqu'elle permet de dire que l'espace des fonctions intégrables est complet, mais en revanche, elle gère mal la notion d'intégrale impropre. Denjoy, Perron, indépendamment proposent une nouvelle construction, reprise et mieux présentée par Kurzweil et Henstock (1950), où apparait concrètement une définition qui généralise l'intégrale de Riemann : la constante δ (pour Riemann) devient une jauge (fonction positive) qui s'adapte à l'intégrant. C'est pourquoi, on parle aussi d'intégrale de jauge. Le lemme d'Henstock prouve comment la jauge s'adapte parfaitement à la fonction f.

⇝ Les fonctions en escalier sont intégrales, et la valeur de leur intégrale est aisément calculable. Si une fonction est comprise uniformément entre deux fonctions intégrables, alors elle est intégrables. Or les fonctions continues (par morceaux) sont enfermables uniformément sur un segment entre deux fonctions en escalier. Les fonctions continues (par morceaux) sur un segment sont donc toutes intégrables.
Puis si on définit, *pour f continue*, les primitives F de f, on trouve alors $\int_a^b f(t)\mathrm{d}t=F(b)-F(a)$.
Mais on fait mieux, à condition de prendre l'intégrale de KH : toute fonction dérivable F (avec F' non nécessairement continue) on a $\int_a^b F'(t)\mathrm{d}t=F(b)-F(a)$. Le calcul de l'intégrale est donc, à 99% du temps, réduit à un calcul de primitive (i.e. trouver la fonction dont la

dérivée est…). Les techniques du début d'année doivent être maitrisées : tableau à connaître par coeur, linéarité, intégration par parties, changement de variables (Règle de Bioche…). On se sert aussi de la positivité et croissance de l'intégrale, et de la règle de Chasles

⇝ Souvent la pratique est à contre-sens de la construction théorique, ainsi des sommes de Riemann. Elles sont théoriquement créées pour calculer des intégrales ; mais dans la pratique, on exploite le calcul d'intégrale (point précédent) pour évaluer la somme de Riemann, rencontrée comme problème. De même de l'extension complexe : on étudie parties réelles et imaginaires séparément pour intégrer la foncion. Ou encore la formule de Taylor : elle permet par du maitrise de calcul intégrale de mieux connaitre une fonction f. Et enfin la comparaison série-intégrale : on maîtrise le calcul intégrale, c'est lui qui permet d'encadrer des calculs sur les séries (er non l'inverse).

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Méthode 1 : primitives
- Savoir-faire - Méthode 2 : Fractions rationnelles
- Savoir-faire - Méthode 3 : Intégration par parties
- Savoir-faire - Méthode 4 : Changement de variables
- Truc & Astuce pour le calcul - Reconnaitre des sommes de Riemann à pas constant : limite
- Truc & Astuce pour le calcul - Reconnaitre des sommes de Riemann à pas constant : vitesse de convergence
- Savoir-faire - A chaque problème sa jauge
- Savoir-faire - Trouver la jauge pour une fonction f admettant une primitive F
- Savoir-faire - Etudier $x \mapsto \int_{h_1(x)}^{h_2(x)} f(t)\mathrm{d}t$
- Savoir-faire - Utilisation des différentes formules (de Taylor)

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\sigma_p = ((\lbrack x_{k-1}, x_k\rbrack, t_k), k \in \lbrack\!\lbrack 1, n\rbrack\!\rbrack)$	Subdivision pointée de $[x_0, x_n]$	$x_0 < x_1 < \cdots < x_{n-1} < x_n$ et $\forall\, k \in \mathbb{N}_n$, $t_k \in [x_{k-1}, x_k]$	t_k est le point de marquage de $[x_{k-1}, x_k]$.
σ_p est δ-fine	(ou adaptée à la jauge $\delta : [a,b] \to \mathbb{R}_+^*$) $[x_{k-1}, x_k] \subset [t_k - \frac{\delta(t_k)}{2}, t_k + \frac{\delta(t_k)}{2}]$	$\forall\, k \in \mathbb{N}_n$, $0 \leqslant x_k - x_{k-1} \leqslant \delta(t_k)$	si δ constante, on la note δ^*
$s_p = ((\lbrack x_{i-1}, x_i\rbrack, t_i), i \in I)$	Sous-subdivision (pointée) de σ_p. ($I \subset \mathbb{N}_n$)	Exploitée pour le lemme de Henstock	I : appui de s_p et $\mathscr{D}(s_p) = \bigcup_{i\in I} [x_{i-1}, x_i]$: domaine de s_p.
$S(f, \sigma_p)$	Somme de Cauchy/Riemann de f pour la subdivision pointée σ_p	$S(f,\sigma_p) = \sum_{k=1}^{n} f(t_k)(x_{k+1} - x_k)$	Cas particuliers : $R_n(f) = \frac{b-a}{n}\sum_{k=0}^{n-1} f(a + \frac{k}{n}(b-a))$, $S_n(f) = \frac{b-a}{n}\sum_{k=1}^{1} f(a + \frac{k}{n}(b-a))$
$\lim_{\delta(\sigma_p)\to 0} S(f,\sigma_p) = I$	f est KH-intégrable d'intégrale égale à I	$\forall\, \epsilon > 0$, $\exists\, \delta : [a,b] > 0$ tq $\forall\, \sigma_p$ δ-fine, $\lvert S(f,\sigma_p) - I\rvert \leqslant \epsilon$	Si δ constant (δ^*) on parle de R-intégrale.
$(\varphi_n) \overset{c.s.}{\to} f$	(φ_n) converge simplement vers f	$\forall\, \epsilon > 0$, $\forall\, x \in I$, $\exists\, N \in \mathbb{N}$ tel que $\forall\, n \geqslant N$, $\lvert f(x) - \varphi_n(x)\rvert \leqslant \epsilon$	Ou encore : $\forall\, x \in I$, $(\varphi_n)(x) \to f(x)$
$(\varphi_n) \overset{c.u.}{\to} f$	(φ_n) converge uniformément vers f	$\forall\, \epsilon > 0$, $\exists\, N \in \mathbb{N}$ tel que $\forall\, x \in I$, $\forall\, n \geqslant N$, $\lvert f(x) - \varphi_n(x)\rvert \leqslant \epsilon$	Si $(\varphi_n) \overset{c.u.}{\to} f$ alors $(\varphi_n) \overset{c.s.}{\to} f$
$\mathscr{E}([a,b])$, $\mathscr{C}_{\mathscr{M}}([a,b])$, $\mathscr{B}([a,b])$	Respectivement algèbre des fonctions en escalier, continues par morceaux, bornées sur le segment $[a,b]$	$\mathscr{E}([a,b]) \subset \mathscr{C}_{\mathscr{M}}([a,b]) \subset \mathscr{B}([a,b]$	.
$\mathscr{I}_{\mathscr{R}}([a,b])$, $\mathscr{I}([a,b])$	Respectivement espace vectoriel des fonctions Riemann-intégrable, Kurzweil-Henstock-intégrable sur le segment $[a,b]$	$\mathscr{I}_{\mathscr{R}}([a,b]) \subset \mathscr{I}([a,b])$	

Retour sur les problèmes

128. Cours
129. Cours
130. C'est un gros ensemble, complet par ailleurs à condition d'élargir la continuité à la continuité presque partout…
131. La partie 6. du cours, hors-programme tente de répondre à cette question
132. Pas de question. L'inégalité de la moyenne (quitte à la couper en morceaux) donne un résultat d'encadrement intégral! C'est souvent lui qu'on retrouve à l'origine des résultats d'encadrement ou des calculs de limite en analyse.

Chapitre 38

Séries numériques

Résumé -

Dans ce chapitre nous étudions (rapidement) un objet central en mathématiques : les séries numériques. Cela la présentation faite ici, elle dérive des suites numériques, mais en réalité c'est bien l'inverse qui lie ces deux objets : les suites dérivent (de plusieurs façons) des séries.

Nous étudierons la notion première de convergence de série et mettrons en place les premières notations.

Ensuite nous nous concentrons sur les séries à termes positifs. Plusieurs raisons : étudier leur convergence est relativement simple (et il existe des moyens d'étude simplifié dans ce cas là). Certains peuvent même écrire qu'elles convergent toutes (à condition d'accepter $+\infty$ comme limite). Une dernière raison est l'usage de la convergence absolue comme critère suffisant (mais non nécessaire) pour montrer la convergence de la série. Lorsqu'on cherche à montrer la convergence absolue, on considère des séries positives.

Muni de ces outils, nous prouverons tranquillement la convergence du développement décimal d'un nombre.

Enfin, au passage nous rencontrons quelques familles de séries à maîtriser : les séries de Riemann, les séries géométriques et dans une moindre mesure : les séries exponentielles et les séries binomiales négatives.

Sommaire

1. Problèmes 782
2. Généralités 783
2.1. Définitions 783
2.2. Propriétés 784
2.3. Telescopage 785
2.4. Opérations pour des séries convergentes 787
2.5. Un cas classique : les séries de signe alterné 787
3. Séries à termes positifs 789
3.1. Majoration des sommes partielles 789
3.2. Comparaison des séries à termes positifs 790
3.3. Exploitation des séries de Riemann 791
3.4. Séries absolument convergentes 792
4. Quelques méthodes d'étude 793
4.1. Plan d'étude 793
4.2. Comparaison série-intégrale 793
4.3. Séries de référence 794
5. Bilan 797

1. Problèmes

Problème 166 - Convergence décimale

Rappelons-nous qu'historiquement une famille importante de suites a été celle des approximations décimales de nombres réelles. Par exemple : $(3-3,1-3,14-3,141-3,1415\ldots)$ qui converge vers π.

Elles sont de la forme : u_{n+1} possède toujours les mêmes premiers termes que u_n avec une décimale supplémentaire. On a donc naturellement une relation de la forme : $u_{n+1} = u_n + d_{n+1} \times 10^{-(n+1)}$ où d_n est la $n+1^{\text{e}}$ décimale de ℓ, la limite envisagée.

On a alors : $u_n = u_{n-1} + d_n 10^{-n} = u_{n-2} + d_{n-1}10^{-n+1} + d_n 10^n = \cdots = u_0 + \sum_{k=0}^{n} d_k 10^{-k}$.

Pour l'étude de ce type de suites, il est nécessaire de s'intéresser aux suites : $\left(\sum_{k=0}^{n} d'_k\right)_{n\in\mathbb{N}}$ …

Convergent-elles nécessairement (dans $\mathbb{R}$) ? Toutes ? Y a-t-il une bijection entre $\mathbb{R}$ et $\mathbb{D}^{\mathbb{N}}$?

Problème 167 - Etudier une suite définie par récurrence

Considérons une suite définie par récurrence à partir de deux suites données (v_n) et (w_n) :

$\forall\, n \in \mathbb{N}$, $u_{n+1} = v_n \times u_n + w_n$.

Notons alors, pour $n \geqslant 1$: $a_n = \dfrac{u_n}{\prod_{k=0}^{n-1} v_k}$.

Alors $a_{n+1} = \dfrac{u_{n+1}}{\prod_{k=0}^{n} v_k} = \dfrac{u_n}{\prod_{k=0}^{n-1} v_k} + \dfrac{w_n}{\prod_{k=0}^{n} v_k}$.

Et donc, par télescopage : $a_n - a_1 = \sum_{k=1}^{n-1} (a_{k+1} - a_k) = \sum_{k=1}^{n-1} \dfrac{w_k}{\prod_{h=0}^{k} v_h}$.

Ainsi u_n, peut s'exprimer explicitement : $u_n = \prod_{k=0}^{n-1} v_k \times \sum_{k=1}^{n-1} \dfrac{w_k}{\prod_{h=0}^{k} v_h} + \dfrac{u_1}{v_0}$.

Il faut pour cela savoir calculer des sommes ou produit (et montrer la convergence de ces sommes et produit).

Comme $\ln(\prod_{h=0}^{k} v_h) = \sum_{h=0}^{k} \ln v_h$, on peut se contenter d'étudier les sommes…

Comment montrer la convergence d'une suite de somme (série) définie par son terme général?

Problème 168 - Reconnaissance de la convergence

On donne une expression explicite de a_n.

Est-il possible de déterminer directement si la série (suite de sommes partielles) $\sum_{n\geqslant 0} a_n$ converge, par un algorithme de décision ?

Est-il possible de calculer directement la limite de la série (suite de sommes partielles) $\sum_{n\geqslant 0} a_n$ si elle converge ?

Problème 169 - Comparaison série/intégrale et transformation d'Abel

On l'a déjà dit : pour connaître la variation (instantanée) d'une suite, on calcule « sa dérivée » : $u'_n = u_n - u_{n-1}$. Son signe indique bien si (u_n) est (localement) croissante ou décroissante.
Dans ces cas-là, on trouve que l'opération réciproque de la dérivation est *exactement* le passage à la suite de sommes partielles :

$$U_n = \sum_{k=0}^{n} u_k + C \iff u_n = U'_n$$

Pouvons-nous transférer toutes les propriétés vues dans les cours sur la dérivation et l'intégration de fonctions aux séries ? En particulier, que devient l'intégration par parties ?
On parle de transformation d'Abel et on l'exploiter exactement au moment où l'on ferait une intégration par parties si le problème posé concernait des fonctions…

2. Généralités

2.1. Définitions

Définition - Séries
Soit $(u_n)_{n\geqslant n_0}$ une suite de nombres réels ou complexes. On pose $S_n = \sum_{k=n_0}^{n} u_k$.
On appelle **série de terme général** u_n la suite $(S_n)_{n\geqslant n_0}$.
On note $\sum u_n$ (ou $\sum_{n\geqslant n_0} u_n$) la série de terme général u_n, à la place de (S_n).
Le nombre S_n s'appelle la **somme partielle** d'ordre n ou n-ième somme partielle.

Remarque - Une série est une suite…
Une série n'est qu'une suite d'un genre bien particulier.
Très couramment, $n_0 = 0$ ou $n_0 = 1$.

Définition - Convergence, limite
• La série $\sum u_n$ est dite **convergente** si la suite (S_n) est convergente.
Dans le cas contraire on dit que $\sum u_n$ est **divergente**.
• Si la série est convergente,

$$S = \lim_{n\to+\infty} S_n = \lim_{n\to+\infty} \sum_{k=n_0}^{n} u_k$$

est appelée **somme de la série** et est notée $\sum_{n=n_0}^{+\infty} u_n$.

Attention - Écriture (1)
Que signifie chacune des trois notations suivantes :

$$1.\ \sum_{n\geqslant 0} u_n \text{ ou } \sum u_n \qquad 2.\ \sum_{n=0}^{+\infty} u_n \qquad 3.\ \sum_{n=0}^{N} u_n$$

1. C'est la série ! (notion mathématique que l'on étudie) *cf. la suite* (a_n)
2. C'est un nombre : la limite de la série ! *cf. la limite* ℓ

Histoire - Nicolas Oresme
Les mathématiciens européens se sont intéressés très tôt à l'étude des séries.



Par exemple, Nicole Oresme (ou Nicolas Oresme), a montré la divergence de la série harmonique. Il est né à Fleury-sur-Orne vers 1320-1322 et mort à Lisieux le 11 juillet 1382, est un philosophe, astronome, mathématicien, économiste, musicologue, physicien, traducteur et théologien français de l'époque médiévale.

Histoire - Mais l'histoire continue
Autour des séries, on retrouve tous les grands mathématiciens. Dans l'ordre chronologique : Fermat, Newton, Taylor, Euler, Lagrange, Abel, Poincaré, Borel… Tous ont apporté leur pierre à l'ouvrage général !

3. C'est un nombre (à nouveau) : la somme partielle *cf. le nombre* a_n

Définition - Suite des restes
$R_n = S - S_n = \sum_{k=n+1}^{+\infty} u_k$ est appelé **reste** d'ordre n de la série.
On a donc nécessairement $\lim_{n\to+\infty} R_n = 0$.

Attention - Écriture (2)
Maintenant au lieu d'écrire $\sum_{k=0}^{\infty} u_k - \sum_{k=0}^{n} u_k$, nous écrirons R_n ou $\sum_{k=n+1}^{+\infty} u_k$.
Cette dernière écriture semble naturelle, et pourtant elle ne peut exister que si la série converge (*pourquoi ?*).
D'ailleurs si l'on veut calculer le reste R_n d'une série convergente, nous devons nécessairement connaître la limite de la série $\sum_{k=0}^{\infty} u_k$.

Le reste n'existe que si on a montré que la limite existe… On peut arranger le coup en exploitant le critère de Cauchy.

Pour aller plus loin - Critère de Cauchy et…
Il arrive qu'on exploiter ce critère, avec une transformation d'Abel en particulier.

Savoir faire - Critère de Cauchy pour les séries
On peut exploiter les équivalences : (S_n) converge si et seulement si (S_n) vérifie le critère de Cauchy
si et seulement si $\forall\, \epsilon > 0, \exists\, N \in \mathbb{N}$ tel que $\forall\, p > q \geqslant N, \left|S_p - S_q\right| \leqslant \epsilon$.
si et seulement si $\forall\, \epsilon > 0, \exists\, N \in \mathbb{N}$ tel que $\forall\, p \leqslant q \geqslant N, \left|\sum_{n=q}^{p} u_n\right| \leqslant \epsilon$.

Définition - Série de même nature
Deux séries sont dites de **même nature** si elles sont toutes deux convergentes ou toutes deux divergentes.

Exemple - La convergence est indépendance des premiers termes
Deux séries $\sum u_n$ et $\sum v_n$ telles qu'à partir d'un certain rang $u_n = v_n$ sont de même nature, mais, en cas de convergence, les sommes peuvent être différentes.

2.2. Propriétés

Proposition - Condition nécessaire pour la convergence
Si la série de terme général u_n converge alors $\lim_{n\to+\infty} u_n = 0$ (la réciproque est fausse !).
Si le terme général ne tend pas vers 0, on dit que la série diverge grossièrement.

Démonstration
Si (S_n) converge vers S, il en est de même de la suite extraite (S_{n-1}).
Alors par addition (soustraction) : $S_n - S_{n-1} = u_n$ converge vers $S - S = 0$ □

Attention - GROSSE ERREUR

La réciproque est absolument fausse. *Comment s'exprime-t-elle?*
L'exercice suivant donne l'exemple d'une série divergente mais dont le terme général tend néanmoins vers 0.
C'est un exemple à connaître par coeur et à mobiliser rapidement en cas de doute.

Exercice

On note pour $k \geqslant 1$, $H_n = \sum_{k=1}^{n} \frac{1}{k}$ la somme partielle de la **série harmonique**.

1. Quelle est la limite de $\left(\frac{1}{n}\right)$?
2. Montrer que pour tout $n \in \mathbb{N}$, $H_{2^n-1} \geqslant \frac{n+1}{2}$
3. Conclure que la série diverge.

(On verra une autre méthode plus loin, et sûrement une autre encore...

Correction

1. Le terme général $\left(\frac{1}{n}\right)$ de la série harmonique converge vers 0.
2. On va faire une sorte de récurrence. Etudions d'abord l'hérédité.

$$H_{2^{n+1}-1} = \sum_{k=1}^{2^{n+1}-1} \frac{1}{k} = H_{2^n-1} + \sum_{k=2^n}^{2^{n+1}-1} \frac{1}{k} \geqslant H_{2^n-1} + \frac{2^{n+1}-1-2^n+1}{2^{n+1}-1}$$

$$H_{2^{n+1}-1} \geqslant H_{2^n-1} + \frac{(2-1)2^n}{2^{n+1}} = H_{2^n-1} + \frac{1}{2}$$

Donc, pour tout $n \geqslant 1$,

$$H_{2^n-1} - H_1 = \sum_{i=1}^{n-1} \left(H_{2^{i+1}-1} - H_{2^i-1}\right) \geqslant \sum_{i=1}^{n-1} \frac{1}{2} = \frac{n-1}{2}$$

Donc comme $H_1 = 1$, on a bien le résultat attendu.

3. La suite extraite (H_{2^n-1}) diverge donc la suite (H_n) ne peut pas converger.

2.3. Telescopage

Heuristique - Processus d'intégration

Lorsque l'on souhaite étudier les *variations* d'une fonction, on calcul le *signe* de la dérivée de f.
Lorsque l'on souhaite étudier les *variations* d'une suite, on calcul le *signe* de la suite (v_n) définie par $v_n := u_{n+1} - u_n$.
Si l'on considère qu'il y a d'une certaine façon une équivalence entre la dérivation d'une fonction et la dérivation $(u_n) \mapsto (v_n)$ d'une suite, on peut se demander à quoi correspond la processus inverse de la dérivation, c'est-à-dire l'intégration pour les suites.
Autrement écrit si (v_n) est obtenue en posant pour tout entier n, $v_n = u_{n+1} - u_n$, comment faire pour obtenir (u_n) si seule la suite (v_n) est connue?
C'est très simple : $u_n = \sum_{k=0}^{n} v_k + u_0 \left(= \sum_{k=0}^{n} (u_{k+1} - u_k) + u_0\right)$ (*remarquons que l'on obtient une formule à une constante prés comme pour le calcul intégral*)

L'exercice suivant donne une première application.

Exercice

Considérons la suite (u_n) définie par récurrence par :

$$u_0 = 1 \qquad \forall\, n \in \mathbb{N} \qquad u_{n+1} = \frac{1}{3}u_n + 2^n$$

(Cas plus générale que les suites arithmético-géométriques).
Cette suite est-elle convergente, quelle est sa limite, peut-on l'exprimer explicitement ? Pour répondre, considérons $v_n = 3^n u_n$.

1. Exprimer v_{n+1} en fonction de v_n.
2. En utilisant la méthode du télescopage, montrer que v_n peut s'exprimer comme une somme.
3. En déduire une expression de u_n, ainsi qu'un équivalent de (u_n).

Correction

On a $v_0 = 3^0 \times 1 = 1$

1. Soit $n \in \mathbb{N}$, $v_{n+1} = 3^{n+1}u_{n+1} = 3^{n+1}(\frac{1}{3}u_n + 2^n) = 3^n u_n + 3 \times 6^n$.
   Et donc $v_{n+1} = v_n + 3 \times 6^n$
2. On a donc $v_{n+1} - v_n = 3 \times 6^n$.
   Ainsi, avec le télescopage : $v_n - v_0 = \sum_{k=0}^{n-1} (v_{k+1} - v_k) = 3\sum_{k=0}^{n-1} 6^k$.
3. On reconnaît la somme d'une suite géométrique, on connaît la valeur de sa somme : $3\sum_{k=0}^{n-1} 6^k = 3 \times \frac{1-6^n}{1-6}$.
   Donc $v_n = v_0 + 3 \times \frac{6^n-1}{5} = 1 + 3 \times \frac{6^n-1}{5} = \frac{5-3+3\times 6^n}{5}$.
   Et par conséquent : $u_n = \frac{1}{3^n} \times \frac{2+3\times 6^n}{5} = \frac{2+3\times 6^n}{5\times 3^n}$.
   Et donc $u_n \sim \frac{3}{5} \times 2^n$

Analyse - L'important ici

Nous avons transformé (u_n) en (v_n) de manière à obtenir une relation de la forme directe $v_{n+1} = v_n + b_n$.
Dans ce cas, nous connaissons les variations de (v_n).
Comment faire pour obtenir (v_n) si l'on connaît ses variations. Il faut employer la méthode réciproque de la dérivation, c'est à dire l'intégration. Ici il s'agit de SOMMER les termes de la suite (b_n).

Proposition - Lien suite-série

La **série** $\sum(u_{n+1} - u_n)$ et la **suite** (u_n) sont de même nature.

Exercice

Dans les cas suivants, déterminer la nature de la série $\sum_{n\geqslant 1} u_n$ et, lorsqu'il y a convergence, calculer la somme de la série.

1. $u_n = \left(1 + \frac{1}{n}\right)^n - 1$;
2. $u_n = \sqrt{n} - \sqrt{n-1}$;
3. $u_n = \frac{1}{\sqrt{n+1}} - \frac{1}{\sqrt{n}}$;
4. $u_n = \frac{1}{n(n+1)}$;
5. $u_n = \ln\left(1 + \frac{1}{n}\right)$.

Correction

1. $\lim(u_n) = e^1$, donc la série diverge grossièrement
2. La série a la même nature que la suite $(\sqrt{(n)})$: elles divergent.
3. La série a la même nature que la suite $(\frac{1}{\sqrt{(n)}})$: elles convergent.
   Pour calculer la limite, on calcule la somme partielle :

$$S_n = \sum_{k=1}^{n} \left(\frac{1}{\sqrt{k+1}} - \frac{1}{\sqrt{k}}\right) = \frac{1}{\sqrt{n+1}} - \frac{1}{\sqrt{1}} \longrightarrow -1$$

4. Notons que $u_n = \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$.
   La série a la même nature que la suite $(\frac{1}{n})$: elles convergent.
   Pour calculer la limite, on calcule la somme partielle :

$$S_n = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) = 1 - \frac{1}{n+1} \longrightarrow 1$$

5. Notons que $u_n = \ln\left(1 + \frac{1}{n}\right) = \ln\frac{n+1}{n} = \ln(n+1) - \ln n$.
   La série a la même nature que la suite $(\ln(n))$: elles divergent.

Proposition - Séries géométriques
Soit $q \in \mathbb{C}$. La série de terme général q^n, $\sum q^n$, appelée série géométrique de raison q, converge si et seulement $|q| < 1$. On a alors

$$\sum_{n=0}^{+\infty} q^n = \frac{1}{1-q}.$$

Démonstration
Si $q \neq 1$:

$$q^n = \frac{1}{q-1}(q^{n+1} - q^n)$$

Donc la série $\sum_{n\geqslant 0} q^n$ a le même comportement que la suite $(\frac{1}{q-1}q^n)_n$: elle converge ssi $|q| < 1$.
Dans ce cas :

$$\sum_{k=0}^{n} q^k = \frac{1}{q-1}(q^{n+1}-1) = \frac{1}{1-q}(1-q^{n+1}) \longmapsto \frac{1}{1-q}$$

Dans le cas $q = 1$:

$$\sum_{k=0}^{n} q^k = \sum_{k=0}^{n} 1^k = (n+1) \longmapsto +\infty$$

□

2.4. Opérations pour des séries convergentes

Proposition - Opérations sur les séries
Soient deux séries $\sum u_n$ et $\sum v_n$ et λ un réel **non nul**. Alors :
• $\sum u_n$ et $\sum \lambda u_n$ sont de même nature
et en cas de convergence $\sum_{n=n_0}^{+\infty} (\lambda u_n) = \lambda \sum_{n=n_0}^{+\infty} u_n$.
• Si $\sum u_n$ et $\sum v_n$ convergent alors $\sum(u_n + v_n)$ converge
et $\sum_{n=n_0}^{+\infty}(u_n+v_n) = \sum_{n=n_0}^{+\infty} u_n + \sum_{n=n_0}^{+\infty} v_n$.
• Si l'une des deux séries $\sum u_n$ et $\sum v_n$ converge et l'autre diverge alors $\sum(u_n+v_n)$ diverge.
• Si $\sum u_n$ et $\sum v_n$ divergent, on ne peut rien conclure quant à la nature de $\sum(u_n+v_n)$.

Démonstration
Il s'agit d'appliquer les théorèmes sur les limites de suites. □

Pour aller plus loin - Produit
Que dire de $\sum u_n \times \sum v_n$? Est-ce que cela existe, est-ce que la limite est alors égale à $\sum u_n v_n$? Non
Il s'agit d'un produit de Cauchy dont on parlera en fin de chapitre.

Proposition - Séries complexes
Soit $\sum u_n$ une série à termes complexes.
Alors $\sum u_n$ converge si et seulement si les séries $\sum \mathrm{Re}\, u_n$ et $\sum \mathrm{Im}\, u_n$ convergent
et on a alors :

$$\sum_{n=0}^{+\infty} u_n = \sum_{n=0}^{+\infty} \mathrm{Re}\, u_n + i \sum_{n=0}^{+\infty} \mathrm{Im}\, u_n.$$

Démonstration
Pour tout entier n, la somme étant finie :

$$S_n = \sum_{k=0}^{n} u_k = \sum_{k=0}^{n} \mathrm{Re}\, u_k + i \sum_{k=0}^{n} \mathrm{Im}\, u_k = \mathrm{Re}(S_n) + i\mathrm{Im}(S_n)$$

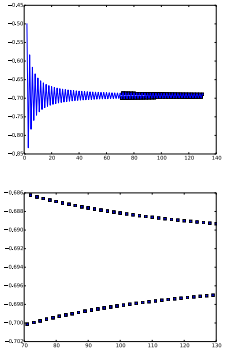
Le résultat équivalent sur les suites numériques permet alors de conclure □

2.5. Un cas classique : les séries de signe alterné

Heuristique - Convergence par « adjacence »
On se trouve dans le cas où $u_n = (-1)^n v_n$ avec pour tout $n \in \mathbb{N}$, $v_n > 0$.
Dans ce cas là, la somme partielle S_n augmente, diminue, augment, diminue…
On peut espérer que cette suite de somme partielle converge, parce que ces suites extraites paires et impaires sont adjacentes.

Définition - Série alternée
On dit que la série $\sum(-1)^n u_n$ est alternée si
— pour tout $n \in \mathbb{N}$, $u_n > 0$ *ce qui fait que la série est de signe alterné*
— la suite (u_n) est décroissante.
— $\lim(u_n) = 0$

Représentation - Visualisation
Ce qui donne les représentations graphiques suivantes :



Exemple - Série harmonique alternée
La série suivante $\sum_{n\geqslant 1} \frac{(-1)^n}{n}$ est appelé série harmonique alternée.
C'est bien une série alternée d'après la définition précédente :
— Ici $u_n = \frac{1}{n} > 0$
— u_n est décroissante
— u_n tend vers 0
Pour voir ce que donne cette série, on peut tracer la suite des sommes partielles, grâce à Python.

Informatique - Visualiser la convergence

```
import matplotlib.pyplot as plt
def serie_alt(n,m):
    """serie alt. harmo., on trace les sommes entre n et m"""
    s=0.
    S=[]
    K=[]
    for k in range(n):
        s=s+(-1)**(k+1)/(k+1)
        for k in range(n,m):
            s=s+(-1)**(k+1)/(k+1)
            S=S+[s]
            K=K+[k+1]
    plt.plot(K,S)
    return(s)
```

Proposition - Critère de Leibniz
Soit (u_n) décroissante, positive, de limite nulle.
On considère la série $\sum_{n\geqslant 0}(-1)^n u_n$.
Alors la série $\sum_{n\geqslant 0}(-1)^n u_n$ (de signe alternés) est convergente.
Par ailleurs, on a l'inégalité de *contrôle* (très importante) :

$$\left|\sum_{k=n}^{+\infty}(-1)^k u_k\right| = \left|\sum_{k=0}^{n-1}(-1)^k u_k - S\right| \leqslant u_n$$

où $S = \sum_{k=0}^{+\infty}(-1)^k u_k$ est la limite (somme) de la série.

Démonstration
Premier cas : si (u_n) est nulle à partir d'un certain rang, la série est stationnaire. L'inégalité est bien obtenue à partir de ce certain rang.
Supposons donc que pour tout $n \in \mathbb{N}$, $u_n > 0$.
Le dessin, nous permet de voir la limite de la suite : il semble qu'il soit intéressant de considérer une somme partielles sur 2.
On a alors deux suites extraites : ceux d'indices pairs et ceux d'indices impairs.
C'est-à-dire on considère deux familles :

— $S_0, S_2, S_4, S_6, \dots, S_{2n}$ et le terme suivant $S_{2n+2}\dots$
— $S_1, S_3, S_5, S_7, \dots, S_{2n+1}$ et le terme suivant $S_{2n+3}\dots$

Nous allons montrer que ces deux suites sont adjacentes.
Considérons donc $n \in \mathbb{N}$,

— $S_{2(n+1)} - S_{2n} = (-1)^{2n+2}u_{2n+2} + (-1)^{2n+1}u_{2n+1} = u_{2n+2} - u_{2n+1}$.
or (u_n) est décroissante donc $u_{2n+2} - u_{2n+1} < 0$ et donc (S_{2n}) est décroissante.
— $S_{2(n+1)+1} - S_{2n+1} = (-1)^{2n+3}u_{2n+3} + (-1)^{2n+2}u_{2n} = u_{2n+2} - u_{2n+3}$.
or (u_n) est décroissante donc $u_{2n+2} - u_{2n+3} > 0$ et donc $(S_{2n}+1)$ est croissante.
— $S_{2n+1} - S_{2n} = -u_{2n+1} \to 0$.

Ces deux suites sont donc adjacentes, et l'on a la suite d'inégalités (v_n) croissante, (u_n) décroissante) :

$$v_0 < \dots < v_n < v_{n+1} < \dots < \ell < \dots < u_{n+1} < u_n < \dots < u_0$$

Les suites extraites paires et impaires de la suite des sommes partielles étant convergentes, la suite des sommes partielles converge (avec la même limite), i.e. que la série converge.
Et on a alors l'inégalité de contrôle des suites adjacentes (u_n) et (v_n) convergent vers ℓ :

$$|u_n - \ell| < |u_n - v_n| \text{ et } |v_n - \ell| < |v_n - u_{n+1}|.$$

Dans ce cas présent : $\ell = \sum_{k=0}^{+\infty}(-1)^k u_k$, $u_n = S_{2n}$ et $v_n = S_{2n+1}$.

alors $|u_n - v_n| = u_{2n+1}$ donc $\left|\sum_{k=0}^{2n}(-1)^k u_k - \sum_{k=0}^{n}(-1)^k u_k\right| = \left|\sum_{k=2n+1}^{+\infty}(-1)^k u_k\right| < u_{2n+1}$.

et $|v_n - u_{n+1}| = u_{2n+2}$ d'où $\left|\sum_{k=0}^{2n+1}(-1)^k u_k - \sum_{k=0}^{n}(-1)^k u_k\right| = \left|\sum_{k=2n+2}^{+\infty}(-1)^k u_k\right| < u_{2n+2}$.

Et ainsi, pour toute valeur $n \in \mathbb{N}$, $\left|\sum_{k=n}^{+\infty} u_k\right| < u_n$ □

Exercice

Montrer que la série $\sum_{k\geqslant 1}\frac{(-1)^k}{k}$ converge (série harmonique alternée).
Jusqu'à quelle valeur de n est-il suffisant de faire le calcul pour avoir une approximation de la limite de cette série à 10^{-5} prés (on peut penser à la rédaction d'un programme informatique d'approximation) ?

Correction

Cette série vérifie le critére de Leibniz, car $(\frac{1}{k})$ tend vers 0 en décroissant.
De plus on a pour tout entier n,

$$\left|\sum_{k=1}^{n}\frac{(-1)^k}{k} - \sum_{k=1}^{+\infty}\frac{(-1)^k}{k}\right| = \left|\sum_{k=n+1}^{+\infty}\frac{(-1)^k}{k}\right| < \frac{1}{n}$$

Donc dés que $\frac{1}{n} < 10^{-5}$, i.e. $n > 10^5$, alors S_n donne une approximation de $\sum_{k=1}^{+\infty}\frac{(-1)^k}{k}$ à au moins 10^{-5} prés.
Cette convergence n'est pas trés rapide. et converge vers $\ln 2$ (nous verrons des méthodes par la suite).

3. Séries à termes positifs

3.1. Majoration des sommes partielles

Heuristique - Motivations

Il y a plusieurs raisons qui motivent l'étude des séries positives.

1. La première est qu'ainsi on peut utiliser facilement le théorème de convergence monotone (des suites), puisque la suite des sommes partielles et dans ce cas une suite croissante.
2. La seconde est que les séries absolument convergentes (donc à termes positives) donne une condition suffisante pour l'étude de la convergence des séries.
3. Et même si on se place dans $\overline{\mathbb{R}^+}$ (on accepte des limite égale à l'infini), on peut affirmer que toute série à termes positifs est convergente. C'est ce qu'on fait dans la définition de l'intégrale de Lebesgue (cf. cours sur la sommabilité)…

Théorème - Condition simple de convergence

Soit $\sum u_n$ une série à termes positifs.
(Il suffit en fait que $u_n \geqslant 0$ à partir d'un certain rang.)
$\sum u_n$ converge si et seulement si la suite (S_n) des sommes partielles est majorée (c'est-à-dire s'il existe M tel que $\forall n, S_n \leqslant M$).

Pour aller plus loin - Sommer une infinité de termes strictement positifs, n'est-ce pas ridicule?

Certains sont choqués à l'idée que l'on puisse sommer une infinité de termes strictement positifs et que cela ne tende pas vers l'infini...
Ainsi, n'a-t-on pas simplement?

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots = 0,5 + 0,25 + 0,125 + \dots \longrightarrow +\infty$$

C'est un choc ***salutaire****, que vous* ***devez avoir****… et* ***dépasser****.*
Prenons l'exemple suivant de la série $\sum_{n\geqslant 0}\frac{1}{2^n}$.

On sait que $\forall\, n \in \mathbb{N}$, $\sum_{k=0}^{n}\frac{1}{2^n} = \frac{1-\frac{1}{2^{n+1}}}{1-\frac{1}{2}} = 2 - \frac{1}{2^n}$.

Or cette suite converge simplement vers 2, donc la série $\sum_{n\geqslant 0}\frac{1}{2^n}$ *converge vers 2*

Dans le cas contraire on a $\lim_{n\to+\infty} S_n = +\infty$.

Démonstration

On note, selon notre habitude $S_n = \sum_{k=0}^{n} u_k$.
La suite (S_n) est une suite croissante car pour tout $n \in \mathbb{N}$, $S_{n+1} - S_n = u_{n+1} \geqslant 0$.
Donc la suite (S_n) converge ssi elle est majorée. □

3.2. Comparaison des séries à termes positifs

Théorème - Inégalités

On suppose qu'à partir d'un certain rang $0 \leqslant u_n \leqslant v_n$. Alors :

$(\sum v_n \text{ converge} \Rightarrow \sum u_n \text{ converge})$ et $(\sum u_n \text{ diverge} \Rightarrow \sum v_n \text{ diverge})$.

Démonstration

Si $\sum v_n$ converge, alors la suite des sommes partielles (V_n) est bornée.
Et comme, pour tout $n \in \mathbb{N}$, $V_n - U_n = \sum_{k=0}^{n}(v_k - u_k) \geqslant 0$
(somme finie de termes positifs).
Donc la suite des sommes partielles (U_n) est également bornée.
D'après le théorème précédent, la série à termes positifs $\sum u_n$ est donc convergente.
La seconde affirmation est simplement la contraposée de la première. □

Proposition - Majoration par négligeabilité

On suppose qu'à partir d'un certain rang $0 \leqslant u_n$ et $0 \leqslant v_n$ et que $u_n = O(v_n)$.
Alors :

$(\sum v_n \text{ converge} \Rightarrow \sum u_n \text{ converge})$ et $(\sum u_n \text{ diverge} \Rightarrow \sum v_n \text{ diverge})$.

Démonstration

Dans ce cas, il existe $M \geqslant 0$ tel que $0 \leqslant u_n \leqslant M v_n$ à partir d'un certain rang.
Et l'on a donc les implications : $\sum v_n$ converge $\Rightarrow \sum M v_n$ converge $\Rightarrow \sum u_n$ converge.
Puis, on a la contraposée. □

Théorème - Équivalents

Si $u_n \underset{n\to+\infty}{\sim} v_n$, et $u_n \geqslant 0$ à partir d'un certain rang,
alors $\sum u_n$ et $\sum v_n$ sont de même nature.

Démonstration

Soit $N \in \mathbb{N}$, tel que pour tout $n \geqslant N$, $u_n \geqslant 0$.
On sait que $u_n \sim v_n$, donc $\lim \frac{u_n}{v_n} = 1$,
Ainsi avec $\epsilon = \frac{1}{2}$ (par exemple), il existe N' tel que $\frac{1}{2} = 1 - \frac{1}{2} \leqslant \frac{u_n}{v_n} \leqslant 1 + \frac{1}{2} = \frac{3}{2}$.
On a donc $u_n = O(v_n)$ et $v_n = O(u_n)$. On a alors la conclusion à partir du théorème précédent. □

On a des résultats plus précis encore :

Exercice

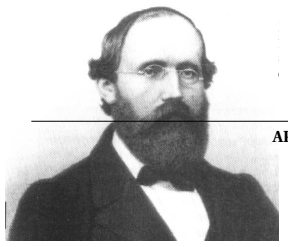
Soient $\sum u_n$ et $\sum v_n$ deux séries à *termes positives* telles que : $u_n \underset{n}{\sim} v_n$. Montrer que :

— si ces séries *convergent* alors les *restes* sont équivalents : $\sum_{k=n}^{+\infty} u_k \underset{n\to+\infty}{\sim} \sum_{k=n}^{+\infty} v_k$
— si ces séries *divergent* alors les *séries* sont équivalents : $\sum_{k=0}^{n} u_k \underset{n\to+\infty}{\sim} \sum_{k=0}^{n} v_k$

Correction

Histoire - Bernard Riemann

Riemann est l'un des plus grand mathématicien.



— Soit $\epsilon > 0$.
Il existe $N \in \mathbb{N}$ tel que $\forall\ n \geqslant N,\ (1-\epsilon)v_n \leqslant u_n \leqslant (1+\epsilon)v_n$ (on exploite la positivité).
On somme de $n \geqslant N$ à l'infini ; pour tout $n \geqslant N$:

$$(1-\epsilon)\sum_{k=n}^{+\infty} v_k \leqslant \sum_{k=n}^{+\infty} u_k \leqslant (1+\epsilon)\sum_{k=n}^{+\infty} v_k \Longrightarrow \left|\frac{\sum_{k=n}^{+\infty} u_k}{\sum_{k=n}^{+\infty} v_k} - 1\right| \leqslant \epsilon$$

— Un peu plus dur (car il faut aussi s'intéresser aux termes u_k avec $k \leqslant N$) : Avec les mêmes notations, en sommant de 1 à $n \geqslant N$:

$$\sum_{k=1}^{N-1}(u_k-(1-\epsilon)v_k)+(1-\epsilon)\sum_{k=1}^{n} nv_k \leqslant \sum_{k=1}^{n} u_k \leqslant \sum_{k=1}^{N-1}(u_k-(1+\epsilon)v_k)+(1+\epsilon)\sum_{k=1}^{n} nv_k$$

En notant $S_1 = \sum_{k=1}^{N-1}(u_k-(1-\epsilon)v_k)$ et $S_2 = \sum_{k=1}^{N-1}(u_k-(1+\epsilon)v_k)$, constant (par rapport à n) :

$$\frac{S_1}{\sum_{k=1}^{n} v_k} + (1-\epsilon) \leqslant \frac{\sum_{k=1}^{n} u_k}{\sum_{k=1}^{n} v_k} \leqslant \frac{S_2}{\sum_{k=1}^{n} v_k} + (1+\epsilon)$$

Or la série de terme général v_k diverge, donc il existe N' tel que $-\epsilon \leqslant \frac{S_1}{\sum_{k=1}^{n} v_k}$ et $\frac{S_2}{\sum_{k=1}^{n} v_k} \leqslant \epsilon$

$$\Longrightarrow \left|\frac{\sum_{k=1}^{n} u_k}{\sum_{k=1}^{n} v_k} - 1\right| \leqslant 2\epsilon$$

On rappelle que la recherche d'équivalents se fait pour des suites tendant vers 0 (restes, pour séries convergentes) ou vers $+\infty$ (sommes partielles, pour séries divergentes).

3.3. Exploitation des séries de Riemann

Théorie

Proposition - Séries de Riemann
Soit $\alpha \in \mathbb{R}$. La série de terme général $\frac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.

Démonstration
Notons $u_n^\alpha = \frac{1}{n^\alpha}$.

$$u_{n+1}^\alpha - u_n^\alpha = \frac{1}{(n+1)^\alpha} - \frac{1}{n^\alpha} = \frac{1}{n^\alpha}\left(\frac{1}{\left(1+\frac{1}{n}\right)^\alpha} - 1\right)$$

$$= \frac{1}{n^\alpha}\left((1+\tfrac{1}{n})^{-\alpha} - 1\right) \underset{n\to+\infty}{\sim} \frac{-\alpha}{n^{\alpha+1}}$$

ou encore pour $\alpha \neq 1$:

$$u_n^\alpha \underset{n\to\infty}{\sim} \frac{1}{\alpha}(u_n^{\alpha-1} - u_{n+1}^{\alpha-1})$$

Donc la série de Riemann $\sum \frac{1}{n^\alpha}$ converge ssi la suite $u_n^{\alpha-1}$ converge i.e. ssi $\alpha > 1$ Dans le cas $\alpha = 1$, on notera que

$$\ln(n+1) - \ln n = \ln(1+\frac{1}{n} \sim \frac{1}{n}$$

Donc la série de Riemann $\sum \frac{1}{n}$ diverge comme la suite $(\ln(n))$. □

Exercice
En exploitant l'exercice de la partie précédente, donner des équivalents des sommes partielles/restes des séries de Riemann

Correction

Pour aller plus loin - Culture
On a les résultats suivants $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, $\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$ *et* $\sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{\pi^6}{945}$

Supposons que $\alpha > 1$. Donc la série converge
On a l'équivalence sur les restes :

$$\sum_{k=n}^{+\infty} \frac{1}{k^\alpha} \underset{n\to\infty}{\sim} \sum_{k=n}^{+\infty} \frac{1}{\alpha-1}\left(\frac{1}{k^{\alpha-1}} - \frac{1}{(k+1)^{\alpha-1}}\right) = \frac{1}{(\alpha-1)n^{\alpha-1}}$$

Supposons que $\alpha < 1$. Donc la série diverge
On a l'équivalence sur les sommes partielles :

$$\sum_{k=1}^{n} \frac{1}{k^\alpha} \underset{n\to\infty}{\sim} \sum_{k=1}^{n} \frac{1}{\alpha-1}\left(\frac{1}{k^{\alpha-1}} - \frac{1}{(k+1)^{\alpha-1}}\right) \sim \frac{1}{(1-\alpha)(n+1)^{\alpha-1}}$$

Et si $\alpha = 1$

$$\sum_{k=1}^{n} \frac{1}{k} \underset{n\to\infty}{\sim} \sum_{k=1}^{n} (\ln(k+1) - \ln k) = \ln(n+1) \sim \ln n$$

Savoir-utiliser

Exercice
Étudier la nature de la série de terme général $u_n = n\ln\left(1+\frac{1}{n}\right) - \cos\frac{1}{\sqrt{n}}$.

Correction
On calcule un équivalent (il faudra bien noter que le terme général est positif).

$$u_n = n\left(\frac{1}{n} - \frac{1}{2n^2} + \frac{1}{3n^3}\right) - \left(1 - \frac{1}{2n} + \frac{1}{24n^2}\right) + o(\tfrac{1}{n^2}) \sim \frac{5}{24n^2}$$

Or la série à termes positifs $\sum \frac{1}{n^2}$ converge, il en est de même de $\sum u_n$.
Le corollaire suivant est plutôt à considérer comme un savoir-faire.

Savoir faire - Méthode du « $n^\alpha u_n$ »
Soit $\sum u_n$ une série à termes positifs.
— S'il existe $\alpha > 1$ réel tel que $\lim_{n\to+\infty} n^\alpha u_n = 0$, alors $\sum u_n$ converge.
— S'il existe $\alpha \leqslant 1$ réel tel que $\lim_{n\to+\infty} n^\alpha u_n = +\infty$, alors $\sum u_n$ diverge.

Pour aller plus loin - Constante de Mascheroni
Notons que la suite $\left(\sum_{n\geqslant 1} \frac{1}{n} - \ln(n)\right)$ *converge.*
On note γ*, sa limite (appelé constante d'Euler-Mascheroni).*
$\gamma \approx 0,5772156649015328606...$

Démonstration
S'il existe $\alpha > 1$ réel tel que $\lim_{n\to+\infty} n^\alpha u_n = 0$,
Alors il existe un rang n_0 tel que pour tout $n \geqslant n_0$, $n^\alpha u_n \leqslant 1$, donc $u_n \leqslant \frac{1}{n^\alpha}$.
Puis comme $\alpha > 1$, la série à termes positifs $\sum \frac{1}{n^\alpha}$ converge et de même pour $\sum u_n$.
S'il existe $\alpha \leqslant 1$ réel tel que $\lim_{n\to+\infty} n^\alpha u_n = +\infty$, alors $\sum u_n$ diverge.
Alors il existe un rang n_0 tel que pour tout $n \geqslant n_0$, $n^\alpha u_n \geqslant 1$, donc $u_n \geqslant \frac{1}{n^\alpha}$.
Puis $\alpha \leqslant 1$, donc la série à termes positifs $\sum \frac{1}{n^\alpha}$ diverge et de même pour $\sum u_n$.
□

3.4. Séries absolument convergentes

Définition - Série absolument convergente
La série $\sum u_n$ ($u_n \in \mathbb{R}$ ou $u_n \in \mathbb{C}$) est dite **absolument convergente** si la série $\sum |u_n|$ est convergente.

Théorème - Implication
Une série absolument convergente est convergente.

Attention - La réciproque est fausse
On exploite le contre-exemple classique suivant : $\sum_{n\geqslant 1} \frac{(-1)^n}{n}$.
— $\sum u_n$ est convergente.
Pour $n \in \mathbb{N}^*$, $a_n = u_{2n+1} + u_{2n+2} = \frac{-1}{2n+1} + \frac{1}{2n+2} = \frac{-1}{4n^2+6n+2}$.
$-a_n > 0$, $-a_n \sim \frac{1}{4n^2}$ et $\sum \frac{1}{4n^2}$ converge.
Donc $\sum a_n$ également.

Enfin, notons que

$$\sum_{n=1}^{\lfloor\frac{N-1}{2}\rfloor} a_n \leqslant \sum_{n=1}^{N} \frac{(-1)^n}{n} \leqslant \sum_{n=1}^{\lfloor\frac{N}{2}\rfloor} a_n$$

Donc par encadrement, la série $\sum u_n$ converge.

— $\sum u_n$ n'est pas absolument convergente, cela signifierait que la série harmonique converge.

Démonstration
Pour tout entier n, on note $u_n^+ = \max(u_n, 0)$ et $u_n^- = \max(-u_n, 0)$.
Alors pour tout $n \in \mathbb{N}$, $u_n = u_n^+ - u_n^-$ alors que $|u_n| = u_n^+ + u_n^-$.
Supposons que la série $\sum |u_n|$, alors par comparaison de série à termes positifs :
$\sum u_n^+$ et $\sum u_n^-$ convergent.
Et par combinaison linéaire : $\sum u_n$ converge. □

4. Quelques méthodes d'étude

4.1. Plan d'étude

Remarque - Différence entre…
Lorsqu'il faut faire des démonstrations de types « théoriques », on exploite souvent la stratégie :

1. Etude (calcul, croissance…) de la (suite des) somme(s) partielle(s).
2. Puis passage à la limite (ou majoration)

Lorsqu'il faut faire des démonstrations pratiques, on ne s'intéresse pas à la suite des sommes partielles, mais **on se concentre sur la suite de terme général** (directement!) grâce aux théorèmes de comparaisons.
Ce sont deux approches très différentes!

Savoir faire - Plan d'étude d'une série numérique

ature de la suite	terme général	méthode d'étude de la série
u_n) diverge		$\sum u_n$ diverge
$\lim_{n\to+\infty} u_n \neq 0$		$\sum u_n$ diverge
$\lim_{n\to+\infty} u_n = 0$	u_n réel, $\forall n, u_n \geqslant 0$	on compare à une série de référence ou on « voit » un téléscopage ou on majore les sommes partielles ou on compare avec une intégrale
	u_n réel, $\forall n, u_n \leqslant 0$	on étudie la série de t.g. $-u_n$
	$u_n = (-1)^n v_n$ si $(v_n) \searrow$ (ou $\nearrow$) (nécessairement $(v_n) \to 0$)	On applique le critère de LEIBNIZ
	u_n réel mais pas de signe constant	on étudie $\sum \lvert u_n\rvert$ avec $\lvert u_n\rvert \geqslant 0$: si $\sum \lvert u_n\rvert$ cv alors $\sum u_n$ cv si $\sum \lvert u_n\rvert$ div : voir au cas par cas
	u_n complexe	on étudie $\sum \lvert u_n\rvert$ avec $\lvert u_n\rvert \geqslant 0$: si $\sum \lvert u_n\rvert$ cv alors $\sum u_n$ cv si $\sum \lvert u_n\rvert$ div : on étudie $\sum \mathrm{Re}\, u_n$ et $\sum \mathrm{Im}\, u_n$

Le tableau sera complété encore l'année prochaine : semi-convergence : convergence de la série et non convergence absolue, critère de d'Alembert…

4.2. Comparaison série-intégrale

Lemme - Comparaison directe
Soient $n_0 \in \mathbb{N}$ et f continue par morceaux, décroissante sur $[n_0, +\infty[$. Alors :

$$\forall n \geqslant n_0 + 1, \int_n^{n+1} f(t)\mathrm{d}t \leqslant f(n) \leqslant \int_{n-1}^{n} f(t)\mathrm{d}t.$$

Proposition - Même comportement série-intégrale
Soient $n_0 \in \mathbb{N}$ et f continue par morceaux, positive, décroissante sur $[n_0, +\infty[$.
Alors $\sum_{n\geqslant n_0} f(n)$ converge si et seulement si l'application $x \mapsto \int_{n_0}^x f(t)\mathrm{d}t$ admet une limite finie quand x tend vers $+\infty$.

Démonstration
On commence par la démonstration du lemme.
Puisque f est décroissante sur $[n, n+1]$,
pour tout $t \in [n, n+1]$, $f(n) \geqslant f(t) \geqslant f(n+1)$.
En passant à l'intégration entre n et $n+1$ (pour la variable t) :

$$\int_n^{n+1} f(n)\mathrm{d}t = f(n) \geqslant \int_n^{n+1} f(t)\mathrm{d}t \geqslant \int_n^{n+1} f(n+1)\mathrm{d}t = f(n+1)$$

On démontre de même : $\int_{n-1}^{n} f(t)\mathrm{d}t \geqslant \int_n^{n-1} f(n)\mathrm{d}t = f(n)$.
Le lemme est ainsi démontré.
On continue avec celle de la proposition.
En additionnant pour n entre n_0+1 et N (avec la relation de Chasles) :

$$\int_{n_0+1}^{N+1} f(t)\mathrm{d}t \leqslant \sum_{n=n_0+1}^{N} f(n) \leqslant \int_{n_0}^{N} f(t)\mathrm{d}t.$$

Tout est positif, la convergence de la série (comme de l'intégrale) est assurée par majoration.
La première inégalité permet d'affirmer : si $\sum_{n\geqslant n_0} f(n)$ converge alors $x \mapsto \int_{n_0}^x f(t)\mathrm{d}t$ converge.
Et la seconde inégalité : si $x \mapsto \int_{n_0}^x f(t)\mathrm{d}t$ converge alors $\sum_{n\geqslant n_0} f(n)$converge. □

Savoir faire - Comment exploiter la comparaison série-intégrale
Si f est monotone à partir d'un certain rang X, alors pour tout $n \geqslant \lfloor X\rfloor + 1$,
on a - cas décroissant - : $\forall N \geqslant N$, $\int_{n+1}^{N+1} f(t)\mathrm{d}t \leqslant \sum_{k=n+1}^{N} f(k) \leqslant \int_n^N f(t)\mathrm{d}t$.
(pour le cas croissant, les inégalités sont inversées).
Puis, par méthodes supplémentaires sur les calculs d'intégrales : IPP, changement de variable, utilisation de la primitive…, on peut transférer, par encadrement les informations sur la série $\sum_{k\geqslant N} f(k)$.

4.3. Séries de référence

Les deux derniers résultats, hors-programme en première année, sont données « pour la culture ».

Truc & Astuce pour le calcul - Série de référence
• Série de Riemann
La série de terme général $\dfrac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.
• Série géométrique
La série de terme général x^n est convergente si et seulement si $|x| < 1$.
• Série du binôme négatif

Soit $r \in \mathbb{N}$. Si $|x| < 1$, la série $\sum_{k \geqslant r} \binom{k}{r} x^{k-r}$ converge ;

$$\sum_{k=r}^{+\infty} \binom{k}{r} x^{k-r} = \sum_{h=0}^{+\infty} \binom{r+h}{h} x^h = \frac{1}{(1-x)^{r+1}}$$

• Série exponentielle

Pour tout x complexe, la série $\sum \frac{x^n}{n!}$ converge ; $\sum_{n=0}^{+\infty} \frac{x^n}{n!} = e^x$.

Exercice

Soit $x \in]-1,1[$.

On note pour tout $n \in \mathbb{N}$, pour tout $p \in \mathbb{N}$, $a_p^n = \binom{p+n}{p} x^p$. On s'intéresse à la série $T^n = \sum_{p \geqslant 0} a_p^n$.

1. Montrer que la série T^n est convergente.
2. Rappeler la formule du triangle de Pascal.
3. Simplifier (téléscopage) $(1-x) \sum_{p=0}^{N} a_p^n$, en déduire : $(1-x) \sum_{p=0}^{+\infty} a_p^n = \sum_{p=0}^{+\infty} a_p^{n-1}$
4. Exprimer T^0, en déduire pour tout $n \in \mathbb{N}$ la valeur de $\sum_{p=0}^{+\infty} \binom{p+n}{p} x^p = \sum_{p=0}^{+\infty} \binom{p+n}{n} x^p$

Correction

1. Soit $x < 1$. $p^2 \times \binom{p+n}{p} x^p \longrightarrow 0$, pour $p \to +\infty$, car $x < 1$.
   Donc la série $\sum_p \binom{p+n}{p} x^p$ converge.
2. On sait que pour $a+1 \leqslant b$, $\binom{b}{a} + \binom{b}{a+1} = \binom{b+1}{a+1}$.
3. $$(1-x) \sum_{p=0}^{N} a_p^n = \sum_{p=0}^{N} \binom{p+n}{p} x^p - \sum_{p=0}^{N} \binom{p+n}{p} x^{p+1} = \binom{n}{0} + \sum_{p=1}^{N} \binom{p+n}{p} x^p - \sum_{p=1}^{N} \binom{p-1+n}{p-1} x^p - \binom{N+n}{N} x^{N+1}$$
   $$= 1 + \sum_{p=1}^{N} \left(\binom{p+n}{p} - \binom{p-1+n}{p-1} \right) x^p - \binom{N+n}{N} x^{N+1}$$
   $$= \binom{n-1}{0} x^0 + \sum_{p=1}^{N} \binom{p-1+n}{p} x^p - \binom{N+n}{N} x^{N+1} = \sum_{p=0}^{N} a_p^{n-1} - \binom{N+n}{N} x^{N+1}$$
   En passant à la limite ($N \to +\infty$), on a donc $(1-x) \sum_{p=0}^{+\infty} a_p^n = \sum_{p=0}^{+\infty} a_p^{n-1}$
4. $T^0 = \sum_{p=0}^{+\infty} \binom{p}{p} x^p = \sum_{p=0}^{+\infty} x^p = \frac{1}{1-x}$.
   Puis on a vu que $T^n = \frac{1}{1-x} T^{n-1}$, donc par récurrence : $T^n = \frac{1}{(1-x)^{n+1}}$

Exercice

Soient les deux suites (S_n) et (S'_n) telles que

$$\forall\, n \in \mathbb{N}^* : S_n = \sum_{k=0}^{n} \frac{1}{k!} \text{ et } S'_n = \frac{1}{n \cdot n!} + \sum_{k=0}^{n} \frac{1}{k!}.$$

1. Montrer que (S_n) et (S'_n) sont adjacentes.

Nous admettons qu'elles convergent vers e (voir dernière question).

2. Ecrire un programme en Python utilisant les suites (S_n) et (S'_n) pour calculer une approximation de e à 10^{-6}
3. Soit $x > 0$. Soient $p, n \in \mathbb{N}$ avec $p \leqslant n$.
   (a) Montrer que $\left(1 + \frac{x}{n}\right)^n \geqslant \sum_{k=0}^{p} \frac{1 \times (1 - \frac{1}{n}) \times \cdots \times (1 - \frac{k-1}{n})}{k!} x^k$
   (b) En faisant tendre n vers l'infini, en déduire que $e^x \geqslant \sum_{k=0}^{p} \frac{x^k}{k!}$.

   (c) En déduire que la suite $\left(\sum_{k=0}^{p} \frac{x^k}{k!} \right)_p$ est convergente (série à termes positifs)
   (d) Par ailleurs, montrer que $\left(1 + \frac{x}{n}\right)^n \leqslant \sum_{k=0}^{n} \frac{1}{k!} x^k$ *(remarquer la différence avec la question (a))*
   (e) En déduire que $e^x = \sum_{k=0}^{+\infty} \frac{x^k}{k!}$ (notation de la limite de la suite définie par une somme).

Correction

1. — $\forall\, n \in \mathbb{N}^*$, $S_{n+1} - S_n = \frac{1}{(n+1)!} > 0$, donc (S_n) est croissante.
   — $\forall\, n \in \mathbb{N}^*$, $S'_{n+1} - S'_n = \frac{1}{(n+1)\cdot(n+1)!} - \frac{1}{n \cdot n!} + \frac{1}{(n+1)!} = \frac{1 - (n+1)^2 + n + 1}{(n+1)\cdot(n+1)!}$
   $= \frac{1 - n^2 - n}{(n+1)\cdot(n+1)!} < 0$, donc (S'_n) est décroissante.
   — $\forall\, n \in \mathbb{N}^*$, $S'_n - S_n = \frac{1}{n \cdot n!} \to_{\infty} 0$
   Les deux suites sont bien adjacentes.
2. **Informatique - Approximation de e**

```
def approx_e(n) :
    S1,S2,fac=1,2,1
    for k in range(n) :
        fac=fac*k
        S1=S1+1/fac
        S2=S1+1/(fac*k)
    diff=S2-S1
    return([S1,S2,diff])
```

Remarquons que les calculs des premiers termes (S_n) et (S'_n) donne :

n	0	1	2	5	7	10	13
S_n	1	2	2,5	2,71$\overline{6}$	2,7182539683	2,7182818011	2,7182818284
S'_n	ND	3	2,75	2,7183	2,7182823129	2,7182818287	2,7182818285

C'est donc une convergence assez rapide vers e.

3. Soit $x > 0$ et $p \leqslant n$.
   (a) $\left(1 + \frac{x}{n}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \frac{x^k}{n^k}$.
   Or $\binom{n}{k} \frac{x^k}{n^k} = \frac{n \times (n-1) \times \ldots (n-k+1)}{n \times n \times \ldots n} \frac{x^k}{k!} = \frac{1 \times (1 - \frac{1}{n}) \times \ldots (1 - \frac{k-1}{n})}{k!} x^k$
   Ainsi, $\left(1 + \frac{x}{n}\right)^n = \sum_{k=0}^{n} \frac{1 \times (1 - \frac{1}{n}) \times \ldots (1 - \frac{k-1}{n})}{k!} x^k$.
   Comme $x > 0$ et $p \leqslant n$, on peut tronquer la somme à $k = p$, on enlève des nombres positifs et donc :
   $\left(1 + \frac{x}{n}\right)^n \geqslant \sum_{k=0}^{p} \frac{1 \times (1 - \frac{1}{n}) \times \ldots (1 - \frac{k-1}{n})}{k!} x^k$.
   (b) Comme p est fixe, le nombre de terme limité, on a pour tout $k \in \mathbb{N}_p$, $\lim_{n \to +\infty} 1 \times (1 - \frac{1}{n}) \times \ldots (1 - \frac{k-1}{n}) = 1$, et donc par élargissement de l'inégalité en faisant tendre n vers 'infini :
   $e^x \geqslant \sum_{k=0}^{p} \frac{1}{k!} x^k$.
   (c) Par ailleurs, la suite $\left(\sum_{k=0}^{p} \frac{1}{k!} x^k \right)_p$ est croissante (on ajoute des termes positifs, comme x), majorée par e^x donc convergente.
   (d) En outre, $\left(1 + \frac{x}{n}\right)^n = \sum_{k=0}^{n} \frac{1 \times (1 - \frac{1}{n}) \times \ldots (1 - \frac{k-1}{n})}{k!} x^k$.
   Or $\forall\, k \in \mathbb{N}_n$, $1 \times (1 - \frac{1}{n}) \times \ldots (1 - \frac{k-1}{n}) \leqslant 1$. Donc $\left(1 + \frac{x}{n}\right)^n \leqslant \sum_{k=0}^{n} \frac{1}{k!} x^k$

(e) En passant à la limite (n tendant vers $+\infty$) : $e^x \leqslant \lim\limits_{n\to+\infty} \sum\limits_{k=0}^{n} \frac{1}{k!}x^k$.

Par double inégalité : $e^x = \lim\limits_{n\to+\infty}\left(\sum\limits_{k=0}^{n}\frac{1}{k!}x^k\right) = \sum\limits_{k=0}^{+\infty}\frac{1}{k!}x^k$

Savoir faire - Calcul exact avec des séries exponentielles

Considérons un polynôme P de degré d (pas trop élevé).

On cherche à calculer la valeur de $S = \sum\limits_{n=0}^{+\infty}\frac{P(n)}{n!}x^n$ où $x \in \mathbb{R}$.

La famille $\left(1, X, X(X-1), \dots X(X-1)\cdots(X-d)\right)$ est échelonnée, composée de $d+1$ polynômes : elle forme une base de $\mathbb{K}_d[X]$.

Donc il existe $a_0, a_1, \dots a_d$ tels que $P = \sum\limits_{k=0}^{d} a_k N_k$ où $N_k = X(X-1)\cdots(X-k)$ (qu'est-ce N_0 ?)

Alors *par linéarité* : $S = \sum\limits_{k=0}^{d} a_k\left(\sum\limits_{n=0}^{+\infty}\frac{N_k(n)}{n!}x^n\right)$ mais $N_k(n)$ **et** $n!$ **se simplifient**…

Exercice

Calculer $S = \sum\limits_{n=0}^{+\infty}\frac{3^n + n^2 2^n}{n!}$

Correction

$n^2 = n(n-1)+n$ et donc $\frac{3^n+n^2 2^n}{n!} = \frac{3^n}{n!} + \frac{n(n-1)}{n!}2^n + \frac{n}{n!}2^n = \frac{1}{n!}3^n + 4\frac{1}{(n-2)!}2^{n-2} + 2\frac{1}{(n-1)!}2^{n-1}$.

Et donc (en étant bien attentif aux indices) : $S = e^3 + 4e^2 + 2e^2 = e^3 + 6e^2$

5. Bilan

Synthèse

⇝ On s'intéresse à un cas particulier de suites : les séries. Ce sont des cas particuliers car on les étudie comme les suites des sommes partielles. Et en même temps, toute suite peut se voir comme suite de sommes partielles d'une série…
Une série convergente a nécessairement son terme général qui tend vers 0. Et plus généralement la suite des restes.

⇝ Pour étudier les séries, on utilise nécessairement d'autres méthodes que celles des suites (sinon, cela ne ferait pas un chapitre différent). Pour le cours et démontrer les propositions : on exploite les résultats sur les suites. Mais, une fois ces propositions démontrées, on n'y revient plus.
Ainsi la méthode est toujours la même : quel est le signe du terme général ? Si il est constant, on peut comparer à une série de Riemann ; si il est alterné, on exploite le critère de Leibniz.

⇝ Lorsque tout est positif, on peut dire d'une certaine façon que tout est plus simple : soit la somme est infinie, soit elle est finie et donc la série convergente. Cela se généralise aux sommes multiples !
Mais, lorsque le terme général change infiniment de signe, tout est plus compliqué. Le critère de convergence absolue peut aider, mais il n'est pas toujours efficace (d'où certains problèmes rencontrés en probabilité discrète de deuxième année).

⇝ On s'intéresse à la convergence (deux points précédents), mais on peut aussi s'intéresser à la valeur exacte de la limite lorsqu'on sait que la série converge.

Pour faire cette étude, il y a beaucoup moins de résultats. La méthode d'emploi des séries entières (deuxième année) est la plus complète. On l'anticipe ici en donnant le résultat pour les séries géométriques, binomiales (négatives) et exponentielles.

⇝ Les séries est le meilleur outil pour étudier le développement décimal des nombres réels.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Critère de Cauchy pour les séries
— Savoir-faire - Méthode du « $n^a u_n$ »
— Savoir-faire - Comment exploiter la comparaison série-intégrale
— Savoir-faire - Plan d'étude d'une série numérique
— Truc & Astuce pour le calcul - Série de référence
— Savoir-faire - Calcul exact avec des séries exponentielles

Notations

Notations	*Définitions*	*Propriétés*	*Remarq*
$\sum\limits_{n\geqslant n_0} u_n$ ou $\sum u_n$	Série de terme général $(u_n)_{n\geqslant n_0}$	On ne peut se poser la question que de la convergence ou non	Elle ne termes.
$\sum\limits_{n=n_0}^{N} u_n$	Somme partielle de la série de terme général $(u_n)_{n\geqslant n_0}$		C'est le suite.
$\sum\limits_{n=n_0}^{+\infty} u_n$	Limite ou Somme de la série de terme général $(u_n)_{n\geqslant n_0}$		On ne l' la conve
$(R_n)_n$	Suite des restes de la série de terme général $(u_n)_{n\geqslant n_0}$	$R_n = \sum\limits_{k=n}^{+\infty} u_k$	On ne l' la conve

Retour sur les problèmes

124. Oui, elles convergent toutes, car ici ce sont des series à termes positifs. Le terme général d_n est majorée par 9×10^n, et les sommes partielles sont majorées par $d_0 + 1$.
On peut associer à tout nombre réel un développement décimal. Mais il n'y a pas injectivité : $0,999\dots99\cdots = 1,0\dots$.
C'est le sens de toute la partie 5 de ce chapitre.

125. Cours. On notera ici la manipulation pour revenir d'un cas relativement générale $u_{n+1} = u_n \times v_n + w_n$ à l'étude d'une série $\sum \ln v_n$…

126. Il faut vraiment apprendre le tableau des méthodes pour montrer la convergence des séries. Et celui qui donne la valeur de la limite de (certaines) séries.

127. L'IPP, c'est $\int_a^b f'(t)g(t)\mathrm{d}t = [f(t)g(t)]_a^b - \int_a^b f(t)g'(t)\mathrm{d}t$.
On démontre ce résultat en dérivant $f\times g$. Si la dérivation c'est le passage $u_n \to u_{n+1} - u_n$, on trouve :

$$\begin{aligned}(uv)_{k+1} - (uv)_k &= u_{k+1}v_{k+1} - u_k v_k = u_{k+1}v_{k+1} - u_k v_{k+1} + u_k v_{k+1} - u_k v_k\\ &= (u_k)' v_{k+1} - u_k (v_k)'\end{aligned}$$

Donc en sommant pour k entre 0 et $n-1$:

$$u_n v_n - u_0 v_0 = [uv]_0^n = \sum_{k=0}^{n-1}(u_{k+1}-u_k)v_{k+1} + \sum_{k=0}^{n-1} u_k(v_{k+1}-v_k)$$

On appelle transformation d'Abel la relation :

$$\sum_{k=0}^{n-1} u_k(v_{k+1}-v_k) = u_n v_n - u_0 v_0 - \sum_{k=0}^{n-1}(u_{k+1}-u_k)v_{k+1}$$

128. En fait, on fais venir par la transformation une infinité de termes négatifs, certes petits mais en nombre suffisant pour réduire la valeur de la somme.
Pour montrer que le résultat que tout nombre est atteignable à partir de la série harmonique alternée en changeant l'ordre, on crée un algorithme. D'un côté les nombres positifs : $1, \frac{1}{3}, \frac{1}{5}\dots$ le nombres d'indices pairs $(\frac{1}{k+1})$ et de l'autre les négatifs : $\frac{-1}{2}, \frac{-1}{4}\dots$. Les sommes de chacune de ces deux suites divergent vers $+\infty$ et $-\infty$ respectivement.
Considérons un nombre ℓ, réel.
On crée deux suites de nombre (p_n) et (i_n) croissantes et la fonction $\varphi : \mathbb{N} \to \mathbb{N}$ bijective par récurrence :
— Si $\ell > 0$, on prend $\varphi(0) = 0$, et donc $u_{\varphi(0)} = u_0 = 1$. On considère alors que $p_0 = 1$ et $i_0 = 0$
Si $\ell \leqslant 0$, on prend $\varphi(0) = 1$, et donc $u_{\varphi(0)} = u_1 = -\frac{1}{2}$ et donc $i_0 = 1$ et $p_0 = 0$.
— On suppose que les suites $(p_k)_{k\leqslant n}$, $(i_k)_{k\leqslant n}$ sont créée ainsi que $\varphi([\![0, n]\!])$.
On considère le nombre $S_n = \sum_{k=0}^{n} u_{\varphi(k)}$, somme partielle.
Si $\ell > S_n$, le terme suivant est à prendre dans les nombres positifs.
Donc on prend $\varphi(n+1) = 2p_n$, puis $p_{n+1} = p_n + 1$ et $i_{n+1} = i_n$.
Si $\ell \leqslant S_n$, le terme suivant est à prendre dans les nombres négatifs.
Donc on prend $\varphi(n+1) = 2(i_n + 1)$, puis $p_{n+1} = p_n$ et $i_{n+1} = i_n + 1$.
On ne démontre pas, mais φ est bien bijective. La suite $|S_n - \ell|$ est décroissante (à peu près - sauf quand on dépasse ℓ) et tend vers 0 donc $(S_n) \to \ell$.
(p_n) et (i_n) indiquent les indices qui reste à prendre dans les nombres positifs ou négatifs...

129. Pas vraiment de question

Chapitre 39

Familles sommables

Résumé -

On définit ici les familles de nombres sommables. Il s'agit d'élargir la question des sommes finies (vues en début d'année), puis des séries (vues au second semestre) à une somme de réels ou de complexes indexés sur un ensemble qui finalement doit être dénombrable (comme $\mathbb{Q}$ ou $\mathbb{N}^2$...).

On commence par étudier ces sommes pour des réels positifs. Le plus difficile est d'obtenir des critère nécessaire ET suffisant : la comparaison bien pratique ne suffit pas toujours ; on peut sommer par paquets, ou bien sur une suite croissante d'ensemble dont la réunion vaut D.

On reprend dans un second temps les méthodes lorsque les nombres sont réels voire complexes.

Finalement, il ne reste qu'une méthode : 1) Prendre la valeur absolue, 2) Sommer dans $\overline{\mathbb{R}}$ et 3) Conclure selon que la somme vaut $+\infty$ ou est un nombre de $\mathbb{R}$.

Sommaire

1. Problème 802
2. Somme de famille de réels positifs 802
2.1. Définition 803
2.2. Cas $I = \mathbb{N}$ 803
2.3. Cas $I = \mathbb{N}^2$ 804
2.4. Comparaisons 805
2.5. Sommation par suite croissante d'ensembles 806
2.6. Sommation par paquets et théorème de Fubini . . . 808
2.7. Enoncé dans $\overline{\mathbb{R}_+} = [0, +\infty]$ 811
3. Familles complexes sommables 812
3.1. Définition 812
3.2. Critère de sommabilité et calcul de somme 812
3.3. Espace vectoriel $\ell^1(D, \mathbb{K})$ 813
3.4. Transfert de propriétés sur $\ell^1(D, \mathbb{K})$ 814
3.5. Sommation par paquets et Fubini 816
3.6. Application : Produit de Cauchy 819
4. Bilan 820

1. Problème

Problème 170 - Somme d'une famille indexé sur $\mathbb{N}^2$

Il nous arrive de rencontrer une famille de nombres définie sur l'ensemble $\mathbb{N}^2$. Par exemple, si on lance deux dés avec une infinité de faces, et qu'on souhaite faire la somme des probabilités des résultats possibles (sur les couples) donc. Comment gérer ces sommes ? En particulier si on note p et q les deux nombres. Faut-il d'abord faire $p \to +\infty$, puis $q \to +\infty$ ou l'inverse ou encore les deux « en même temps » ?

Problème 171 - Changement d'ordre de l'addition des termes d'une série

Considérons la somme $\sum_{n\geqslant 0} \frac{(-1)^n}{n+1}$.

Notons, pour tout entier n, $S_n = \sum_{k=0}^{n} \frac{(-1)^k}{k+1}$. Alors, on démontrera que (S_n) converge (vers $\ln 2$, par ailleurs).

Que pensez alors de la sommation suivante :

$$\begin{aligned} S &= 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} + \frac{1}{9} - \frac{1}{10} + \frac{1}{11} - \frac{1}{12} + \dots \\ &= 1 - \frac{1}{2} - \frac{1}{4} + \frac{1}{3} - \frac{1}{6} - \frac{1}{8} + \frac{1}{5} - \frac{1}{10} - \frac{1}{12} + \frac{1}{7} - \frac{1}{14} - \frac{1}{16} + \dots \\ &= \frac{1}{2} - \frac{1}{4} + \frac{1}{6} - \frac{1}{8} + \frac{1}{10} - \frac{1}{12} + \frac{1}{14} - \frac{1}{16} + \dots = \frac{1}{2} S \end{aligned}$$

Etonnant : $S = \frac{1}{2}S$, alors que $S = \ln 2$. Pourquoi ?

Mieux : on peut même trouver n'importe quelle limite possible $\ell \in \mathbb{R}$, en changeant l'ordre de sommation. Comment démontrer ce résultat ?

Problème 172 - Ordre de calcul

On a vu dans le problème précédent que $\sum_{n\geqslant 1} \frac{(-1)^n}{n}$ admet une limite, mais que si l'on change l'ordre du calcul, la valeur limite évolue.

Peut-on se débarrasser des problèmes du même genre : dépendance selon l'ordre de sommation ? En particulier, en probabilité, il peut ne pas avoir d'ordre naturel entre les événements $[X = a]$ et donc les nombres $\mathbf{P}(X = a)$ pour $a \in A$, où $A = X(\Omega)$ est dénombrable (et X est une variable aléatoire). On aimerait que le résultat (qui conduit à l'espérance de X, par exemple) ne donne pas des nombres différents selon l'ordre de l'opération.

Problème 173 - Structure d'espace vectoriel ?

Si deux familles sont sommables, en est-il de même de toutes combinaisons linéaires de ces familles ? Et que dire de la somme de cette combinaison linéaire alors ?

2. Somme de famille de réels positifs

Soit I un ensemble non vide et $\mathscr{P}_f(I)$, l'ensemble des parties finies de I.

2.1. Définition

Définition - Famille de réels positifs sommable
Une famille $(\alpha_i)_{i\in I}$ de réels positifs ou nuls est dite sommable, si

$$\exists\, M\in\mathbb{R}+, \forall\ J\in\mathscr{P}_f(I), \sum_{i\in J}\alpha_i \leqslant M$$

Si tel est le cas, on définit et on note la somme de la famille $(\alpha_i)_{i\in I}$ par :

$$S_I(\alpha) := \sum_{i\in I}\alpha_i = \sup_{J\in\mathscr{P}_f(I)}\sum_{j\in J}\alpha_i$$

Si la famille n'est pas sommable, alors on pose $\sum_{i\in I}\alpha_i = +\infty$ (ce qui est bien la valeur de la borne supérieure…)

Remarque - Rappel
Une somme indexée par un ensemble vide existe et vaut 0.

Exemple - Cas I fini
Si I est fini, alors toute famille de réels positifs $(\alpha_i)_{i\in I}$ est sommable et sa somme en tant que famille sommable est sa somme habituelle : $S_I(\alpha) = \sum_{i\in I}\alpha_i$.

Exercice
Supposons qu'il existe $a>0$ tel que pour tout $i\in I$, $\alpha_i = a$.
Alors montrer que $(\alpha_i)_{i\in I}$ est sommable $\iff$ I est fini.

Correction
Si I est fini, alors $(\alpha_i)_{i\in I}$ est sommable.
Réciproquement, si la famille est sommable, il existe $M>0$ tel que pour tout $J\in\mathscr{P}_f(I)$, $\sum_{i\in J}\alpha_i < M$.

Mais comme la famille est constante, $\sum_{i\in J}\alpha_i = a\times \mathrm{card}(J)$, donc pour tout $J\in\mathscr{P}_f(I)$, $\mathrm{card}(J)\leqslant \frac{M}{a}$.

Par l'absurde, I possède donc nécessairement moins de $\lfloor\frac{M}{a}\rfloor$ éléments, donc I est fini.

2.2. Cas $I=\mathbb{N}$

Proposition - Cas $I=\mathbb{N}$. Les séries positifs
La suite $(u_n)_{n\in\mathbb{N}}$ est sommable si et seulement si la série $\sum_{n\geqslant 0}u_n$ converge.

En cas de sommabilité : $S_{\mathbb{N}}(u) = \sum_{n=0}^{+\infty}u_n$.

Démonstration
Supposons que $(u_n)_{n\in\mathbb{N}}$ est sommable.
Il existe donc $M>0$ tel que $\forall\ J\in\mathbb{N}$, $\sum_{i\in J}u_n\leqslant M$.

On peut prendre pour M : $S_{\mathbb{N}}(u)$ En particulier pour $J=[\![0,n]\!]$, on trouve que

$$\sum_{k=0}^{n}u_k \leqslant S_{\mathbb{N}}(u)$$

i.e. : la suite des sommes partielles est majorée.
Il s'agit d'une série à termes positifs, donc cette condition est suffisante pour affirmer que la série est convergente.

Et on a $\sum_{n=0}^{+\infty}u_n \leqslant S_{\mathbb{N}}(u)$.

Réciproquement, supposons que la série soit convergente.
Soit J une partie finie de $\mathbb{N}$. On note $N=\max J$, donc $J\subset[\![0,N]\!]$.
Comme la série est à termes positifs :

$$\sum_{n\in J}u_n \leqslant \sum_{n=0}^{N}u_n \leqslant \sum_{n=0}^{+\infty}u_n$$

Ainsi, $\{\sum_{n\in J}u_n, J\in\mathscr{P}_f(\mathbb{N})\}$ est majoré par $\sum_{n=0}^{+\infty}u_n$ (indépendant de J).

Donc la famille $(u_n)_{n\in\mathbb{N}}$ est sommable et on trouve $S_{\mathbb{N}}(u)\leqslant\sum_{n=0}^{+\infty}u_n$.

On a donc montré l'équivalence et par double inégalité, on a $S_{\mathbb{N}}(u)=\sum_{n=0}^{+\infty}u_n$. □

Remarque - Notation
Si la famille $(u_i)_{i\in I}$ est sommable, on peut noter sa sommes $S_I(u)$ ou bien $\sum_{i\in I}u$, il n'y a pas de contradiction lorsqu'on écrit quelque chose comme $\sum_{p\in\mathbb{N}^*}\frac{1}{n^\alpha}$.

Cela peut tout autant désigner la limite de la série ou la somme de la famille sommable.

2.3. Cas $I=\mathbb{N}^2$

Savoir faire - Sous ensembles finis de $\mathbb{N}^2$
Se concentrer sur $[\![0,N]\!]\times[\![0,P]\!]$ car les familles sont à termes positifs.

Exercice
Montrer la sommabilité de la famille $\left(\frac{1}{p^2q^2}\right)_{(p,q)\in(\mathbb{N}^*)^2}$

Correction
Soit J une partie finie de $\mathbb{N}^2$.
Alors $A=\{p\in\mathbb{N}\mid\exists\, q\in\mathbb{N}$ tel que $(p,q)\in J\}$ est fini donc majoré par un entier P. Et $B=\{q\in\mathbb{N}\mid\exists\, p\in\mathbb{N}$ tel que $(p,q)\in J\}$ est fini donc majoré par un entier Q. On a donc pour tout $(p,q)\in J$, $(p,q)\in[\![1,P]\!]\times[\![1,Q]\!]$.
Puis par positivité des termes $\frac{1}{p^2q^2}$ pour $(p,q)\in[\![1,P]\!]\times[\![1,Q]\!]\setminus J=K$,

$$\sum_{(p,q)\in J}\frac{1}{p^2q^2} = \sum_{(p,q)\in\mathbb{N}_P\times\mathbb{N}_Q}\frac{1}{p^2q^2} - \sum_{(p,q)\in K}\frac{1}{p^2q^2} \leqslant \sum_{(p,q)\in\mathbb{N}_P\times N_Q}\frac{1}{p^2q^2} = \sum_{p=1}^{P}\frac{1}{p^2}\sum_{q=1}^{Q}\frac{1}{q^2} \leqslant \zeta(2)^2$$

Cette majoration est indépendante de J. Donc la famille $\left(\frac{1}{p^2q^2}\right)_{(p,q)\in(\mathbb{N}^*)^2}$ est sommable.

Savoir faire - Montrer qu'une famille n'est pas sommable
Si l'on trouve une suite $(J_n)_{n\in\mathbb{N}}$ de sous-ensembles finis de I tel que $S_n := \sum_{i\in J_n}u_i$ n'est pas majorée, alors nécessairement la suite n'est pas sommable.

Exercice
On cherche à étudier la sommabilité de la famille $\left(\frac{1}{p^2+q^2}\right)_{(p,q)\in(\mathbb{N}^*)^2}$

1. Par une comparaison série-intégrale, montrer que
$$\sum_{q=1}^{Q}\frac{1}{p^2+q^2} \geqslant \frac{1}{p}\left(\arctan\frac{Q+1}{p} - \arctan\frac{1}{p}\right)$$
2. Montrer alors que la suite $\left(\sum_{p=1}^{n}\sum_{q=1}^{2p-1}\frac{1}{p^2+q^2}\right)_n$ n'est pas majorée.
3. Conclure

Correction

1. Soit $p\in\mathbb{N}^*$. Soit $Q\in\mathbb{N}$. $t\mapsto\frac{1}{p^2+t^2}$ est décroissante sur $\mathbb{R}$ donc sur $[q,q+1]$, $\frac{1}{p^2+q^2}\geqslant\int_q^{q+1}\frac{\mathrm{d}t}{p^2+t^2}$, puis en sommant (relation de Chasles) :
$$\sum_{q=1}^{Q}\frac{1}{p^2+q^2}\geqslant\int_1^{Q+1}\frac{\mathrm{d}t}{p^2+t^2} = \frac{1}{p}\left[\arctan\frac{t}{p}\right]_1^{Q+1} = \frac{1}{p}\left(\arctan\frac{Q+1}{p}-\arctan\frac{1}{p}\right)$$
2. Soit $n\in\mathbb{N}^*$. Considérons alors $Q=2p-1$, on trouve
$$\sum_{p=1}^{n}\left(\sum_{q=1}^{2p-1}\frac{1}{p^2+q^2}\right)\geqslant\sum_{p=1}^{n}\frac{1}{p}\underbrace{\arctan 2-\arctan 1}_{:=A} = nA$$
Donc la suite $\left(\sum_{p=1}^{n}\sum_{q=1}^{2p-1}\frac{1}{p^2+q^2}\right)_n$ n'est pas majorée.

3. La famille $\{\sum_{(p,q)\in J}\frac{1}{p^2+q^2}, J\in\mathscr{P}_f((\mathbb{N}^*)^2)\}$ n'est donc pas majorée.
   La famille $\left(\frac{1}{p^2+q^2}\right)_{(p,q)\in(\mathbb{N}^*)^2}$ n'est pas sommable.

2.4. Comparaisons

Proposition - Comparaison des ensembles
Soit $(\alpha_i)_{i\in I}\in\mathbb{R}_+^I$, une famille de réels positifs.
Supposons que $(\alpha_i)_{i\in I}$ est une famille sommable
Soit $I'\subset I$.
Alors $(\alpha_i)_{i\in I'}$ est une famille sommable et $\sum_{i\in I'}\alpha_i\leqslant\sum_{i\in I}\alpha_i$.

Démonstration
Soit $J'\in\mathscr{P}_f(I')$, alors $J'\subset I'\subset I$, donc $J'\in\mathscr{P}_f(I)$.
Comme $(\alpha_i)_{i\in I}$ est une famille est sommable :

$$\sum_{i\in J'}\alpha_i\leqslant\sum_{i\in I}\alpha_i$$

Donc $(\alpha_i)_{i\in I'}$ est une famille est sommable et $\sum_{i\in I'}\alpha_i\leqslant\sum_{i\in I}\alpha_i$. □

Proposition - Comparaison de termes
Soit $(\alpha_i)_{i\in I}\in\mathbb{R}_+^I$, une famille de réels positifs.
Soit $(\beta_i)_{i\in I}\in\mathbb{R}_+^I$, une autre famille de réels positifs tels que : $\forall\, i\in I$, $(0\leqslant)\beta_i\leqslant\alpha_i$.
• Si $(\alpha_i)_{i\in I}$ est une famille est sommable, alors $(\beta_i)_{i\in I}$ est une famille est sommable.
Et $\sum_{i\in I}\beta_i\leqslant\sum_{i\in I}\alpha_i$.
• Si $(\beta_i)_{i\in I}$ n'est pas une famille sommable, alors $(\alpha_i)_{i\in I}$ n'est pas une famille sommable (contraposée).
Et $\sum_{i\in I}\beta_i=\sum_{i\in I}\alpha_i=+\infty$.

Démonstration
Soit $J\in\mathscr{P}_f(I)$.
Alors par comparaison de somme finie :

$$\sum_{i\in J}\beta_i\leqslant\sum_{i\in J}\alpha_i\leqslant\sum_{i\in I}\alpha_i$$

La seconde majoration étant donnée par sommabilité de (α_i) par définition d'une borne supérieure.
Donc pour tout $J\in\mathscr{P}_f(I)$, $\sum_{i\in J}\beta_i$ est bornée par $\sum_{i\in I}\alpha_i$.
Ainsi $(\beta_i)_{i\in I}$ est une famille est sommable et $\sum_{i\in I}\beta_i$, le plus petit des majorants vérifie : $\sum_{i\in I}\beta_i\leqslant\sum_{i\in I}\alpha_i$.
La seconde partie de la proposition est la contraposition. □

Théorème - I est au plus dénombrable
Si $(\alpha_i)_{i\in I}$ est une famille de réels positifs sommable, alors $I'=\{i\in I\mid\alpha_i>0\}$ est au plus dénombrable.

Remarque - Rappels
On rappelle qu'un ensemble E est dénombrable s'il existe une bijection $\varphi:\mathbb{N}\to E$.
Cette bijection permet d'indexer les éléments de E (i.e. les nommer, mais aussi les ordonner).
On dit qu'un ensemble est au plus dénombrable s'il est dénombrable ou fini.
Il suffit que E s'injecte dans $\mathbb{N}$ pour être au plus dénombrable (i.e : $\exists\,\psi : E\to\mathbb{N}$, injective.

Démonstration
Considérons $(\alpha_i)_{i\in I'}$, une famille de réels positifs sommable. On rappelle que l'ensemble $\mathscr{P}=\{p_1,p_2,\dots\}$ des nombres premiers est infini (et dénombrable).
Soit $n\in\mathbb{N}^*$. Posons $I_n=\{i\in I\mid\alpha_i\geqslant\frac{1}{n}\}$.
Pour $i\in I_n$, $0\leqslant\frac{1}{n}\leqslant\alpha_i$, donc $\sum_{i\in I_n}\frac{1}{n}$ est sommable.
Il est donc nécessaire que I_n soit fini, pour tout $n\in\mathbb{N}$.
Et par ailleurs, on a aussi pour tout entier n : $I_n\subset I_{n+1}$. Notons $C_n=\mathrm{Card}(I_{n+1}\setminus I_n)$.
On peut associer un nombre $p_n^1, p_n^2\dots p_n^{C_n}$, à chacun des n nombres de $I_{n+1}\setminus I_n$.
On a alors

$$I_n=\biguplus_{k=1}^{n-1}(I_{k+1}\setminus I_k)=\biguplus_{k=1}^{n-1}\{p_k^1,\cdots p_k^{C_k}\}$$

Si $i\in I'$, alors il existe un unique $n\in\mathbb{N}$ tel que $i\in I_{n+1}\setminus I_n$. Puis, $\varphi(i)\in\{p_n^1,\cdots p_n^{C_n}\}$.
L'application $\varphi:I\to\mathbb{N}$ est injective. Donc $I'=\bigcup I_n$ est au plus dénombrable (réunion croissante d'ensembles). □

Remarque - Intégration d'une fonction
Il est donc vain d'espérer intégrer une fonction sur un intervalle I de $\mathbb{R}$ (donc non dénombrable) en posant $\int_I f=\sum_{i\in I}f(i)$.

2.5. Sommation par suite croissante d'ensembles

A partir de maintenant, toutes les familles seront indexées par un ensemble au plus dénombrable, on le note D.

Théorème - Critère de sommabilité - Suite croissante de parties
Soit (D_n) une suite croissante de parties de D, de réunion : $D=\bigcup_{n\in\mathbb{N}}D_n$.
On note : Soit $(u_d)_{d\in D}\in\mathbb{R}_+^D$, une famille de réels positifs.
(u_d) est sommable si et seulement si :

1. Pour tout $n\in\mathbb{N}$, $(u_d)_{d\in D_n}$ est sommable
2. $\left(\sum_{d\in D_n}u_d\right)_{n\in\mathbb{N}}$ est une suite convergente (ici croissante majorée).

Si tel est le cas, alors on a : $\sum_{d\in D}u_d=\lim_{n\to+\infty}\sum_{d\in D_n}u_d$.

Remarque - D_n fini?
Si il est possible que pour tout $n\in\mathbb{N}$, D_n est fini ; il est également tout à fait possible que pour tout $n\in\mathbb{N}$, D_n n'est pas fini… Dans le premier cas, on en tire un savoir-faire.

Démonstration
Notons d'abord que pour tout $n\in\mathbb{N}$, $D_n\subset D_{n+1}\subset D$.
• Supposons $(u_d)_{d\in D}$ sommable.
Soit $n\in\mathbb{N}$. $(u_d)_{d\in D_n}$ est sommable d'après la proposition comparaison des ensembles et car $D_n\subset D$.
et par ailleurs : $\sum_{d\in D_n}u_d\leqslant\sum_{d\in D_{n+1}}u_d\leqslant\sum_{d\in D}u_d$.
Ainsi, la suite $\left(\sum_{d\in D_n}u_d\right)_{n\in\mathbb{N}}$ est croissante majorée et donc convergente et $\lim_{n\to+\infty}\sum_{d\in D_n}u_d\leqslant\sum_{d\in D}u_d$.
• Supposons que pour tout $n\in\mathbb{N}$, $(u_d)_{d\in D_n}$ est sommable et $(\sum_{d\in D_n}u_d$ est une suite convergente.
Soit $J\in\mathscr{P}_f(D)$. J est fini de cardinal N, notons $i_1,\dots i_N$ les éléments de J.
Pour tout $j\in\mathbb{N}_N$, $i_j\in D$, donc il existe $n(j)$ tel que $i_j\in D_{n(j)}$.
Notons $R=\max(N(1),\dots N(j))$, alors pour tout $j\in\mathbb{N}_N$, $i_j\subset D_{N(j)}\subset D_R$ par croissance de

(D_n).
Et ainsi $J \subset D_R$.
Mais la suite (u_d) est sommable sur D_R, donc

$$\sum_{d\in J} u_d \leqslant \sum_{d\in D_R} u_d \leqslant \lim_{n\to+\infty} \sum_{d\in D_n} u_d$$

par croissance de la suite $\left(\sum_{d\in D_n} u_d\right)_n$.
Ainsi la famille $(u_d)_{d\in D}$ est sommable et $\sum_{d\in D} u_d \leqslant \lim_{n\to+\infty} \sum_{d\in D_n} u_d$. □

Savoir faire - Construire une suite croissance d'ensembles finis

Une stratégie classique consiste, dans le cas où D est dénombrable sans être fini à considérer : $\sigma : \mathbb{N} \to D$, une bijection.
Puis pour tout $n \in \mathbb{N}$, on considère $D_n = \sigma([\![0, n]\!])$. On a $D = \bigcup_{n\in\mathbb{N}} D_n$.

Savoir faire - Exploitation d'une suite croissante d'ensembles finis

Si $(D_n)_n$ est une suite croissante d'ensembles finis d'union D.
Alors toutes les sommes $S_n := \sum_{d\in D_n} u_d$ sont finies et la suite (S_n) est croissante.
La convergence de S_n est équivalente à la sommabilité de (u_d) sur D.
Et on a $\lim(S_n) = \sup S_n = \sum_{d\in D} u_d$.

Proposition - Invariance de la sommabilité et de la somme par permutation des indices

Soient D et D' deux ensembles au plus dénombrables.
Soit $(u_d)_{d\in D} \in (\mathbb{R}_+)^D$. S'il exite une bijection $\sigma : D' \to D$,
alors $(u_d)_{d\in D}$ est sommable $\iff (u_{\sigma(d')})_{d'\in D'}$ est sommable.
Et en cas de sommabilité $\sum_{d\in D} u_d = \sum_{d'\in D'} u_{\sigma(d')}$

Démonstration
Supposons (u_d) est sommable et considérons la bijection $\sigma : D \to D'$.
Soit $J' \in \mathscr{P}_f(D')$. Alors $\sigma(J') \in \mathscr{P}_d(D)$.
Donc $\sum_{i\in J'} u_{\sigma(i)} = \sum_{d\in\sigma(J')} u_d \leqslant \sum_{d\in D} u_d$, indépendant de J'.
Donc $(u_{\sigma(d')})_{d'\in D'}$ est sommable et $\sum_{d'\in D'} u_{\sigma(d')} \leqslant \sum_{d\in D} u_d$.
L'équivalence est assurée en considérant $\sigma^{-1} : D \to D'$ et cela donne l'inégalité réciproque.
On a donc bien l'équivalence des sommabilités et l'égalité : $\sum_{d\in D} u_d = \sum_{d'\in D'} u_{\sigma(d')}$ □

Application - Série à termes positifs

Si $\sum_{n\geqslant 0} u_n$ est un série, à termes positifs, convergente, alors $(u_n)_{n\in\mathbb{N}}$ est sommable.
Et donc pour tout $\sigma \in S_{\mathbb{N}}$, la série $\sum_{n\geqslant 0} u_{\sigma(n)}$ converge.
Puis $\sum_{n=0}^{+\infty} u_n = \sum_{n\in\mathbb{N}} u_n = \sum_{n\in\mathbb{N}} u_{\sigma(n)} = \sum_{n=0}^{+\infty} u_{\sigma(n)}$.

Proposition - Sommabilité d'une combinaison linéaire

Soit D, un ensemble au plus dénombrable.
Soient $(u_d)_{d\in D}$ et $(v_d)_{d\in D} \in (\mathbb{R}_+)^D$ deux familles de réels positifs, sommables.
Alors $(u_d + v_d)_{d\in D}$ et $\forall\, \lambda \in \mathbb{R}_+$, $(\lambda u_d)_{d\in D}$ sont sommables.
Et $\sum_{d\in D} (u_d + v_d) = \sum_{d\in D} u_d + \sum_{d\in D} v_d$ et $\sum_{d\in D} \lambda u_d = \lambda \sum_{d\in D} u_d$.

Démonstration
On suppose que D est dénombrable sans être fini.
Soit $\sigma : \mathbb{N} \to D$, une bijection.
Posons pour tout $n \in \mathbb{N}$, $D_n = \sigma([\![0, n]\!])$. On a $D = \bigcup_{n\in\mathbb{N}} D_n$.
On exploite alors le critère de sommabilité pour suite croissance de sous-ensemble.
• Pour tout $n \in \mathbb{N}$, D_n est fini, donc $(u_d + v_d)_{d\in D_n}$ et $(\lambda u_d)_{d\in D_n}$ sont sommables.
• $\sum_{d\in D_n} u_d + v_d = \sum_{d\in D_n} u_d + \sum_{d\in D_n} v_d \longrightarrow \sum_{d\in D} u_d + \sum_{d\in D} v_d$.
$\sum_{d\in D_n} \lambda u_d = \lambda \sum_{d\in D_n} u_d \longrightarrow \lambda \sum_{d\in D} u_d$.
□

2.6. Sommation par paquets et théorème de Fubini

Remarque - Rappel : sommation finie par paquets

On suppose que I (fini) s'écrit $I = \biguplus_{k=1}^{n} A_k$.
Alors $\sum_{i\in I} a_i = \sum_{k=1}^{n} \left(\sum_{i\in A_k} a_i\right)$.

Théorème - Sommation par paquets

Soit $(P_i)_{i\in I}$ une partition de D (i.e. $D = \biguplus_{i\in I} P_i$).
Soit $(u_d) \in (\mathbb{R}_+)^D$.
$(u_d)_{d\in D}$ est sommable si et seulement si

$$\begin{cases} \forall\, i \in I,\ (u_d)_{d\in P_i} \text{ est sommable,} \\ \text{puis la famille } \left(\sum_{d\in P_i} u_d\right)_{i\in I} \in (\mathbb{R}_+)^I \text{ est sommable} \end{cases}$$

Dans ce cas, on a alors : $\sum_{d\in D} u_d = \sum_{i\in I} \left(\sum_{d\in P_i} u_d\right)$.

Remarque - I au plus dénombrable

Notons que I est au plus dénombrable. Il peut être fini, même si D est dénombrable.

Démonstration
Notons que toutes les réunions qui vont suivre sont disjointes.
• Supposons que $(u_d)_{d\in D}$ est sommable.
Soit $i \in I$. Comme $P_i \subset D$, on a : la famille $(u_d)_{d\in P_i}$ est sommable.
On définit alors $s_i = \sum_{d\in P_i} u_d$. Soit $J \in \mathscr{P}_f(I)$. On doit démontrer que $\sum_{i\in J} s_i$ est majorée.
$D' = \biguplus_{i\in J} P_i$ est une partie de D.
Considérons, pour tout $i \in J$, Pf_i, une partie finie de P_i.
Alors (sommes finies + positivité) :

$$\sum_{i\in J} \left(\sum_{d\in Pf_i} u_d\right) = \sum_{d\in\bigcup_{i\in J} Pf_i} u_d \leqslant \sum_{d\in D} u_d$$

En passant à la borne supérieure (un nombre fini de fois) pour chaque i de J :

$$\sum_{i\in J} s_i = \sum_{i\in J} \left(\sum_{d\in P_i} u_d\right) \leqslant \sum_{d\in D} u_d$$

Donc $(s_i)_{i\in I}$ est sommable et $\sum_{i\in I} s_i \leqslant \sum_{d\in D} u_d$.
• Réciproquement.
Soit $J \in \mathscr{P}_f(D)$. Notons, pour tout $i \in I$, $Pf_i = J \cap P_i$.
On a donc $J = \bigcup_{i\in I} Pf_i$.
Soit $I_0 = \{i \in I \mid Pf_i \neq \emptyset\}$ est un ensemble fini, sinon, $J = \bigcup_{i\in J} Pf_i = \bigcup_{i\in I_0} Pf_i$ serait infini.
Pour tout $i \in I$, $Pf_i \subset J$, donc Pf_i est fini et on a donc $J = \biguplus_{i\in I_0} Pf_i$, réunion disjointe.
Ainsi, par positivité des termes

$$\sum_{d\in J} u_d = \sum_{d\in\bigcup_{i\in I_0} Pf_i} = \sum_{i\in I_0} \left(\sum_{d\in Pf_i} u_d\right) \leqslant \sum_{i\in I_0} s_i \leqslant \sum_{i\in I} \left(\sum_{d\in P_i} u_d\right)$$

Donc $(u_d)_{d\in D}$ est sommable et $\sum_{d\in D} u_d \leqslant \sum_{i\in I} s_i$ □

Remarque - Avec l'ordre sur $\mathbb{N}$

Si la partition est directement indexée par $\mathbb{N}$ (ou une partie finie), i.e $I \subset \mathbb{N}$, alors on peut profiter de la relation d'ordre induite et considérer $D_k = \bigcup_{i=0}^{k} P_i$, on a alors (D_k) suite croissante convergent vers D.

On peut alors exploiter directement le théorème de suites croissantes d'ensemble.

Savoir faire - Application du théorème de sommation par paquets avec $I = \mathbb{N}$

Si $D = \biguplus_{n\in\mathbb{N}} P_n$.

$(u_d)_{d\in D} \in (\mathbb{R}_+)^D$ est sommable si et seulement si :

1. Pour tout $n \in \mathbb{N}$, $(u_d)_{d\in P_n}$ est sommable,
2. puis $\sum_{n\geqslant 0}\left(\sum_{d\in P_n} u_d\right)$ converge (série à termes positifs).

Et dans ce cas : $\sum_{d\in D} u_d = \sum_{n=0}^{+\infty}\sum_{d\in P_n} u_d$.

Exemple - Sommabilité de $\left(\frac{1}{(p+q)^\alpha}\right)_{(p,q)\in(\mathbb{N}^*)^2}$

On a $(\mathbb{N}^*)^2 = \bigcup_{n\in\mathbb{N}\setminus\{0,1\}} \underbrace{\{(p,q)\in\mathbb{N}^2 \mid p+q=n\}}_{P_n}$.

Soit $n \in \mathbb{N}$ et $n \geqslant 2$, $P_n = \{(n-1,1),(n-2,2),\dots(1,n-1)\}$, donc P_n est fini.

Ainsi $\left(\frac{1}{(p+q)^\alpha}\right)_{(p,q)\in P_n}$ est sommable.

Et par ailleurs, $s_n = \sum_{(p,q)\in P_n} \frac{1}{n^\alpha} = \frac{\text{card}(P_n)}{n^\alpha} = \frac{n-1}{n^\alpha}$.

Puis $s_n \sim \frac{1}{n^{\alpha-1}}$, donc $\sum_{n\geqslant 2} s_n$ converge ssi $\alpha - 1 > 1$, i.e. $\alpha > 2$.

Il y a équivalence, donc la famille $\left(\frac{1}{(p+q)^\alpha}\right)_{(p,q)\in(\mathbb{N}^*)^2}$ est sommable ssi $\alpha > 2$.

Et dans ce cas :

$$\sum_{(p,q)\in(\mathbb{N}^*)^2} \frac{1}{(p+q)^\alpha} = \sum_{n=2}^{+\infty} \frac{n}{n^\alpha} - \frac{1}{n^\alpha} = \zeta(\alpha-1) - \zeta(\alpha)$$

Le théorème suivant apparait alors comme un corollaire :

Théorème - Fubini - suites doubles positifs indexées sur $\mathbb{N}^2$

Considérons une suite doublement indexée de réels positifs $(u_{p,q})_{(p,q)\in\mathbb{N}^2}$.

$(u_{p,q})_{(p,q)\in\mathbb{N}^2}$ est sommable si et seulement si

1. pour tout $p \in \mathbb{N}$, la série $\sum_{q\geqslant 0} u_{p,q}$ converge
2. puis la série $\sum_{p\geqslant 0}\left(\sum_{q=0}^{+\infty} u_{p,q}\right)$ converge

ou bien, si et seulement si

1. pour tout $q \in \mathbb{N}$, la série $\sum_{p\geqslant 0} u_{p,q}$ converge
2. puis la série $\sum_{q\geqslant 0}\left(\sum_{p=0}^{+\infty} u_{p,q}\right)$ converge

On a alors

$$\sum_{(p,q)\in\mathbb{N}^2} u_{p,q} = \sum_{p=0}^{+\infty}\left(\sum_{q=0}^{+\infty} u_{p,q}\right) = \sum_{q=0}^{+\infty}\left(\sum_{p=0}^{+\infty} u_{p,q}\right) = \sum_{n=0}^{+\infty}\left(\sum_{p+q=n} u_{p,q}\right)$$

Remarque - Indice de la somme

Evidemment, le résultat s'adapte (comme dans l'exemple précédent), en prenant une partie de $\mathbb{N}^2$ qui ne « commencent » pas en $(0,0)$…

Démonstration

On exploite le théorème de sommation par paquets, en notant que

$$\mathbb{N}^2 = \biguplus_{p\in\mathbb{N}} (\{p\}\times\mathbb{N}) = \biguplus_{q\in\mathbb{N}} (\mathbb{N}\times\{q\}) = \biguplus_{n\in\mathbb{N}} \{(p,q) \mid p+q=n\}$$

□

Exercice

1. Etudier la sommabilité de $\left(\frac{1}{(pq)^\alpha}\right)_{(p,q)\in(\mathbb{N}^*)^2}$.
   Dans le cas sommable, donner la valeur de la somme.
2. Si on note $d(n)$, le nombre de diviseurs de n, montrer alors que cette somme vaut $\sum_{n=1} \frac{d(n)}{n^\alpha}$.

Correction

1. Soit $p \in \mathbb{N}^*$. La somme $\sum_{q\geqslant 1} \frac{1}{(pq)^\alpha} = \frac{1}{p^\alpha}\sum_{q\geqslant 1}\frac{1}{q^\alpha}$.
   Cette série converge ssi $\alpha > 1$ de somme $\frac{\zeta(\alpha)}{p^\alpha}$.
   Puis, la série $\sum_{p\geqslant 1}\frac{\zeta(\alpha)}{p^\alpha}$ converge ssi $\alpha > 1$ et sa limite est $\zeta(\alpha)^2$. Si $\alpha < 1$, la somme diverge (par positivité, et parce qu'une sous-somme diverge).
2. On peut aussi noter que $(\mathbb{N}^*)^2 = \biguplus_{n\in\mathbb{N}^*} \{(p,q)\in(\mathbb{N}^*)^2 \mid pq = n\}$.
   On a alors, pour $n \in \mathbb{N}^*$ fixé, une somme finie : $\sum_{pq=n} \frac{1}{(pq)^\alpha} = \frac{1}{n^\alpha}\sum_{p\mid n} 1 = \frac{d(n)}{n^\alpha}$.
   Ainsi, dans le cas convergent (i.e. $\alpha > 1$) : $\sum_{n=1}^{+\infty} \frac{d(n)}{n^\alpha} = \left(\zeta(\alpha)\right)^2$.

Théorème - Fubini - suites doubles positifs indexées sur un produit cartésien

Considérons une suite doublement indexée de réels positifs $(u_{d,d'})_{(d,d')\in D\times D'}$.

$(u_{d,d'})_{(d,d')\in D\times D'}$ est sommable si et seulement si

1. pour tout $d \in D$, la famille $(u_{d,d'})_{d'\in D'}$ est sommable de somme s_d
2. puis la famille $(s_d)_{d\in D}$ est sommable.

ou bien, si et seulement si

1. pour tout $d' \in D'$, la famille $(u_{d,d'})_{d\in D}$ est sommable de somme $s_{d'}$
2. puis la famille $(s_{d'})_{d'\in D'}$ est sommable.

On a alors

$$\sum_{(d,d')\in D\times D'} u_{d,d'} = \sum_{d\in D}\left(\sum_{d'\in D'} u_{d,d'}\right) = \sum_{d'\in D'}\left(\sum_{d\in D} u_{d,d'}\right)$$

Démonstration

On considère les partitions $D\times D' = \biguplus_{d\in D}\{d\}\times D' = \biguplus_{d'\in D'} D\times\{d'\}$.

□

Corollaire - Produit
Si $(u_d)_{d\in D} \in (\mathbb{R}_+)^D$ et $(v_{d'})_{d'\in D'} \in (\mathbb{R}_+)^{D'}$ sont deux familles sommables, alors $(u_d v_{d'})_{(d,d')\in D\times D'}$ est sommable. Et

$$\sum_{(d,d')\in D\times D'} u_d v_{d'} = \sum_{d\in D} u_d \times \sum_{d'\in D'} v_{d'}$$

Démonstration
On note pour tout $(d,d') \in D\times D'$, $a_{d,d'} = u_d v_{d'}$.
On fixe d dans D, la famille $(a_{d,d'})_{d'\in D'} = u_d (v_{d'})_{d'\in D'}$ est sommable.
Et $s_d := \sum_{d\in D'} a_{d,d'} = u_d \sum_{d\in D'} v_{d'}$ est sommable car $(u_d)_{d\in D}$ sommable.
On peut appliquer le théorème de Fubini.
On a alors $\sum_{(d,d')\in D\times D'} a_{d,d'} = \sum_{d\in D} u_d \times \sum_{d'\in D'} v_{d'}$. □

Remarque - La réciproque est fausse
Par exemple avec $u_n = 0$ et $v_n = \dfrac{1}{n+1}$.
Mais si les familles sont à valeurs dans $\mathbb{R}_+^*$, alors la réciproque devient vraie

2.7. Enoncé dans $\overline{\mathbb{R}_+} = [0,+\infty]$

Remarque - Convention
Soit $(u_d)_{d\in D}$ une famille d'éléments de $\overline{R_+}$.
On note par convention $\sum_{d\in D} u_d = +\infty$ si il existe $d \in D$ tel que $u_d = \infty$, ou si $(u_d)_{d\in D}$ n'est pas sommable.

Théorème - Sommation par paquets dans $\mathbb{R}_+$ - cas général
Soit $(P_i)_{i\in I}$ une partition de l'ensemble D (i.e. $D = \biguplus_{i\in I} P_i$).
Pour toute famille $(u_d)_{d\in D} \in (\mathbb{R}_+)^D$, on a :

$$\sum_{d\in D} u_d = \sum_{i\in I}\left(\sum_{d\in P_i} u_d\right) \quad \text{(égalité dans } \overline{\mathbb{R}}\text{)}$$

que la famille $(u_d)_{d\in D}$ soit sommable ou non (fini ou non).

Démonstration
• Si $(u_d)_{d\in D}$ est sommable, l'égalité est vraie. C'est le théorème de sommation par paquets.
• Si $(u_d)_{d\in D}$ est non sommable i.e. $\sum_{d\in D} u_d = +\infty$. Deux options :

1. $\exists\, i \in I$ tel que $\sum_{d\in P_i} u_d = +\infty$.
   Alors $\sum_{i\in I}\left(\sum_{d\in P_i} u_d\right) = +\infty = \sum_{d\in D} u_d$.
2. $\forall\, i \in I$, $\sum_{d\in P_i} u_d < +\infty$, i.e. $(u_d)_{d\in P_i}$ est sommable.
   Alors, par l'absurde, $\left(\sum_{d\in P_i} u_d\right)_{i\in I}$ n'est pas sommable, sinon $(u_d)_{d\in D}$ serait sommable.
   Et donc $\sum_{i\in I}\left(\sum_{d\in P_i} u_d\right) = +\infty = \sum_{d\in D} u_d$.

□

Savoir faire - Etude d'une famille sommable
On se place dans $\overline{\mathbb{R}}$, on peut donc calculer d'abord la somme.
(Si besoin, on ajoute : « sous réserve de convergence »).

Et on tire la conclusion selon la valeur de la somme : $S \in \mathbb{R}_+$ ou $S = +\infty$.
Les méthodes s'adaptent.

3. Familles complexes sommables

3.1. Définition

On considère des nombres à valeurs dans le corps $\mathbb{K} = \mathbb{C}$ ou $\mathbb{R}$ (total!).
On suppose également que D (ensemble des indices) est un ensemble au plus dénombrable, non vide.

Pour aller plus loin - Autre option ?
On peut poser comme définition : $(z_d)_{d\in D}$ est sommable si il existe $S \in \mathbb{C}$ tel que $\forall\, \epsilon > 0$, $\exists\, B \in \mathscr{P}_f(D)$ tel que $|S - \sum_{d\in D} z_d| \leqslant \epsilon$.
Ces deux définitions sont-elles équivalentes?

Définition - Famille complexe sommable
Une famille $(z_d)_{d\in D} \in \mathbb{K}^D$ est dite sommable si la famille de réels positifs $(|z_d|)_{d\in D}$ est sommable.
On note $\ell^1(D,\mathbb{K})$, l'ensemble des familles sommables indexées sur D et à valeurs dans $\mathbb{K}$.

Application - Cas des suites indexées sur $\mathbb{N}$
$(z_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ est sommable ssi $\sum_{n\geqslant 0} |z_n|$ converge.

Exemple - Famille non sommable et série (semi-)convergente
$\left(\dfrac{(-1)^k}{k}\right)_{k\in\mathbb{N}^*} \notin \ell^1(\mathbb{N}^*,\mathbb{R})$, bien que la série $\sum_{k\geqslant 1} \dfrac{(-1)^k}{k}$ converge.

Savoir faire - Montrer la sommabilité d'une famille de réels ou de complexes
On montre la sommabilité de la famille des valeurs absolues, respectivement modules.
On commence donc toujours par considérer $(|z_d|)_{d\in D}$.

Exercice
Soit $z \in \mathbb{C}$ tel que $|z| < 1$. Etudier la sommabilité de $(z^{pq})_{(p,q)\in(\mathbb{N}^*)^2}$.

Correction
Soit $p \in \mathbb{N}^*$, la série $\sum_{q\geqslant 1} |z^{pq}| = \sum_{q\geqslant 1} (|z|^p)^q$ est convergente de somme $S_p := \sum_{q=1}^{+\infty} |z^{pq}| = \dfrac{|z|^p}{1-|z|^p}$.
Puis $S_p \sim_{p\to\infty} |z|^p$, et la série $\sum_{p\geqslant 1} |z|^p$ converge. Donc $(S_p)_{p\in\mathbb{N}^*}$ est sommable et donc $(z^{pq})_{(p,q)\in(\mathbb{N}^*)^2}$ est une famille complexe sommable.

3.2. Critère de sommabilité et calcul de somme

Remarque - Rappels
Pour les encadrements (voire les équivalences), on exploite souvent les relations :
— Si $x \in \mathbb{R}$: $|x| = \max(x,-x) (\geqslant 0)$, $x^+ := \max(x,0) = x\mathbb{1}_{x\geqslant 0} (\geqslant 0)$ et $x^- := \max(0,-x) = -x\mathbb{1}_{x\leqslant 0} (\geqslant 0)$.
On a alors $|x| = x^+ + x^-$, $x = x^+ - x^-$ et les équivalences : $x \geqslant 0 \Leftrightarrow x^- = 0 \Leftrightarrow x = x^+$ et $x \leqslant 0 \Leftrightarrow x^+ = 0 \Leftrightarrow x = x^-$
— Si $z \in \mathbb{C}$, $z = \mathrm{Re}(z) + i\mathrm{Im}(z)$, et les équivalence
$z \in \mathbb{R} \Leftrightarrow \mathrm{Im}(z) = 0 \Leftrightarrow z = \mathrm{Re}(z)$ et $z \in i\mathbb{R} \Leftrightarrow \mathrm{Re}(z) = 0 \Leftrightarrow z = \mathrm{Im}(z)$.
On peut donc couper z en l'addition de 4 nombres réels positifs (dont deux multipliés par i).
Et $\left.\begin{matrix}\mathrm{Re}(z)\\ \mathrm{Im}(z)\end{matrix}\right\} \leqslant |z| = \sqrt{\mathrm{Re}^2(z)+\mathrm{Im}^2(z)} \leqslant \mathrm{Re}(z)+\mathrm{Im}(z)$.

Savoir faire - Décomposition en « morceaux »
$(x_d) \in (\mathbb{R})^D$ est sommable $\Longleftrightarrow$ $(x_d^+)_{d\in D}$ et $(x_d^-)_{d\in D}$ sont sommables.
$(z_d) \in (\mathbb{C})^D$ est sommable $\Longleftrightarrow$ $(\mathrm{Re}(z_d))_{d\in D}$ et $(\mathrm{Im}(z_d))_{d\in D}$ sont sommables.

Proposition - Critères de sommabilité
Soient $(x_d)_{d\in D} \in (\mathbb{R}_+)^D$ et $(z_d)_{d\in D} \in \mathbb{C}^D$, deux familles.
Si on a $\forall\, d \in D, |z_d| \leqslant x_d$ et $(x_d)_{d\in D}$ sommable,
alors $(z_d)_{d\in D}$ sommable.

Ce qui se convertit en un second savoir-faire qu'on exploite très fréquemment (une condition suffisante, seulement) :

Savoir faire - Sommabilité par majoration
$\forall\, d \in D, |z_d| \leqslant x_d$ et $(x_d)_{d\in D}$ sommable $\Longrightarrow (z_d)_{d\in D}$ est sommable.

Démonstration
Par comparaison, $|z_d| \leqslant x_d$, donc $(|z_d|)_{d\in D}$ est sommable, et donc $(z_d)_{d\in D}$ est sommable. □

Définition - Somme d'une famille sommable
Soit $(x_d)_{d\in D} \in \ell^1(D,\mathbb{R})$ une famille de réels, sommable.
On pose alors $\displaystyle\sum_{d\in D} x_d = \sum_{d\in D} x_d^+ - \sum_{d\in D} x_d^-$.
Soit $(z_d)_{d\in D} \in \ell^1(D,\mathbb{C})$ une famille de complexes, sommable.
On pose alors

$$\begin{aligned}\sum_{d\in D} z_d &= \sum_{d\in D} \mathrm{Re}(z_d) + i\sum_{d\in D} \mathrm{Im}(z_d)\\ &= \sum_{d\in D} \mathrm{Re}(z_d)^+ - \sum_{d\in D} \mathrm{Re}(z_d)^- + i\sum_{d\in D} \mathrm{Im}(z_d)^+ - i\sum_{d\in D} \mathrm{Im}(z_d)^-\end{aligned}$$

Remarque - Elargissement
Ces définitions élargissent bien les définitions précédentes.

3.3. Espace vectoriel $\ell^1(D,\mathbb{K})$

Remarque - Addition
On a vu que si $(a_d)_{d\in\mathbb{D}}$ et $(b_d)_{d\in\mathbb{D}}$ sont positifs et sommables et $\lambda > 0$, alors $(\lambda a_d + \mu b_d)_{d\in D}$ est sommable. Et $\displaystyle\sum_{d\in D} \lambda a_d + \mu b_d = \lambda \sum_{d\in D} a_d + \mu \sum_{d\in D} b_d$.
Qu'en est-il si $\mu < 0$ ou (a_d) pas toujours positif?

Application - Montrer que $\displaystyle\sum_{d\in D} (a_d - b_d) = \sum_{d\in D} a_d - \sum_{d\in D} b_d$ (avec $a_d, b_d \in \mathbb{R}$)
Soit $(a_d)_{d\in D}$ et $(b_d)_{d\in D}$ deux familles de réels, sommables.
$|a_d - b_d| \leqslant |a_d| + |b_d|$. Donc $(a_d - b_d)$ est sommable.
Notons $D^+ = \{d \in D \mid a_d \geqslant b_d\}$ et $D^- = \{d \in D \mid a_d \leqslant b_d\}$.
On a pour $d \in D^+$,
$(a_d - b_d)^+ = a_d - b_d = (a_d^+ - a_d^-) - (b_d^+ - b_d^-) = (a_d^+ + b_d^-) - (a_d^- + b_d^+)$.
$(a_d - b_d)^- = 0$ Ainsi, $(a_d^- + b_d^+) + (a_d - b_d)^+ = (a_d^+ + b_d^-)$. Tout est positif.
Donc $\displaystyle\sum_{d\in D^+} \left((a_d^- + b_d^+) + (a_d - b_d)^+\right) = \sum_{d\in D^+} (a_d^+ + b_d^-)$,
et $\displaystyle\sum_{d\in D^+} (a_d - b_d)^+ = \sum_{d\in D^+} (a_d^+ + b_d^-) - \sum_{d\in D^+} (a_d^- + b_d^+)$
$\displaystyle= \sum_{d\in D^+} a_d^+ - \sum_{d\in D^+} a_d^- - \sum_{d\in D^+} b_d^+ + \sum_{d\in D^+} b_d^-$.
On a pour $d \in D^-$,
$(a_d - b_d)^- = b_d - a_d = (a_d^- + b_d^+) - (a_d^+ + b_d^-)$.
$(a_d - b_d)^+ = 0$ Ainsi, $(a_d^+ + b_d^-) + (a_d - b_d)^- = (a_d^- + b_d^+)$. Tout est positif.
Donc $\displaystyle\sum_{d\in D^-} \left((a_d^+ + b_d^-) + (a_d - b_d)^-\right) = \sum_{d\in D^+} (a_d^- + b_d^+)$,

et $\displaystyle\sum_{d\in D^-} (a_d - b_d)^- = \sum_{d\in D^-} (a_d^- + b_d^+) - \sum_{d\in D^-} (a_d^+ + b_d^-)$
$\displaystyle= -\sum_{d\in D^-} a_d^+ + \sum_{d\in D^-} a_d^- + \sum_{d\in D^-} b_d^+ - \sum_{d\in D^-} b_d^-$.
Enfin, comme $D = D^+ \uplus D^-$, on trouve :

$$\begin{aligned}\sum_{d\in D} a_d - b_d &= \sum_{d\in D^+} (a_d - b_d)^+ - \sum_{d\in D^-} (a_d - b_d)^-\\ &= \left(\sum_{d\in D^+} a_d^+ - \sum_{d\in D^+} a_d^- - \sum_{d\in D^+} b_d^+ + \sum_{d\in D^+} b_d^-\right) + \left(\sum_{d\in D^-} a_d^+ - \sum_{d\in D^-} a_d^- - \sum_{d\in D^-} b_d^+ + \sum_{d\in D^-} b_d^-\right)\\ &= \sum_{d\in D} (a_d^+ - a_d^-) - \sum_{d\in D} (b_d^+ - b_d^-) = \sum_{d\in D} a_d - \sum_{d\in D} b_d\end{aligned}$$

Proposition - Espace vectoriel
$\ell^1(D,\mathbb{K})$ est un sous-espace vectoriel de $(\mathbb{K}^D, +, \cdot)$.
C'est-à-dire, si $\lambda, \lambda' \in \mathbb{K}$ et $(z_d)_{d\in D}$, $(z'_d)_{d\in D}$ sommables,
alors $(\lambda z_d + \lambda' z'_d)_{d\in D}$ est sommable. Et

$$\sum_{d\in D} \lambda z_d + \lambda' z'_d = \lambda \sum_{d\in D} z_d + \lambda' \sum_{d\in D} z'_d$$

Démonstration
• La famille nulle est sommable, donc $(0)_{d\in D} \in \ell^1(D,\mathbb{K})$.
• Soient $\lambda, \lambda' \in \mathbb{K}$ et $(z_d)_{d\in D}$, $(z'_d)_{d\in D} \in \ell^1(D,\mathbb{K})$.
Alors, pour tout $d \in D$, (inégalité triangulaire) :

$$|\lambda z_d + \lambda' z'_d| \leqslant |\lambda||z_d| + |\lambda'||z'_d|$$

Il s'agit, à droite, d'une famille sommable :
pour tout $J \in \mathscr{P}_f(D)$, la somme $\displaystyle\sum_{d\in J} \left(|\lambda||z_d| + |\lambda'||z'_d|\right)$ est bornée, majorée par $|\lambda| \sum_{d\in D} |z_d| + |\lambda'| \sum_{d\in D} |z'_d|$.
Donc la famille $\left(|\lambda z_d + \lambda' z'_d|\right)_{d\in D}$ est sommable.
ainsi la famille $\left(\lambda z_d + \lambda' z'_d\right)_{d\in D}$ est sommable.
Il reste alors à calculer la somme. Nous le ferons plus loin avec des outils plus efficaces : suite croissante d'ensembles
□

Pour aller plus loin - Et le produit direct?
En fait, il s'agit plutôt du produit scalaire.
On exploite l'inégalité de Cauchy-Schwarz pour tout famille finie $J \subset D$:

$$\sum_{d\in J} |z_d z'_d| \leqslant \sqrt{\sum_{d\in J} |z_d|^2 \sum_{d\in J} |z'_d|^2}$$

Il suffit plutôt donc que $(z_d)_{d\in D}$ et $(z'_d)_{d\in D} \in \ell^2(D,\mathbb{K})$.

3.4. Transfert de propriétés sur $\ell^1(D,\mathbb{K})$

Proposition - Réduction de la famille d'indexation
Si $(z_d)_{d\in D} \in \ell^1(D,\mathbb{K})$ et $D' \subset D$, alors $(z_d)_{d\in D'} \in \ell^1(D',\mathbb{K})$

Démonstration
$(z_d)_{d\in D}$ est sommable, donc $(|z_d|)_{d\in D}$ puis $(|z_d|)_{d\in D'}$ et enfin $(z_d)_{d\in D'}$ sommables. □

Remarque - Comparaison des valeurs des sommes
Cela n'a pas de sens, car ce sont des nombres complexes à ce niveau là…
Notons pour la propriété suivante, qu'il s'agit d'une implication et non d'une équivalence pour démontrer la sommabilité.
Elle donne, en revanche, dès que la sommabilité est assurée, une façon simple de calculer la somme.

Proposition - Suite croissante d'ensembles donnant D
Soit $(z_d)_{d\in D} \in \ell^1(D,\mathbb{K})$. Supposons que $D = \bigcup_{n\in\mathbb{N}} D_n$.
Alors, pour tout $n \in \mathbb{N}$, $(z_d)_{d\in D_n} \in \ell^1(D_n,\mathbb{K})$ et $\displaystyle\sum_{d\in D} z_d = \lim_{n\to+\infty} \sum_{d\in D_n} z_d$.

Démonstration
Encore, une fois : $(z_d)_{d\in D}$ est sommable et donc $\left((\mathrm{Re}(z_n))^+\right)_{d\in D}, ((\mathrm{Re}(z_n))^-)_{d\in D}, \left((\mathrm{Im}(z_n))^+\right)_{d\in D}$ et $((\mathrm{Im}(z_n))^-)_{d\in D}$ sont sommables.
On applique à chacun le résultat vu plus pour les séries à termes positifs.
Donc pour tout $n\in D_n$, ces quatre familles sont sommables sur D_n.
Et par linéarité du passage à la limite :

$$\begin{aligned}\sum_{d\in D} z_d &:= \sum_{d\in D}\mathrm{Re}(z_d)^+ - \sum_{d\in D}\mathrm{Re}(z_d)^- + i\sum_{d\in D}\mathrm{Im}(z_d)^+ - i\sum_{d\in D}\mathrm{Im}(z_d)^-\\ &= \lim_{n\to\infty}\sum_{d\in D_n}\mathrm{Re}(z_d)^+ - \lim_{n\to\infty}\sum_{d\in D_n}\mathrm{Re}(z_d)^- + i\lim_{n\to\infty}\sum_{d\in D_n}\mathrm{Im}(z_d)^+ - i\lim_{n\to\infty}\sum_{d\in D_n}\mathrm{Im}(z_d)^-\\ &= \lim_{n\to\infty}\left(\sum_{d\in D_n}\mathrm{Re}(z_d)^+ - \sum_{d\in D_n}\mathrm{Re}(z_d)^- + i\sum_{d\in D_n}\mathrm{Im}(z_d)^+ - i\sum_{d\in D_n}\mathrm{Im}(z_d)^-\right)\\ &= \lim_{n\to+\infty}\sum_{d\in D_n} z_d\end{aligned}$$

□

Attention - La réciproque est fausse
A bien avoir en tête.
$\mathbb{N}^* = \bigcup_{n\in\mathbb{N}} [\![1,n]\!]$ et $x_k = \dfrac{(-1)^{k-1}}{k}$; pour tout $n\in\mathbb{N}$, la famille $(x_k)_{k\in[\![1,n]\!]}$ est sommable.
Et la somme $\sum_{k\in[\![1,n]\!]} x_k$ admet une limite : $\ln 2\in\mathbb{R}$.
Et pourtant, la famille $(x_k)_{k\in\mathbb{N}^*}$ n'est pas sommable.
Finalement, la réciproque est vraie que pour des familles à valeurs dans $\mathbb{R}_+$, (ou que dans $\mathbb{R}_-\ldots$). La sommabilité est plus exigeante que la convergence… (comme pour les intégrales)

Savoir faire - Utiliser la propriété des suites croissantes d'ensemble pour calculer une somme (1)
On a vu que D était au plus dénombrable.
- Si D est fini, les calculs numériques sont simples.
- Si D est infini, il existe $\varphi:\mathbb{N}\to D$ bijective. On note alors $D_n = \varphi([\![0,n]\!])$
  On a donc $D = \bigcup D_n$ et chaque D_n est fini.
  On exploite alors $\sum_{d\in D} z_d = \lim_{n\to+\infty}\sum_{d\in D_n} z_d$.

Application - Cas d'une somme sur $\mathbb{N}$
En appliquant la proposition précédente, avec la décomposition $\mathbb{N} = \bigcup [\![0,n]\!]$.
Donc $\sum_{n\in\mathbb{N}} z_n = \lim_{n\to+\infty}\sum_{k=0}^{n} z_k = \sum_{k=0}^{+\infty} z_k$.
Ainsi : si $(z_n)\in\ell^1(\mathbb{N},\mathbb{C})$ est une suite complexe sommable i.e $\sum_{n\geqslant 0}|z_n|$ convergente,
alors $\sum_{n\in\mathbb{N}} z_n = \sum_{n=0}^{+\infty} z_n$.

Théorème - Calcul de la somme avec indexation entière
Soit $\sigma : D'\to D$ une bijection. Soit $(z_d)_{d\in D}\in\mathbb{K}^D$.
on a $(z_d)_{d\in D}\in\ell^1(D,\mathbb{K}) \iff (z_{\sigma(d')})_{d'\in D'}\in\ell^1(D',\mathbb{K})$.
En cas de sommabilité, on a $\sum_{d\in D} z_d = \sum_{d'\in D'} z_{\sigma(d')}$.

Corollaire - Version avec $D=\mathbb{N}$
Si $(z_n)\in\mathbb{C}^N$ et si $\sum_{n\in\mathbb{N}} z_n$ est absolument convergente,
Alors pour tout $\sigma\in S_{\mathbb{N}}$, $\sum_{n\in\mathbb{N}} z_{\sigma(n)} = \sum_{n\in\mathbb{N}} z_n = \sum_{n=0}^{+\infty} z_n$.

Démonstration
On a vu le résultat pour les sommes à termes posifis

$$(|z_d|)_{d\in D}\in\ell^1(D,\mathbb{R}_+) \Longleftarrow (|z_{\sigma(d')}|)_{d\in D'}\in\ell^1(D',\mathbb{R}_+)$$

Et on conclut par définition de la sommabilité.
Quant à la valeur de la somme, on exploite la sommation croissante.
D' est au plus dénombrable. Il existe $\varphi:\mathbb{N}\to D'$, bijective (cas non fini).
On a alors $D' = \bigcup D'_n$, où $D'_n = \varphi([\![0,n]\!])$.
Puis, en notant $D_n = \sigma(D'_n)$, on a $D = \bigcup D_n$.
Comme la somme est finie : $\sum_{d\in D_n} z_d = \sum_{d'\in D'_n} z_{\sigma(d')}$.
Enfin, en passant à la limite, on trouve le résultat attendu : $\sum_{d\in D} z_d = \sum_{d'\in D'} z_{\sigma(d')}$ □

On peut compléter le savoir-faire précédent, avec, en plus, un changement de variables.

Savoir faire - Utiliser la propriété des suites croissantes d'ensemble pour calculer une somme (2)
On suppose que D est dénombrable, on reprend $\varphi:\mathbb{N}\to D$ bijective et $D_n = \varphi([\![0,n]\!])$
On a : $\sum_{d\in D} z_d = \lim_{n\to+\infty}\sum_{d\in D_n} z_d = \sum_{n=0}^{+\infty} z_{\varphi(n)}$.

Corollaire - La somme comme une forme linéaire
L'application $\ell^1(D,\mathbb{K})\to\mathbb{K}$, $(z_d)_{d\in D}\mapsto\sum_{d\in D} z_d$ est une forme linéaire.
Et pour tout $(z_d)_{d\in D}\in\ell^1(D,\mathbb{K})$, on a $\left|\sum_{d\in D} z_d\right| \leqslant \sum_{d\in D}|z_d|$.

Démonstration
Soient $\lambda,\lambda'\in\mathbb{C}$, $(z_d),(z'_d)\in\ell^1(D,\mathbb{C})$ deux familles sommables.
Soit $\varphi:N\to D$ et (D_n) tel que $D=\bigcup D_n$ et $D_n=\varphi([\![0,n]\!])$.
Alors pour tout $n\in\mathbb{N}$, la somme étant finie :

$$\sum_{d\in D_n}\lambda z_d+\lambda' z'_d = \sum_{k=0}^{n}\lambda z_{\varphi(k)}+\lambda' z'_{\varphi(k)} = \lambda\sum_{k=0}^{n} z_{\varphi(k)} + \lambda'\sum_{k=0}^{n} z'_{\varphi(k)} = \lambda\sum_{d\in D_n} z_d + \lambda'\sum_{d\in D} z'_d$$

. En passant à la limite, on retrouve le résultat attendu.
De même, on a $\left|\sum_{d\in D_n} z_d\right| \leqslant \sum_{d\in D_n}|z_d|$, puis on passe à la limite. □

3.5. Sommation par paquets et Fubini

Théorème - Sommation par paquets dans $\mathbb{K}$ - cas général
Soit $(P_i)_{i\in I}$ une partition de l'ensemble D.
Soit $(z_d)_{d\in D}\in(\mathbb{K})^D$, on a :
$(z_d)_{d\in D}$ est sommable si et seulement si :

$$\begin{cases}\text{1. Pour tout } i\in I,\ (|z_d)_{d\in P_i} \text{ est sommable, on note } S_i^{va} \text{ sa somme}\\ \text{2. } (S_i^{va})_{i\in I} := \left(\sum_{d\in P_i}|z_d|\right)_{i\in I} \text{ est une famille sommable.}\end{cases}$$

En cas de sommabilité :

$$\sum_{d\in D} z_d = \sum_{i\in I}\left(\sum_{d\in P_i} z_d\right)$$

Démonstration
L'équivalence de sommabilité vient du fait que $(z_d)_{d\in D}$ est sommable si et seulement si $(|z_d|)_{d\in D}$ est sommable.
Puis, on applique le résultat dans $\overline{\mathbb{R}_+}$.
Pour le calcul de $\sum_{d\in D} z_d$.
On la décompose en 4 parties, sachant que (par exemple)

$$\sum_{d\in D} \mathrm{Re}(z_d)^- = \sum_{i\in I}\left(\sum_{d\in D} \mathrm{Re}(z_d)^-\right)$$

On applique ensuite la formule de linéarité d'une somme □

Exercice
Faire la démonstration en démontrant que I est dénombrable donc de la forme $\{i_1,\dots i_n\dots\}$, puis en considérant $D_n = \cup_{i=1}^n P_i$ (réunion disjointe) donc (D_n) est une suite croissante…

Correction

Application - Somme sur $\mathbb{Z}$
Soit $(z_n)_{n\in\mathbb{Z}} \in \mathbb{C}^{\mathbb{Z}}$, une famille définie sur $\mathbb{Z}$.
Alors $(z_n)_{n\in\mathbb{Z}}$ est sommable
$\iff$ $(z_n)_{n\in\mathbb{N}}$ et $(z_n)_{n\in\mathbb{Z}^*_-}$ sont sommables (car $Z = \mathbb{N}\uplus\mathbb{Z}^*_-$).
$\iff$ $(z_n)_{n\in\mathbb{N}}$ et $(z_{-n})_{n\in\mathbb{N}^*}$ sont absolument convergentes
Et en cas de sommabilité $\sum_{n\in\mathbb{Z}} z_n = \sum_{n=0}^{+\infty} z_n + \sum_{n=1}^{+\infty} z_{-n} = z_0 + \sum_{n=0}^{+\infty} z_n + z_{-n}$ On a aussi $\sum_{n\in\mathbb{Z}} z_n = \lim_{n\to+\infty} \sum_{k=-n}^{n} z_k$, car $\mathbb{N} = \cup [\![-n,n]\!]$.

Attention - Pas de sommablité par la somme
Il faut bien s'assurer d'abord de la sommabilité avant le calcul.
La famille $(z_n)_{n\in\mathbb{N}}$ définie par : $\forall\, n\in\mathbb{N}^*$, $z_n = 1$ et $z_{-n} = -1$, et $z_0 = 0$
vérifie $\sum_{k=-n}^{n} z_k = 0$, pour tout $n\in\mathbb{N}$.
Et pourtant cette famille $(z_n)_{n\in\mathbb{N}}$ n'est pas sommable.

Reprenons un calcul précédent :
Exercice
On considère $r\in[0,1[$, $\theta\in[0,2\pi[$ et $z_n = r^n e^{in\theta}$ si $n\leqslant 0$, $z_n = r^{-n}e^{in\theta}$ si $n>0$.

1. Montrer que $(z_n)_{n\in\mathbb{Z}}$ est sommable.
2. Calculer $\sum_{n\in\mathbb{Z}} z_n$.

Correction

1. $|z_n| = r^{|n|}$ et comme $0r<1$, alors $(|z_n|)_{n\in\mathbb{N}}$ et $(|z_n|)_{n\in\mathbb{Z}_-}$ sont sommables (car $r\in[0,1[$). Donc $(z_n)_{n\in\mathbb{Z}}$ est sommable.
2. Puis,
$$\sum_{n\in\mathbb{Z}} z_n = \sum_{n=0}^{+\infty}(re^{i\theta})^n + \sum_{n=1}^{+\infty}(re^{-i\theta})^n = \frac{1}{1-re^{i\theta}} + \frac{re^{-i\theta}}{1-re^{-i\theta}}$$
$$= \frac{1-re^{-i\theta}+re^{-i\theta}-r^2}{(1+r^2-2r\cos\theta} = \frac{1-r^2}{1-2r\cos\theta+r^2}$$

Théorème - Fubini - suites doubles complexes indexées sur un produit cartésien
Considérons une suite numérique doublement indexée $(z_{d,d'})_{(d,d')\in D\times D'}$.
$(z_{d,d'})_{(d,d')\in D\times D'}$ est sommable si et seulement si
1. pour tout $d\in D$, la famille $(z_{d,d'})_{d'\in D'}$ est sommable
2. puis la famille $\left(\sum_{d'}|z_{d,d'}|\right)_{d\in D}$ est sommable.

On a alors
$$\sum_{(d,d')\in D\times D'} z_{d,d'} = \sum_{d\in D}\left(\sum_{d'\in D'} z_{d,d'}\right) = \sum_{d'\in D'}\left(\sum_{d\in D} z_{d,d'}\right)$$

Démonstration
On exploite les équivalences : $(z_{d,d'})_{(d,d')\in D\times D'}$ est sommable
si et seulement si $(|z_{d,d'}|)_{(d,d')\in D\times D'}$ est sommable
si et seulement si pour tout $d\in D$, la famille $(|z_{d,d'}|)_{d'\in D'}$ est sommable ($\Leftrightarrow$ $(z_{d,d'})_{d'\in D'}$ est sommable) ;
et la famille $\left(\sum_{d'}|z_{d,d'}|\right)_{d\in D}$ est sommable.
On exploite ensuite $D\times D' = \biguplus_{d\in D}(\{d\}\times D')$ et le théorème de sommation par paquets, pour obtenir l'égalité sommatoire. □

Deux cas d'application en particulier :

Proposition - Produit de termes
Soient $(z_d)_{d\in D}\in\ell^1(D,\mathbb{C})$ et $(z'_{d'})_{d'\in D'}\in\ell^1(D',\mathbb{C})$.
Alors $(z_d z'_{d'})_{(d,d')\in D\times D'}\in\mathbb{C}^{D\times D'}$ est sommable.
Et $\sum_{(d,d')\in D\times D'} z_d z'_{d'} = \left(\sum_{d\in D} z_d\right)\times\left(\sum_{d'\in D'} z'_{d'}\right)$.

Exercice
Faire la démonstration

Correction

Proposition - Fubini complexe indexé sur $\mathbb{N}$
Soit $(z_{(p,q)})_{(p,q)\in\mathbb{N}^2}\in\mathbb{C}^{\mathbb{N}^2}$.
$(z_{p,q})_{(p,q)\in\mathbb{N}^2}$ est sommable si et seulement si
$\begin{cases}$ 1. Pour tout $p\in\mathbb{N}$, la série $\sum_{q\geqslant 0}|z_{p,q}|$ converge
2. La série $\sum_{p\geqslant 0}\left(\sum_{q=0}^{+\infty}|z_{p,q}|\right)$ converge. $\end{cases}$
Et on a alors $\sum_{(p,q)\in\mathbb{N}^2} z_{p,q} = \sum_{p=0}^{+\infty}\left(\sum_{q=0}^{+\infty} z_{p,q}\right) = \sum_{q=0}^{+\infty}\left(\sum_{p=0}^{+\infty} z_{p,q}\right)$.

On peut arbitrairement faire l'interversion $p\leftrightarrow q$.
Exercice
Faire la démonstration

Correction

Exemple - Convergence et somme de $\sum_{n\geqslant 0}\frac{z^{2^n}}{1-z^{2^{n+1}}}$
Soit $z\in\mathbb{C}$ et on note pour tout entier $n\in\mathbb{N}$, $z_n = \frac{z^{2^n}}{1-z^{2^{n+1}}}$.
On considère que les nombres complexes z tel que pour tout $n\in\mathbb{N}$, $z^{2^{n+1}}\neq 1\dots$
• Pour $|z|<1$, $|z_n|\sim|z|^{2^n} = o(|z|^n)$ et $(|z|^n)$ est sommable car la série associée est convergente.
Donc $(z_n)_{n\in\mathbb{N}}$ est sommable.
• Pour $|z|>1$, $|z_n|\sim\frac{1}{|z|^{2n}}$ et donc $(z_n)_{n\in\mathbb{N}}$ est sommable.
• Pour $|z|=1$, alors $|z_n| = \frac{1}{|1-z^{2^{n+1}}|}\geqslant\frac{1}{2}$, donc $\sum|z_n|$ diverge grossièrement.
Ainsi, $(z_n)_{n\in\mathbb{N}}$ n'est pas sommable. Finalement, $(z_n)_{n\in\mathbb{N}}$ est sommable si et seulement si $z\notin\mathbb{U}$.

Calculons maintenant la somme en notant que $\frac{1}{1-z^{2^{n+1}}} = \sum_{k=0}^{+\infty} \left(z^{2^{n+1}}\right)^k$.

$$\sum_{n\in\mathbb{N}} z_n = \sum_{n=0}^{+\infty}\sum_{k=0}^{+\infty} z^{2^n} z^{k(2^{n+1})} = \sum_{(n,k)\in\mathbb{N}^2} z^{(2k+1)2^n}$$

Or $\mathbb{N}^2 \to \mathbb{N}^*$, $(n,k) \mapsto (2k+1)2^n$ est bijective. Ainsi

$$\sum_{n\in\mathbb{N}} z_n = \sum_{h=1}^{+\infty} z^h = \frac{z}{1-z}$$

3.6. Application : Produit de Cauchy

Définition - Produit de Cauchy
Soient $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites complexes.
Le produit de Cauchy des deux séries $\sum_{n\geqslant 0} a_n$ et $\sum_{n\geqslant 0} b_n$ est la série $\sum_{n\geqslant 0} c_n$,
avec, pour tout $n\in\mathbb{N}$, $c_n = \sum_{p+q=n} a_p b_q = \sum_{h=0}^{n} a_h b_{n-h}$.

Proposition - Produit de séries absolument convergentes
Soient $\sum_{n\geqslant 0} a_n$ et $\sum_{n\geqslant 0} b_n$ deux séries absolument convergentes,
alors leur produit de Cauchy $\sum_{n\geqslant 0} c_n$ est une série abs. convergente.
Et on a $\sum_{n=0}^{+\infty} c_n = \sum_{n=0}^{+\infty} a_n \times \sum_{n=0}^{+\infty} b_n$.

Démonstration
Les hypothèses sont équivalentes à l'affirmation que $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont sommables.
Donc $(a_p b_q)_{(p,q)\in\mathbb{N}^2}$ est sommable.
Or $\mathbb{N}^2 = \biguplus_{n\in\mathbb{N}} \{(p,q)\in\mathbb{N}^2 \mid p+q=n\}$.
Ainsi, pour tout $n\in\mathbb{N}$, $(a_p b_q)_{p+q=n}$ est une famille (finie) sommable et $\left(\sum_{n\geqslant 0} |a_p b_q|\right)$ est sommable. Or, on sait par inégalité triangulaire que $|c_n| = \left|\sum_{p+q=n} a_p b_q\right| \leqslant \sum_{p+q=n} |a_p b_q|$.
Donc $(c_n)_{n\in\mathbb{N}}$ est sommable (i.e. $\sum c_n$ est absolument convergente).
Et
$$\sum_{n=0}^{+\infty} a_n \times \sum_{n=0}^{+\infty} b_n = \sum_{(p,q)\in\mathbb{N}^2} a_p b_q = \sum_{n=0}^{+\infty}\sum_{p+q=n} a_p b_q = \sum_{n=0}^{+\infty} c_n$$
□

Exemple - Exponentielle
Soient $z, z'\in\mathbb{C}$. Les séries $\sum_{n\geqslant 0} \frac{z^n}{n!}$ et $\sum_{n\geqslant 0} \frac{z'^n}{n!}$ sont absolument convergentes.
Donc leur produit de Cauchy est absolument convergent
$$c_n = \sum_{p+q=n} \frac{z^p z'^q}{p!q!} = \frac{1}{n!}\sum_{p=0}^{n} \binom{n}{p} z^p z'^{n-p} = \frac{(z+z')^n}{n!}$$
Et on trouve donc $\exp z \times \exp z' = \exp(z+z')$.

Application - Formule du binôme négative
Soit $z\in\mathbb{C}$ avec $|z|<1$. Donc la famille $(z^n)_{n\in\mathbb{N}}$ est sommable.
On a alors, pour tout $p\in\mathbb{N}$ (par récurrence),
$$\sum_{n=0}^{+\infty} c_{n,p+1} z^n \frac{1}{(1-z)^{p+1}} = \frac{1}{1-z}\times\frac{1}{(1-z)^p} = \sum_{n=0}^{+\infty} z^n \times \sum_{n=0}^{+\infty} c_{n,p} z^n$$

Pour aller plus loin - A démontrer autrement
Ou bien par dénombrement directement.
Ou bien avec la formule de Newton et une puissance entière négative…

Par produit de Cauchy : $c_{n,p+1} = \sum_{k=0}^{n} 1\, c_{k,p}$.
Mais aussi par inversion : $(1-z)\times\sum_{n=0}^{+\infty} c_{n,p+1} z^n = \sum_{n=0}^{+\infty} c_{n,p} z^n$,
par produit de Cauchy : $c_{n,p+1} - c_{n-1,p+1} = c_{n,p}$ donc $c_{n,p+1} = c_{n,p} + c_{n-1,p+1}$.
Cela rappelle la formule du Pascal, en posant $c_{n,p} = \binom{n+p}{n}$, on retrouve
$$c_{n,p+1} = \binom{n+1+p}{n} = \binom{n+p}{n} + \binom{n+p}{n-1} = c_{n,p} + c_{n-1,p+1}$$
Et l'initiation est juste : $c_{n,0} = 1 = \binom{n}{n}$.
On a donc la formule du binôme négatif :
$$\forall\, |z|<1,\quad \frac{1}{(1-z)^{p+1}} = \sum_{n=0}^{+\infty}\binom{n+p}{p} z^n = \sum_{n=0}^{+\infty}\binom{n+p}{n} z^n$$

Attention - Cas de non convergence absolue
Considérons $a_n = b_n = \frac{(-1)^n}{\sqrt{n+1}}$.
Les séries $\sum a_n$ et $\sum b_n$ sont semi-convergence (critère de Leibniz), i.e. convergentes mais non absolument convergentes.
Le produit de Cauchy donne $c_n = \sum_{h=0}^{n} \frac{(-1)^n}{\sqrt{(h+1)(n-h+1)}}$.
Or $x\mapsto (x+1)(n+1-x)$ est maximal en $x=\frac{n}{2}$ et vaut $(\frac{n}{2}+1)^2$.
d'où $|c_n| \geqslant (n+1)\frac{2}{n+2} \geqslant 1$, donc $\sum c_n$ diverge grossièrement : la famille $(c_n)_{n\in\mathbb{N}}$ n'est pas sommable.

4. Bilan

Synthèse

- Une famille de nombres positif indexé par I est sommable si l'ensemble des sommes possibles sur une partie finie de I est majorée. La somme est alors égale à la borne supérieure.
  Nécessairement : la famille I est dénombrable, si $I\subset\mathbb{N}$, alors cela est équivalent à l'absolue convergence de la série.
  On a deux autres stratégies pour montrer la sommabilité : la sommation par paquets, ou la sommation par suite croissante d'ensembles.
- Dans le cas de famille sommable de termes positifs, tout se passe parfaitement : linéarité, changement d'ordre de sommation, et Fubini ! On a même, dans ce cas, une stratégie « idéale ». Sans se poser de question, on se place dans $\overline{R}$ et on calcule la somme des termes (dans l'ordre qui nous arrange) ; si la somme est un nombre réel, alors la famille est sommable (on peut appliquer alors Fubini…) ; sinon la somme vaut $+\infty$ et la famille n'est pas sommable.
- Dans le cas des familles de nombres (u_n) réels ou complexes, on étudie la sommabilité par l'étude du module de (u_n). Il est nécessaire et suffisant d'étudier (u_n^+) et (u_n^-) (voire les parties réelles et imaginaires). Quand la famille est sommable, on peut alors effectuer une sommation par paquets (ensembles disjoints) ou faire des interversions d'ordre de somme (Fubini - c'est le cas pour le produit de Cauchy, par exemple).

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Sous-ensembles finis de $\mathbb{N}^2$
- Savoir-faire - Montrer qu'une famille n'est pas sommable
- Savoir-faire - Trouver une suite croissance d'ensemble d'indexation (fini)
- Savoir-faire - Exploitation d'une suite croissante d'ensembles finis
- Savoir-faire - Application du théorème de sommation par paquets avec $I = \mathbb{N}$
- Savoir-faire - Etude d'une famille sommable
- Savoir-faire - Montrer la sommabilité d'une famille de réels ou de complexes
- Savoir-faire - Décomposition en morceaux
- Savoir-faire - Sommabilité par majoration
- Savoir-faire - Utiliser la propriété des suites croissantes d'ensemble pour calculer une somme (1)
- Savoir-faire - Utiliser la propriété des suites croissantes d'ensemble pour calculer une somme (2)

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\mathscr{P}_f(I)$	Ensemble des parties (ou sous-ensembles) finis de I		
$D = \bigcup_{n\in\mathbb{N}} D_n$	$(D_n)_{n\in\mathbb{N}}$ est une suite croissante de parties de D de réunion égal à D	$\forall\, n \in \mathbb{N}$, $D_n \subset D_{n+1}$ et $\forall\, x \in D$, $\exists\, n \in \mathbb{N}$ tel que $x \in D_n$	Si $(u_d)_{d\in D}$ sommable, alors : $\sum_{d\in D} u_d = \lim_{n\to+\infty}\left(\sum_{d\in D_n} u_d\right)$
$D = \biguplus_{i\in I} P_i$	$(P_i)_{i\in I}$ est une partition de D	$\forall\, x \in D$, $\exists! i \in I$ tel que $x \in P_i$ et $\forall\, i \in I$, $P_i \subset D$.	Si $(u_d)_{d\in D}$ sommable : $\sum_{d\in D} u_d = \sum_{d\in\biguplus_{i\in I}} u_d = \sum_{i\in I}\sum_{d\in P_i} u_d$
$\ell_1(D, A)$ (avec $A = \mathbb{R}_+, \mathbb{R}$ ou $\mathbb{C}$)	Espace vectoriel des familles de nombres de A, indexés par D et sommables		

Retour sur les problèmes

133. Cours
134. Cours
135. Cours
136. Cours

Chapitre 40

Fonctions de deux variables

Résumé -

Dans ce chapitre, nous aimerions clarifier à la sauce mathématicienne quelques méthodes exploitées en physique, où les fonctions ont pour arguments plusieurs variables.
Nous devons dans un premier temps, élargir la notion de limite : les valeurs absolues sont remplacées par des normes, les intervalles par des boules. Cela nécessite quelques définitions.
Puis, nous passons rapidement sur la continuité des fonctions de plusieurs variables pour nous concentrer ensuite sur la dérivation. Au passage, nous essayons d'illustrer tant que possible ce chapitre par des zooms sur les méthodes de physiques. Nous anticipons aussi le théorème des fonctions implicites et surtout les méthodes d'optimisation (sans ou avec contraintes) étudiés en seconde année.

Sommaire

1. Problèmes 824
2. Topologie 825
2.1. Le cadre : espace vectoriel normé 825
2.2. Initiation à la topologie sur un espace normé 829
2.3. Topologie relative 831
2.4. Compact 832
2.5. Adhérences et intérieurs 834
3. Continuité 835
3.1. Limite 835
3.2. Critère de continuité (ou non) à l'aide de suites . . . 838
3.3. Exemple d'applications continues 839
3.4. Continuité sur un compact 841
3.5. Représentation graphique 841
4. Calcul différentiel 843
4.1. Développement limité. Différentiabilité 843
4.2. Dérivées partielles 844
4.3. Application de classe $\mathscr{C}^1$ 845
4.4. Règle de la chaine 848
5. Visualisation et optimisation 851
5.1. Tangente à une courbe, à une surface 851
5.2. Interprétation physique du gradient 854
5.3. Optimum libre 855
5.4. Optima liés 857
6. Bilan 858

1. Problèmes

Problème 174 - Suite $(u_n)_{n\in\mathbb{N}}$ avec $\forall\ n\in\mathbb{N}$, $u_n\in\mathbb{R}^p$

Rappel :

$$(u_n)\to\ell\iff\forall\,\epsilon>0,\exists\,N\in\mathbb{N}\text{ tel que }\forall\ n\geqslant N,|u_n-\ell|\leqslant\epsilon$$

Comment généraliser la définition de la convergence d'une suite, lorsque celle-ci est à valeurs dans un espace vectoriel $\mathbb{R}^n$.
En particulier, que faire de la valeur absolue ?

Problème 175 - Si la valeur absolue est remplacée par une norme...

On a vu qu'il existe de nombreuses normes sur un même espace vectoriel. A priori, chaque norme définie pour une même suite, sa propre limite. Ce n'est pas pratique...
A quelle condition la limite de (u_n) est indépendante de la norme considérée ?
Cette condition est-elle alors toujours vérifiée ? Ce qui serait bien pratique...

Problème 176 - Continuité et représentation de $f:\mathbb{R}^2\to\mathbb{R}$

Qu'est ce qu'une fonction continue de plusieurs variables ? La question a-t-elle un sens ? Comment faut-il dessiner une fonction $f(x,y)$ sans lever le crayon, alors qu'en fait ce dessin est celui d'une surface ?

Problème 177 - Dérivation de $\mathbb{R}\to\mathbb{R}$. De $\mathbb{R}^n\to\mathbb{R}$?

On sait
- que les fonctions réelles se dérivent en calculant

$$\forall\ x\in I,\lim_{h\to0}\frac{f(x+h)-f(x)}{h}$$

- Lorsque cette limite existe, on la note $f'(x)$.
- On a le théorème essentiel suivant : f est dérivable en x_0 ssi f admet un D.L. d'ordre 1 en x_0 : $f(x)=f(x_0)+A(x-x_0)+o(x-x_0)$. Dans ce cas $f'(x_0)=A$
- La dérivée de f (en x_0) précise donc le comportement de f au voisinage de x_0, une fois que l'on a fait disparaître le terme dominant donnant la valeur de premier ordre (i.e. $f(x_0)$).
- Ainsi, la croissance (ou décroissance) d'une fonction est une critère local donné localement par tout $f'(x)$. L'étude du signe de f' permet alors de **généraliser** les variations de f à tout l'intervalle d'étude.

Que vaut approximativement $\sqrt{4,001}$?

Problème 178 - Dérivation ⇒ continuité

Est-ce que toute fonction dérivable $f : \mathbb{R}^2 \to \mathbb{R}$ est nécessairement continue?
Sinon, comment trouver un contre-exemple?

Problème 179 - « Tout problème mathématique est le calcul d'un maximum »

comme le disait Euler. Comment faire alors pour trouver le maximum d'une fonction $f : \mathbb{R}^p \to \mathbb{R}$?
Et si, on ajoute en outre des contraintes sur les vecteurs $\vec{u}$ de $\mathbb{R}^p$?

2. Topologie

2.1. Le cadre : espace vectoriel normé

Heuristique - Pourquoi la topologie?

Selon Wikipédia, l'étymologie du mot « topologie » (en grec $\tau o \pi o \lambda o \gamma \iota \alpha$) procède de l'association de deux noms grecs $\tau o \pi o \sigma$ (topos, masculin) et $\lambda o \gamma \iota \alpha$ (logia, féminin) qui signifient respectivement « le lieu » et « l'étude ». Littéralement, topologie signifie l'« étude d'un lieu » ou « étude topique ».
Elle s'intéresse donc à définir ce qu'est un lieu (appelé aussi « espace ») et quelles peuvent en être les propriétés. Une ancienne dénomination fut analysis situs, c'est-à-dire « l'étude du lieu ».
La topologie est une branche des mathématiques concernant l'étude des déformations spatiales par des transformations continues (sans arrachages ni recollement des structures). La topologie s'intéresse plus précisément aux espaces topologiques et aux applications qui les lient, dites « continues ».
En analyse, grâce aux informations qu'elle fournit sur l'espace considéré, elle permet d'obtenir un certain nombre de résultats (existence ou unicité de solutions d'équations différentielles, notamment).

Espace vectoriel normé

On se place dans des espaces vectoriels : on a besoin de pouvoir additionner les éléments (vecteurs) et les multiplier par des nombres.
On rappelle :

Définition - Norme

Soit E, un $\mathbb{K}$e.v. (où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$).
$N : E \to \mathbb{R}^+$ est un norme si :

1. $\forall\, x \in E,\ N(x) \geqslant 0$
2. $\forall\, x \in E,\ N(x) = 0 \iff x = 0$
3. $\forall\, x \in E,\ \lambda \in \mathbb{K},\ N(\lambda \cdot x) = |\lambda| N(x)$
4. $\forall\, x, y \in E,\ N(x+y) \leqslant N(x) + N(y)$ (inégalité triangulaire)

Un *espace vectoriel* muni d'une norme est appelé un espace vectoriel normé

Remarque - Norme et produit scalaire

Nous avons vu ce qu'est un produit scalaire défini sur un espace vectoriel.
Si $(\cdot|\cdot)$ est un produit scalaire défini sur E, alors $N : x \mapsto \sqrt{(x|x)}$ est une norme.
On dit que c'est la norme (euclidienne) associée au produit scalaire.
Réciproquement, si N est une norme, elle dérive d'un produit scalaire si et seulement si $(x, y) \mapsto \frac{1}{2}(N(x+y) - N(x) - N(y))$ est un produit scalaire (c'est alors le produit scalaire en question).

Savoir faire - Renverser l'inégalité triangulaire

Dans beaucoup d'exercices, il faut utiliser l'inégalité triangulaire pour également minorer $d(x, y) = \|x - y\|$.
Comme $\|x\| = \|x + y - y\| \leqslant \|x - y\| + \|y\|$,
donc $\|x - y\| \geqslant \|x\| - \|y\|$, et de même $\|y - x\| \geqslant \|y\| - \|x\|$,
or $\|x - y\| = \|y - x\|$, donc

$$\|x - y\| \geqslant \big|\|x\| - \|y\|\big|$$

Rappelons que l'on a la majoration : $\|x - y\| \leqslant \|x\| + \|-y\| = \|x\| + \|y\|$

Remarque - Notation

Il arrive souvent de noter la norme $\|\cdot\|$ au lieu de N.

Définition - Distance

Soit E un $\mathbb{K}$ev. $d : E^2 \to \mathbb{R}^+$ est un distance si :

1. $\forall\, x, y \in E,\ d(x, y) \geqslant 0$
2. $\forall\, x, y \in E,\ d(x, y) = 0 \iff x = y$
3. $\forall\, x, y \in E,\ d(x, y) = d(y, x)$
4. $\forall\, x, y, z \in E,\ d(x, y) \leqslant d(x, z) + d(z, y)$

Un espace vectoriel muni d'une distance est appelé espace métrique.

Exercice
Montrer que si N est une norme sur E, alors $d : (x, y) \mapsto N(x - y)$ est une distance sur E.
Tout espace normé est donc un espace métrique

Correction

Exemple de normes (espaces vectoriels de dimension finie)

Proposition - Exemple de normes de $\mathbb{R}^2$, $\mathbb{R}^3$ ou $\mathbb{K}^n$

Considérons l'espace vectoriel $\mathbb{K}^n$.
Alors, les applications suivantes en sont des normes
- $\|(x_1, x_2, \dots x_n)\|_1 = \sum_{i=1}^n |x_i|$
- $\|(x_1, x_2, \dots x_n)\|_\infty = \max_i(|x_i|)$
- $\|(x_1, x_2, \dots x_n)\|_2 = \sqrt{\sum_{i=1}^n x_i^2}$
  Cette dernière norme dérive du produit scalaire $(x|y) \mapsto \sum_{i=1}^n x_i y_i$

Il est important de savoir démontrer cela.

Démonstration
Soit $x = (x_1, x_2, \dots x_n)$ un élément de $\mathbb{K}^n$.
- $\|\cdot\|_1$.
  1. $\forall\, i \in \mathbb{N}_n,\ |x_i| \geqslant 0$, donc $\sum_{i=1}^n |x_i| = \|(x_1, x_2, \dots x_n)\|_1 \geqslant 0$
  2. Si $\|(x_1, x_2, \dots x_n)\|_1 = 0$, alors $\sum_{i=1}^n |x_i| = 0$, il s'agit une somme de termes positifs, elle est nulle si et seulement si chacun des termes est nuls, donc $\forall\, i \in \mathbb{N}_n,\ |x_i| = 0$
  3. $\|\lambda \cdot x\|_1 = \|(\lambda x_1, \lambda x_2, \dots \lambda x_n)\|_1 = \sum_{i=1}^n |\lambda x_i| = |\lambda| \sum_{i=1}^n |x_i| = |\lambda| \|x\|_1$
  4. $\|x + y\|_1 = \sum_{i=1}^n |x_i + y_i| \leqslant \sum_{i=1}^n (|x_i| + |y_i|)$, car pour tout entier i, $|x_i + y_i| \leqslant |x_i| + |y_i|$.
     Donc $\|x + y\|_1 \leqslant \sum_{i=1}^n |x_i| + \sum_{i=1}^h |y_i| = \|x\|_1 + \|y\|_1$
- $\|\cdot\|_\infty$.
  1. $\forall\, i \in \mathbb{N}_n,\ |x_i| \geqslant 0$, donc $\max i |x_i| = \|(x_1, x_2, \dots x_n)\|_\infty \geqslant 0$
  2. Si $\|(x_1, x_2, \dots x_n)\|_\infty = 0$, alors $\max_i |x_i| = 0$, donc $\forall\, j \in \mathbb{N}_n,\ |x_j| = 0$
  3. $\|\lambda \cdot x\|_\infty = \max(|\lambda x_1|, |\lambda x_2|, \dots |\lambda x_n|) = |\lambda| \max_i |x_i| = |\lambda| \|x\|_\infty$
  4. $\|x + y\|_\infty = \max_i |x_i + y_i| \leqslant \max_i (|x_i| + |y_i|) \leqslant \max_j |x_j| + \max_k |x_k|$,
     Donc $\|x + y\|_\infty \leqslant \|x\|_\infty + \|y\|_\infty$

— $\|\cdot\|_2$.

1. $\forall\ i\in\mathbb{N}_n$, $x_i^2\geqslant 0$, donc la norme est définie et $\sqrt{\sum_{i=1}^n x_i^2}=\|(x_1,x_2,\dots x_n)\|_1\geqslant 0$
2. Si $\|(x_1,x_2,\dots x_n)\|_2=0$, alors $\sum_{i=1}^n x_i^2=0$, il s'agit une somme de termes positifs, elle est nulle si et seulement si chacun des termes est nuls, donc $\forall\ i\in\mathbb{N}_n$, $x_i^2=0$, donc $x_i=0$.
3. $\|\lambda\cdot x\|_2=\|(\lambda x_1,\lambda x_2,\dots\lambda x_n)\|_2=\sqrt{\sum_{i=1}^n\lambda^2x_i}=\sqrt{\lambda^2}\sum_{i=1}^n x_i^2=|\lambda|\|x\|_2$
4. $\|x+y\|_2^2=\sum_{i=1}^n(x_i+y_i)^2=\sum_{i=1}^n(x_i^2+y_i^2+2x_iy_1)$
$=\sum_{i=1}^n x_i^2+\sum_{i=1}^n y_i^2+2\sum_{i=1}^n x_iy_i\leqslant\|x\|_2^2+\|y\|_2^2+2\sqrt{\sum_{i=1}^n x_i^2}\sqrt{\sum_{i=1}^n y_i^2}$
d'après l'inégalité de Cauchy-Schwarz (que vaut-elle?).

Donc en prenant la racine carrée, $\|x+y\|_2\leqslant\sqrt{(\|x\|_2+\|y\|^2)^2}$, cqfd.

La relation de la norme $\|\cdot\|_2$ avec le produit scalaire est un "simple" calcul.

□

Convergence dans E

On retrouve la même définition que pour la convergence de suites réelles, mais où la valeur absolue est remplacée par la norme.

Définition - Convergence d'un espace vectoriel normé
Soit $(x_n)\in E^{\mathbb{N}}$ une suite d'élément de E.
On dit que (x_n) converge vers x dans $(E,\|\cdot\|)$ si :

$$\forall\ \epsilon>0,\exists\ N\in\mathbb{N}\mid\forall\ n\geqslant N,\|x_n-x\|\leqslant\epsilon$$

Comme pour le cas réel : si la suite (x_n) converge, sa limite est unique, elle est notée $\lim(x_n)$. On dit alors simplement que (x_n) est une suite convergente.

Exercice
Montrer l'unicité de la limite

Correction
On suppose qu'il en existe deux x et x'.
Par séparabilité, on note $\epsilon=\frac{\|x-x'\|}{3}>0$ si $x\neq x'$.
On applique la définition avec ce ϵ, x et x', on prend $n=\max(N,N')$, on trouve (inégalité triangulaire) :

$$3\epsilon=\|x-x'\|\leqslant\|x-u_n\|+\|u_n-x'\|\leqslant 2\epsilon$$

Absurde !

Voici un exemple de convergence pour $\|\cdot\|_\infty$.

Exemple - Convergence de $\begin{pmatrix}(1+\frac{1}{n})^n & n\sin\frac{1}{n}\\ \sqrt{n+1}-\sqrt{n} & \arctan n\end{pmatrix}$

Pour la norme $\|M\|_\infty=\max_{i,j}(|_i[M]^j|)$, la convergence de la suite est équivalente à la convergence de chacun des coefficients des termes de la suite.

Ici M_n converge vers $\begin{pmatrix}e & 1\\ 0 & \frac{\pi}{2}\end{pmatrix}$ (pour chacune des trois normes : $\|\cdot\|_1$, $\|\cdot\|_2$ ou $\|\cdot\|_3\dots$).

Normes équivalentes

Attention - Résultat qui dépend de la norme
A priori la convergence d'une suite dépend de la norme considérée ! C'est un vrai et grave problème, en particulier pour les suites (ou séries) de fonctions que vous verrez en seconde année.
Mais nous verrons plus loin que souvent ce problème se résout : il suffit que E soit de dimension finie où les normes sont équivalentes.

Heuristique - Une même limite pour deux normes différentes
Pour **un même espace vectoriel**, nous pouvons avoir **plusieurs normes** en présence.
Est-il possible qu'une même suite de nombres de l'espace vectoriel considéré converge vers des limites différentes, selon la norme considérée?
Pour s'assurer que la limite est identique, il faut que pour deux normes $\|\cdot\|_1$ et $\|\cdot\|_2$, on ait :
$\Big(\forall\ \epsilon_1,\exists\ N_1\in\mathbb{N}\text{ tq }\forall\ n\geqslant N_1,\|x_n-\ell\|_1<\epsilon_1\Big)\Longrightarrow\Big(\forall\ \epsilon_2,\exists\ N_2\in\mathbb{N}\text{ tq }\forall\ n\geqslant N_2,\|x_n-\ell\|_2<\epsilon_2\Big)$
et
$\Big(\forall\ \epsilon_1,\exists\ N_2\in\mathbb{N}\text{ tq }\forall\ n\geqslant N_2,\|x_n-\ell\|_2<\epsilon_1\Big)\Longrightarrow\Big(\forall\ \epsilon_2,\exists\ N_1\in\mathbb{N}\text{ tq }\forall\ n\geqslant N_1,\|x_n-\ell\|_1<\epsilon_2\Big)$
Pour cela il faut que $\|x_n-\ell\|_1$ soit petite en même temps que $\|x_n-\ell\|_2$, pour tout (x_n) et ℓ.
Notre habitude pour démontrer une convergence est d'utiliser des majorations et minorations, il faut et il suffit ici que les normes soient comparables (majorer et minorer) avec de constante de proportionnalité :

$$\exists\ A,B\text{ tels que }\forall\ X\in E\qquad\|X\|_1\leqslant A\|X\|_2\text{ et }\|X\|_2\leqslant B\|X\|_1$$

Que l'on peut résumer en une formule

Proposition - Normes équivalentes
Soit E un espace vectoriel normé, muni de deux normes N et N'.
On dit que N et N' sont équivalentes si il existe a et $b\in\mathbb{R}_+^*$ tel que :
$$\forall\ x\in E,\qquad aN'(x)\leqslant N(x)\leqslant bN'(x).$$
Il s'agit d'une relation d'équivalence.

Exercice
Montrer que N' et N sont équivalentes si et seulement si :
$\forall\ (x_n)\in E^{\mathbb{N}}$, $(x_n)\to 0$ pour $N\Leftrightarrow(x_n)\to 0$ pour N'.

Correction
Supposons $i)$, i.e. $AN\leqslant N'\leqslant BN$.
Si (x_n) converge vers 0 pour N.
alors pour tout ϵ, il existe n_0 tel que $\forall\ n\geqslant n_0$, $N(x_n)\leqslant\frac{\epsilon}{B}$ donc $N'(x_n)\leqslant BN(x_n)\leqslant\epsilon$.
donc (x_n) converge vers 0 pour N'.
Reciproquement, si (x_n) converge vers 0 pour N'.
alors pour tout ϵ, il existe n_0 tel que $\forall\ n\geqslant n_0$, $N'(x_n)\leqslant\frac{\epsilon}{A}$ donc $N(x_n)\leqslant AN'(x_n)\leqslant\epsilon$.
donc (x_n) converge vers 0 pour N.
Donc $ii)$ est vraie.
Pour démontrer que $ii)\Rightarrow i)$ nous allons démontrer la contraposée.
Supposons que N et N' ne sont pas équivalentes.
Alors $\forall\ A\in\mathbb{R}$, $\exists\ x\in E$ tel que $N(x)>AN'(x)$ ou $N'(x)>AN(x)$.
Considérons donc la première situation. Donc $\forall\ n\in\mathbb{N}$, $\exists\ x_n\in E$ tel que $N(x_n)>nN'(x_n)$.
et pour tout $\lambda\in\mathbb{R}_+$, $N(\lambda x_n)=\lambda N(x_n)>\lambda nN'(x_n)=nN'(x_n)$.
Notons $y_n=\frac{x_n}{N(x_n)}$ (i.e. $\lambda=\frac{1}{N(x_n)}$).
Alors comme $N(x_n)>0$, $N(y_n)=N\big(\frac{x_n}{N(x_n)}\big)=1>nN'(y_n)$
et donc $N(y_n)=1$, donc (y_n) ne converge pas vers 0 pour N,
alors que $N'(y_n)<\frac{1}{n}$ et donc (y_n) converge vers 0 pour N'
Par conséquent donc $ii)$ est faux.

Notons que tout $\mathbb{K}$ espace vectoriel de dimension n est isomorphe à $\mathbb{K}^n$. L'isomorphisme (réciproque) peut aisément transférer la norme…

Proposition - Equivalence des normes usuelles
Soit $E=\mathbb{K}^n$, un espace vectoriel sur $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$.
Alors, pour tout $x\in E$, $\|x\|_\infty\leqslant\|x\|_1\leqslant\sqrt{n}\|x\|_2\leqslant n\|x\|_\infty$.

Démonstration
Soit $x\in E$ écrit dans la base canonique $(x_1,x_2,\dots x_n)$.
$\|x\|_\infty=\max(|x_i|)$, donc pour tout $i\in\mathbb{N}_n$, $|x_i|\leqslant\|x\|_\infty$ et il existe i_0 tel que $\|x\|_\infty=|x_{i_0}|$.
$\|x\|_1=\sum_{k=1}^n|x_k|=|x_{i_0}|+\sum_{k\neq i_0}|x_k|\geqslant|x_{i_0}|=\|x\|_\infty$.
le résultat est optimal avec $x=(1,0,\dots,0)$, on a $\|x\|_\infty=\|x\|_1=1$.
Cauchy-Schwarz : $\|x\|_1=\sum_{k=1}^n 1\times|x_k|\leqslant\sqrt{\sum_{k=1}^n 1^2}\times\sqrt{\sum_{k=1}^n|x_k|^2}=\sqrt{n}\|x\|_2$.
Le résultat est optimal avec $x=(1,1,\dots,1)$, on a $\|x\|_1=n$ et $\|x\|_2=\sqrt{n}$,
donc $\|x\|_1=\sqrt{n}\|x\|_2$.
Enfin, pour tout $i\in\mathbb{N}_n$, $|x_i|\leqslant\|x\|_\infty$, donc $\|x\|_2^2=\sum_{k=1}^n|x_i|^2\leqslant\sum_{k=1}^n\|x\|_\infty=n\times\|x\|_\infty$,
donc en prenant la racine, $\|x\|_2\leqslant\sqrt{n}\|x\|_\infty$.
Le résultat est optimal avec $x=(1,1,\dots,1)$, on a $\|x\|_\infty=1$ et $\|x\|_2=\sqrt{n}$,
donc $\|x\|_2=\sqrt{n}\|x\|_1$. □

Exercice
Montrer que pour tout $x \in \mathbb{R}^n$, $\|x\|_2 \leqslant \|x\|_1$

Correction

Ces normes sont équivalentes, est-ce un hasard?

Proposition - Norme équivalentes dans $\mathbb{R}^2$
Toutes les normes de $\mathbb{R}^2$ sont équivalentes.

Démonstration
Soit N, une norme quelconque de $\mathbb{R}^2$. Nous allons montrer que N est semblable à $\|\cdot\|_\infty$.
Par transitivité, toutes les normes seront semblables.
• Notons $A = N(e_1) + N(e_2) > 0$
Pour tout vecteur $u = (a,b) = ae_1 + be_2 \in \mathbb{R}^2$,
$N(u) = N(ae_1+be_2) \leqslant N(ae_1)+N(be_2) = |a|N(e_1)+|b|N(e_2) \leqslant \max(|a|,|b|)(N(e_1)+N(e_2)) = A\|u\|_\infty$
• Réciproquement, considérons $K = \{N(u) \mid \|u\|_\infty = 1\}$.
Notons que $\{u = (a,b) \in \mathbb{R}^2 \mid \|u\|_\infty = 1\} = \{1\} \times [-1,1] \cup [-1,1] \times \{-1,1\} \cup [-1,1] \times \{1\} \cup [-1,1] \times \{1\}$.
On va étudier K, en quatre parties.
Considérons donc $K_1 = \{N(u) \mid u = (1,b) \& b \in [-1,1]\}$.
Soit $f_1 : [-1,1] \to \mathbb{R}_+,\ b \mapsto N(1,b)$.
Montrons que f_1 est continue. Par inégalité triangulaire renversée :
$|f_1(b) - f_1(b')| = \left|N(1,b) - N(1,b')\right| \leqslant N((1,b)-(1,b')) = N(0,(b-b')) = |b-b'|N(e_2)$
Donc f_1 est $N(e_2)$-lipschitzienne donc continue.
Ainsi f_1 est continue, définie sur un compact donc atteint ses bornes.
Il existe $b_0 \in [-1,1]$ tel que $\inf\{f_1(b), b \in [-1,1]\} = f_1(b_0) = N(1,b_0) > 0$ car $(1,b_0) \neq 0$.
De même, $K_2 = \{N(u) \mid u = (-1,b) \& b \in [-1,1]\}$, $K_3 = \{N(u) \mid u = (a,1) \& a \in [-1,1]\}$ et $K_4 = \{N(u) \mid u = (a,-1) \& a \in [-1,1]\}$ admettent chacun une borne inférieure strictement positive.
Donc il existe $B > 0$ tel que $B = \inf K$.
On a alors, pour tout $u \in \mathbb{R}^2$, en notant $v = \frac{1}{\|u\|_\infty} u$:
$$N(u) = N(\|u\|_\infty v) = \|u\|_\infty N(v) \geqslant B\|u\|_\infty$$
car $\|v\|_\infty = 1$. □

Pour aller plus loin - Espace vectoriel normé de dimension finie (ex : $\mathbb{K}^n$)
*Soit E est un espace vectoriel normé **de dimension finie**.*
Alors la convergence de toute suite ne dépend pas de la norme considérée.
(soit elle converge vers ℓ pour tout norme, soit elle diverge pour toute norme).
En fait : toutes les normes définie sur E sont équivalentes.

Avec des boules

On raisonne parfois en terme de boules pour élargir la notion d'intervalles :

Définition - Boules ouvertes / fermées
Soit $(E, \|\cdot\|)$ un espace vectoriel normé. Soit $x \in E$ et $\rho \in \mathbb{R}_+^*$. On appelle :
• boule ouverte de centre x et de rayon ρ, l'ensemble $B(x,\rho) = \{y \in E \mid \|x-y\| < \rho\}$.
• boule fermé de centre x et de rayon ρ, l'ensemble $B_f(x,\rho) = \{y \in E \mid \|x-y\| \leqslant \rho\}$

Proposition - Suite - en terme de boule
Dans $(E, \|\cdot\|)$ espace vectoriel normé,
$(x_n) \to x$ si et seulement si $\forall\, \epsilon > 0, \exists\, N \in \mathbb{N}$ tel que $\forall\, n \geqslant N,\ x_n \in B_f(x,\epsilon)$
$$(x_n)_{n\in\mathbb{N}} \to x \Leftrightarrow \bigcap_{\epsilon>0} \bigcup_{N\in\mathbb{N}} \bigcap_{n\geqslant N} B(x_n,\epsilon) = \{x\}$$

2.2. Initiation à la topologie sur un espace normé

Ouverts et fermés

Pour chacun des résultats énoncés (définition et théorème), nous ferons le parallèle avec la situation dans $\mathbb{R}$. Dans toute la suite, $(E, \|\cdot\|)$ un espace vectoriel normé.

Définition - Partie ouverte de E
Une partie Ω de E est dite ouverte si $\Omega = \emptyset$ ou si
$$\forall\, x \in \Omega, \exists\, \rho > 0 \text{ tel que } B(x,\rho) \subset \Omega$$

Exemple - Sur $\mathbb{R}$
Les intervalles ouverts $]a,b[$ de $\mathbb{R}$, sont des ouverts. De même les réunions d'intervalles ouverts de $\mathbb{R}$.
Exemple - Sur $\mathbb{R}^2$
L'ensemble $]0,1[\times]0,1[$ est un ouvert de $\mathbb{R}^2$.

Pour aller plus loin - Topologie
L'ensemble des parties ouvertes de E s'appelle topologie de E

Savoir faire - Montrer qu'une partie est un ouvert. Avec des voisinage!
Pour montrer que O est ouvert, en règle générale on exploite directement la définition et donc des voisinages.

Exercice
Montrer que $A :=]0,1[\times[0,1]$ n'est pas une partie ouverte de $\mathbb{R}^2$

Correction
$b = (\frac{1}{2}, 1) \in A$. $\forall\, \rho > 0$, il existe $x = b + \frac{\rho}{2}(0,1)$ tel que $x \in B_f(b,\rho)$ (pour la norme $\|\cdot\|_\infty$) et $x \notin A$.

Proposition - Stabilité d'ouverts
Les parties $\emptyset$ et E sont des ouverts de E.
Une réunion d'ouverts est un ouvert.
Une intersection finie d'ouverts est un ouvert

Attention - Ce n'est pas le cas d'une intersection infinie dénombrable d'ouverts
$\bigcap_{n\in\mathbb{N}^*}]\frac{-1}{n}, \frac{1}{n}[= \{0\}$, qui n'est pas ouvert

Démonstration
Si $x \in \bigcup_{i\in I} A_i$, alors $\exists\, i \in I$ tel que $x \in A_i$, ouvert.
$\exists\, \rho > 0$ tel que $B(x,\rho) \subset A_i \subset \bigcup_{i\in I} A_i$.
Si $x \in \bigcap_{i=1}^{n} A_i$, alors $\forall\, i \in \mathbb{N}_n$, $x \in A_i$.
$\exists\, \rho_i$ tel que $B(x,\rho_i) \subset A_i$.
On prend $\rho = \min(\rho_i)$ et on a $\forall\, i \in \mathbb{N}_n$, $B(x,\rho) \subset B(x,\rho_i) \subset A_i$
Ainsi $B(x,\rho) \subset \bigcap_{i=1}^{n} A_i$ □

Définition - Partie fermée de E
Une partie F de E est dite fermée si $F = \emptyset$ ou si $E \setminus F$ est un ouvert de E

Exemple - Sur $\mathbb{R}$. Sur E
Les intervalles fermés $[a,b]$ de $\mathbb{R}$, sont des fermés de $\mathbb{R}$. Les singletons $\{x\}$ sont des fermés de E et plus généralement les boules fermés de E sont des fermés.
Exercice
Montrer que $B = B_f(a,r)$ est un fermé de E. On peut s'aide d'un dessin!

Pour aller plus loin - Dessin
En topologie, on peut s'aider facilement d'un dessin.
Mais cela ne fera pas office de démonstration…

Correction
On note $\Omega = E \setminus B$.
$\forall\, x \in \Omega$, $d = \|a-x\| > r$. Soit $\rho = \dfrac{d-r}{2}$. Pour tout $y \in B(x,\rho)$
$$\|a-y\| \geqslant \|a-x\| - \|x-y\| \Longleftrightarrow \|y-a\| \geqslant d-\rho = \frac{2d-d+r}{2} = \frac{d+r}{2} > \frac{r+r}{2} = r$$
Donc $y \notin B$, i.e. $y \in \Omega$. Donc $B(x,\rho) \subset \Omega$
Comme le complémentaire d'une réunion est une intersection :

Proposition - Stabilité de fermés
Les parties $\emptyset$ et E sont des fermés de E.
Une intersection de fermés est un fermé.
Une réunion finie de fermé est un fermé

Exercice
A démontrer

Correction

Attention - Faux pour une réunion infinie dénombrable de fermés
$\bigcup_{n\in\mathbb{N}^*}[\frac{1}{n}, 1-\frac{1}{n}] =]0,1[$, qui n'est pas fermé

Un premier lien avec les suites

Proposition - Caractérisation des fermés
F est un fermé de E
ssi pour toute suite $(x_n) \in F^{\mathbb{N}}$ de F, convergente, on a $\lim(x_n) \in F$

Démonstration
Supposons que F est fermé. Notons $\Omega = E \setminus F$
Soit $(x_n) \in F^{\mathbb{N}} \to \ell$.
Supposons que $\ell \notin F$. Donc $\ell \in \Omega$.
Donc $\exists\, \epsilon > 0$ tel que $B(\ell,\epsilon) \in \Omega$, car Ω est ouvert.
Or $\exists\, N \in \mathbb{N}$ tel que $\forall\ n \geqslant N$, $x_n \in B(\ell,\epsilon)$, donc $x_N \in \Omega$.
Ceci est impossible, donc nécessairement $\ell \in F$.
Réciproquement, supposons que pour toute suite $(x_n) \in F^{\mathbb{N}}$ de F, convergente, on a $\lim(x_n) \in F$.
Soit $r \in \Omega = E \setminus F$.
Si $\forall\ n \in \mathbb{N}$, $\exists\, x_n \in F$ tel que $x_n \in B(r, \frac{1}{n})$, alors $(x_n) \to r$,
mais ceci est impossible, par hypothèse (sinon : $r \in F$)
Donc $\exists\, N \in \mathbb{N}$ tel que $\forall\ x \in F$, $x \notin B(r, \frac{1}{N})$, donc $B(r, \frac{1}{N}) \cap F = \emptyset$, ie $B(r, \frac{1}{N}) \subset \Omega$ □

Savoir faire - Montrer qu'une partie est un fermé. Avec des suites!
Pour montrer que F est fermé, en règle générale on exploite des suites convergentes à limite assurément dans F. Exemple : Montrer qu'un sev de dimension finie est fermé (à l'aide d'une écriture sur une base).

‘

2.3. Topologie relative

Heuristique - Dans $\mathbb{R}^2_+$
L'ensemble $S = \{(x,y) \in \mathbb{R}^2_+ \mid x \geqslant 0, y \geqslant 0, x+y < 1\}$ est-il ouvert ou fermé? Cela semble compliqué.
Dans $\mathbb{R}^2$, $(0,0) \in \mathbb{R}_+$, mais il n'existe aucune boule centré en $(0,0)$ contenu dans S (quel que soit la norme).
Et en même temps $(1,0) \in \overline{S}$ mais il n'existe aucune boule centré en $(1,0)$ contenu dans $\overline{S}$.
Dans $\mathbb{R}^2$, S n'est ni ouvert, ni fermé.
Mais ce n'est pas le cas si l'on regarde QUE dans $\mathbb{R}^2_+$. En effet, dans ce cas, la boule ouverte (euclidienne) centré en $(0,0)$ de rayon $r = \frac{1}{10}$ n'a que des éléments dans S, puisqu'également nécessairement dans $\mathbb{R}^2_+$.
Donc dans $\mathbb{R}^2_+$, S est ouvert.

Définition - Ouvert/fermé relatif à une partie
Si E est l'espace vectoriel normé et A est une partie de E, alors
1. on dit que U est un ouvert relatif à A, si :
$\forall\ x \in U, \exists\, \epsilon > 0$ tel que $B(x,\epsilon) \cap A \subset U$.
2. on dit que V est un fermé relatif à A, si :
$A \setminus V$ est un ouvert relatif de A.

Exemple - Ouvert relatif non ouvert
Notons tout de suite qu'un ouvert relatif n'est pas pas forcément ouvert pour l'espace.
Si on considère $f : [-1,1] \to \mathbb{R}$, $x \mapsto x$ et $O =]-2,0[$, ouvert de $\mathbb{R}$,
Alors, (nous verrons) par continuité de f, $f^{-1}(O) = [-1,0[$ est donc un ouvert (relatif) de $[-1,1]$, mais pas un ouvert de $\mathbb{R}$.
En effet, si $x \in [-1,0[$, il existe $\epsilon (= -\frac{x}{2}) > 0$ tel que $B(x,\epsilon) \cap [-1,1] \subset [-1,0[$ (même pour $x = 1$).

Proposition - Caractérisations rapides
Soit A une partie de E. On a alors les caractéristiques importantes :
- U est un ouvert relatif de A si et seulement si il existe O ouvert de E tel que $U = O \cap A$.
- V est un fermé relatif de A si et seulement si il existe F fermé de E tel que $V = F \cap A$.

Démonstration
Supposons qu'il existe O ouvert de E tel que $U = O \cap A$.
Soit $x \in U$, donc $x \in O$ (et A).
Ainsi $\exists\, \rho > 0$ tel que $B(x,\rho) \subset O$, et donc
$\forall\ y \in A$, si $\|y - x\| < \epsilon$, alors $y \in O \cap A = U$. Donc U est un ouvert (de A).
Réciproquement, si U est un ouvert relatif de A.
Pour tout $x \in U$, alors il existe $\epsilon_x > 0$ tel que $B(x,\epsilon_x) \cap A \subset U$.
On note $O = \bigcup_{x\in U} B(x,\epsilon_x)$, réunion d'ouverts de E, donc partie ouverte de E.
Et enfin, pour tout $a \in O \cap A$, $\exists\, x \in U, \epsilon_x > 0$ tel que $a \in B(x,\epsilon_x) \cap A \subset U$.
réciproquement si $a \in U$, alors $a \in A$ et $a \in B(a,\epsilon_a) \subset O$, donc $a \in A \cap O$.
Donc $U = O \cap A$.
V est un fermé relatif de A ssi $A \setminus V$ est un ouvert relatif de A,
ssi $\exists\, O$ ouvert de E tel que $\overline{V} = A \setminus V = O \cap A$.
ssi $\exists\, F = \overline{O}$ fermé de F tel que $V = F \cap A$ (en passant au complémentaire). □

2.4. Compact

Définition - Compact (propriété de Bolzano-Weierstrass)
On dit qu'un ensemble $K \subset E$ est compact,
si pour toute suite d'éléments de K, on peut extraire une suite convergente dans K.
Formellement : $\forall\ (x_n) \in K^{\mathbb{N}}, \exists\, x \in K, \varphi : \mathbb{N} \to \mathbb{N}\nearrow\nearrow$ tel que $x_{\varphi(n)} \to x$.

On a une caractérisation simple des compacts de $\mathbb{R}^n$:

Pour aller plus loin - Normes équivalentes
Pour démontrer classiquement que toutes les normes sont équivalentes dans $\mathbb{K}^n$, on exploite les propriétés d'optimalité sur des compacts

Proposition - Compact de $\mathbb{R}^p$
Les compacts de $\mathbb{R}^p$ sont exactement les parties fermées et bornées de $\mathbb{R}^p$

On notera que dans la première partie de la démonstration, on n'a pas exploité que $E = \mathbb{R}^n$.

Démonstration
Si K est un compact de $\mathbb{R}^p$.
Alors K est fermé, puisque si l'on considère une suite convergente (x_n) vers x,
alors toute extraction de (x_n) convergera vers x et nécessairement $x \in E$.

Et K est borné. Supposons le contraire : $\forall\, M\in\mathbb{R}_+, \exists\, x\in E$ tel que $\|x\|>M$.
on peut donc créer une suite $(x_n)\in K^{\mathbb{N}}$ tel que $\forall\, n\in\mathbb{N}, \|x_n\|\geqslant n$.
Notons $x=\lim(x_{\varphi(n)})$, alors $\forall\, n\in\mathbb{N}, \|x_{\varphi(n)}\|\geqslant\varphi(n)$
et à partir d'un certain rang : $\|(x_{\varphi(n)})\|>\|x\|+1$. Impossible.
Réciproquement. Supposons que K est fermé et borné.
Soit (x_n) une suite de $K\subset\mathbb{R}^p$. Supposons que $x_n=(x_n^1,x_n^2\dots x_n^p)$.
Alors (x_n^1) est une suite bornée de $\mathbb{R}$. Elle admet une sous-suite convergente : $x^1_{\varphi_1(n)}\to x^1$.
Alors $(x^2_{\varphi_1(n)})$ est une suite bornée de $\mathbb{R}$. Elle admet une sous-suite convergente : $x^2_{\varphi_1(\varphi_2(n))}\to x^2$.
(…) Alors (x_n^p) est une suite bornée de $\mathbb{R}$. Elle admet une sous-suite convergente : $x^p_{\varphi_1\circ\cdots\circ\varphi_p(n)}\to x^p$.
Notons $\psi=\varphi_1\circ\cdots\circ\varphi_p$. Comme K est fermé, $x=\lim x_{\psi(n)}\in K$. Donc K compact. □

On a une propriété *essentielle* comparable au lemme de Cousin :

Théorème - Caractérisation Borel-Lebesgue
Soit E un espace normé. Soit $K\subset E$.
K est compact si et seulement si pour toute famille d'ouverts recouvrant K, on peut en extraire un recouvrement fini.
Formellement : $\forall\,(O_i)\in\mathscr{P}(E)^I$ famille d'ouverts de E telle que $K\subset\bigcup_{i\in I}O_i$,
$\exists\, J\subset I$, **fini** tel que $K\subset\bigcup_{i\in J}O_i$.

Exercice
A-t-on le lemme de Cousin en toute dimension ?
Si K est compact, est-ce que pour tout $\delta: K\to\mathbb{R}_+^*$,
il existe $N\in\mathbb{N}$, $x_1,x_2,\dots x_N\in K$ tel que $K\subset\bigcup_{i=1}^N B\big(x_i,\frac{\delta(x_i)}{2}\big)$?
où $B\big(x_i,\frac{\delta(x_i)}{2}\big)$ est la boule ouverte de centre x_i et de rayon $\frac{\delta(x_i)}{2}$.

Correction
Evidemment, on a le recouvrement $K\subset\bigcup_{x\in K}B\big(x,\frac{\delta(x)}{2}\big)$.
On peut en extraire un recouvrement fini.
On propose la démonstration du théorème à l'aide d'un exercice (avec beaucoup de raisonnements par l'absurde).

Exercice
1. On considère K un compact de E.
   (a) Montrer que pour tout $\epsilon>0$, il existe $N\in\mathbb{N}$, $x_1,\dots x_n\in K$ tel que $K\subset\bigcup_{i=1}^n B(x_i,\epsilon)$.
   On dit que K est précompact
   (b) Soit $(O_i)_{i\in I}$ un recouvrement de K par des ouverts.
   Montrer qu'il existe $\alpha>0$ tel que $\forall\, x\in K, \exists\, i\in I$ tel que $B(x,\alpha)\subset O_i$
   (c) En déduire le sens direct du théorème.
2. On suppose que K vérifie la propriété d'extraction finie de recouvrements (dite de Borel-Lebesgue).
   (a) On considère une suite (F_n) décroissante, de fermés non vide de K. Montrer que $\bigcap_{n\in\mathbb{N}}F_n\neq\emptyset$.
   (b) En déduire la réciproque du théorème.

Correction
1. (a) Soit $\epsilon>0$. Soit $x_1\in K$. Définissons (si possible) par récurrence la suite (x_n) par : x_n existe et $x_{n+1}\in K\setminus\bigcup_{i=1}^n B(x_i,\epsilon)$.
Supposons qu'on a ainsi définie une suite infinie (dénombrable).
On peut extraire de (x_n) une sous-suite convergente $(x_{\varphi(n)})\to x\in K$.
Il existe n_0, tel que $\forall\, n\geqslant n_0, |x_{\varphi(n)}-x|<\frac{\epsilon}{3}$,
donc par inégalité triangulaire : $x_{\varphi(N+1)}\in B(x_{\varphi(n)},\epsilon)$.
Ce qui est contradictoire, donc la définition constructive de (x_n) s'arrête à un rang N.
On a alors $K\setminus\bigcup_{i=1}^N B(x_i,\epsilon)=\emptyset$ donc $K\subset\bigcup_{i=1}^N B(x_i,\epsilon)$.

(b) Raisonnons par l'absurde. Supposons que $\forall\,\alpha>0$ tel que $\exists\, x\in K$, tel que $\forall\, i\in I$ tel que $B(x,\alpha)\not\subset O_i$.
Prenons $\alpha\leftarrow\frac{1}{n}$. On crée une suite $(x_n)\in K^{\mathbb{N}}$ telle que $\forall\, i\in I$, $B(x_n,\frac{1}{n})\not\subset O_i$.
On peut extraire de (x_n) une suite convergente dans K, notée $(x_{\varphi(n)})\to x\in K$.
Il existe $i_0\in I$ tel que $x\in O_{i_0}$, puisque $(O_i)_{i\in I}$ recouvre K.
O_{i_0} est un ouvert donc il existe $\eta>0$ tel que $B(x,\eta)\subset O_{i_0}$.
La suite $(\varphi(n))\to+\infty$ et est croissante. Il existe $m_1\in\mathbb{N}$ tq $\forall\, n\geqslant m_1:\frac{1}{\varphi(n)}\leqslant\frac{\eta}{3}$.
Et $x_{\varphi(n)}\to x$, donc il existe $m_2\in\mathbb{N}$ tel que $\forall\, n\geqslant m_2$, $\|x-x_{\varphi(n)}\|\leqslant\frac{\eta}{3}$.
Soit $m=\max(m_1,m_2)$. Soit $a\in B(x_{\varphi(m)},\frac{1}{\varphi(m)})$, alors

$$\|a-x\|\leqslant\|a-x_{\varphi(m)}\|+\|x_{\varphi(m)}-x\|\leqslant 2\frac{\eta}{3}$$

Donc $B(x_{\varphi(m)},\frac{1}{\varphi(m)})\subset B(x,\eta)\subset O_{i_0}$. Contradiction.

(c) Soit $(O_i)_{i\in I}$ un recouvrement de K par des ouverts. Donc il existe $\alpha>0$, tel que $\forall\, x\in K$, $\exists\, i(x)\in I$ tel que $B(x,\alpha)\subset O_{i(x)}$.
Puis avec $\epsilon\leftarrow\alpha$, $\exists\, N, x_1,\dots x_N\in K$ tel que $K\subset\bigcup_{k=1}^N B(x_k,\alpha)\subset\bigcup_{k=1}^N O_{i(x_k)}$.
(il n'est pas impossible que $i(x_k)=i(x_h)\dots$, mais cela ne change rien), on a recouvert K avec un nombre fini d'ouverts.

2. (a) Raisonnons par l'absurde. Supposons que $\bigcap_{n\in\mathbb{N}}F_n=\emptyset$.
Notons $K=K\setminus\emptyset=K\setminus\bigcap_{n\in N}F_n=\bigcup_{n\in\mathbb{N}}(K\setminus F_n)$.
Ainsi, K est recouvert par les ouverts : $O_n=E\setminus F_n$.
Il existe donc $J\subset\mathbb{N}$, **fini** tel que $K\subset\bigcup_{n\in J}O_n$.
Exploitons maintenant la décroissance : $F_{n+1}\subset F_n$, donc $O_n\subset O_{n+1}$ et donc $K\subset O_N$.
Ainsi $F_N=\emptyset$. Impossible
(b) Soit $(x_n)\in K^{\mathbb{N}}$, une suite d'éléments de K.
Soit $F_n=\overline{\{x_p,p\geqslant n\}}$. Alors F_n est fermé, $x_n\in F_n$ donc F_n non vide.
Enfin $\{x_p,p\geqslant n+1\}\subset\{x_p,p\geqslant n\}\subset F_n$.
Comme F_n est fermé, en prenant l'adhérence : $F_{n+1}\subset F_n$.
On peut appliquer le résultat précédent, et il existe $x\in F_n$, pour tout $n\in\mathbb{N}$.
On a alors x est limite de suite extraite de (x_n).

2.5. Adhérences et intérieurs

Remarque - Cas « pathologique » …
Les fermés ou les ouverts sont deux cas typiques exceptionnels : la frontière est à prendre dans son ensemble (fermés) ou la frontière est à rejeter dans son ensemble (ouverts). La plupart du temps les cas sont plus intermédiaires…

Définition - Adhérence
Soit A une partie de E.
On note $\overline{A}=\{x\in E\mid\forall\,\epsilon>0,\exists\, a\in A\mid\|x-a\|<\epsilon\}=\bigcap_{\epsilon>0}\Big(\bigcup_{a\in A}B(a,\epsilon)\Big)$.
Alors $A\subset\overline{A}$. $\overline{A}$ est un fermé.
En fait , $\overline{A}=\bigcap_{F\in\mathscr{F}_A}F$, où $\mathscr{F}_A$ est l'ensemble de tous les fermés contenant A.
C'est une borne supérieure : $\overline{A}$ est le plus petit fermé contenant A.
En particulier A est fermé si et seulement si $\overline{A}=A$.

Démonstration
Soit $a\in A$, $\forall\,\epsilon>0$, $\|a-a\|<\epsilon$, donc $a\in\overline{A}$. Ainsi $A\subset\overline{A}$.
$\overline{A}$ est un fermé : Soit (x_n) est une suite convergente vers x d'éléments de $\overline{A}$.
Soit $\epsilon>0$, $\exists\, N\in\mathbb{N}$ tel que $\|x_N-x\|<\frac{\epsilon}{2}$ et $\exists\, a\in A$ tel que $\|x_N-a\|<\frac{\epsilon}{2}$ car $x_N\in\overline{A}$.
Par inégalité triangulaire, $\|x-a\|<\epsilon$. Donc $x\in\overline{A}$.
Si A est un fermé, alors
$\forall\, a\in\overline{A}$, $\forall\, n\in\mathbb{N}$, $(\epsilon=\frac{1}{n})$, $\exists\, a_n\in A$ tel que $\|a-a_n\|<\frac{1}{n}$, donc $a=\lim(a_n)$ avec $(a_n)\in A^{\mathbb{N}}$.
Donc $a\in A$, car A est fermé.
Donc si A est fermé, alors $\overline{A}=A$ (l'inclusion $A\subset\overline{A}$ est triviale). Soit G fermé contenant A.
Alors $\forall\,\epsilon>0$, $\bigcup_{a\in A}B(a,\epsilon)\subset\bigcup_{g\in G}B(g,\epsilon)$.
Puis $\bigcap_{\epsilon>0}\Big(\bigcup_{a\in A}B(a,\epsilon)\Big)\subset\bigcap_{\epsilon>0}\Big(\bigcup_{g\in G}B(g,\epsilon)\Big)=\overline{G}=G$ □

Savoir faire - Caractérisation de $x \in \overline{A}$

Soit A une partie quelconque de E. Un élément $x \in \overline{A}$ si l'une des assertions suivantes est vérifiée :

i) $\forall\, \epsilon > 0, \exists\, a \in A$ tel que $\|x-a\| < \epsilon$
ii) $\forall\, \epsilon > 0, B(x,\epsilon) \cap A \neq \emptyset$
iv) $\exists\, (x_n) \in A^{\mathbb{N}}$ tel que $\lim(x_n) = x$.
iii) $d(x,A) = 0$

Exercice
Montrer que ces assertions sont équivalentes.
Montrer qu'elles signifient bien équivalente à $x \in \overline{A}$

Correction
i) et ii) sont clairement équivalentes. Et iii) également.
Si $i)$ est vérifiée en prenant $\epsilon = \frac{1}{n}$, on crée une suite de vecteurs $(a_n) \in A$ tel que $x = \lim(a_n)$.
Or ces vecteurs sont dans A donc dans $\overline{A}$, qui est fermé. Donc $x \in \overline{A}$.
Réciproquement, Si $\exists\, \epsilon > 0$ tel que $B(x,\epsilon) \cap A = \emptyset$.
Alors comme $B(x,\epsilon)$ est un ouvert, $E \setminus B(x,\epsilon)$ est un fermé, il qui contient A.
Donc $\overline{A} \subset E \setminus B(x,\epsilon)$ et donc $x \notin A$.

Définition - Partie dense
Une partie A est dite dense dans E si $\overline{A} = E$

Définition - Intérieur
Soit A une partie de E.
On note $A^o = \{x \in E \mid \exists\, \epsilon > 0, \forall\, a : \|x-a\| < \epsilon \Rightarrow a \in A\}$ Alors $A^o \subset A$. A^o est un ouvert.
En fait , $A^o = \bigcup_{O \in \mathscr{O}_A} O$, où $\mathscr{O}_A$ est l'ensemble des ouverts inclus dans A.
C'est une borne inférieure : A^o est le plus grand ouvert contenu dans A.
En particulier A est ouvert si et seulement si $A^o = A$.

Savoir faire - Caractérisation de $x \in A^o$

Soit A une partie quelconque de E. Un élément $x \in A^o$ si l'une des assertions suivantes est vérifiée :

i) A est un voisinage de x
ii) $\exists\, \epsilon > 0, B(x,\epsilon) \subset A$

Démonstration
A^o est un ouvert : Soit $x \in A^o$, donc il existe $\epsilon > 0$ tel que $B(x,\epsilon) \subset A$.
Soit $u \in B(x, \frac{\epsilon}{3})$,
Pour tout $z \in B(u, \frac{\epsilon}{3})$, alors $\|z-u\| < \frac{\epsilon}{3}$ et $\|u-x\| < \frac{\epsilon}{3}$.
Donc par inégalité triangulaire : $\|z-x\| \leqslant \|z-u\| + \|u-x\| < \frac{2\epsilon}{3}$, donc $z \in B(x,\epsilon) \subset A$.
Donc pour tout $u \in B(x, \frac{\epsilon}{3})$, il existe $\epsilon' (= \frac{\epsilon}{3})$ tel $B(u,\epsilon') \subset A$,
Ainsi pour tout $u \in B(x, \frac{\epsilon}{3})$, $u \in A^o$.
Par conséquent, pour tout $x \in A^o$, il existe ϵ'' tel que $B(x,\epsilon'') \subset A^o$.
Tous les ouverts de A sont dans A^o :
Soit $x \in \Omega$ un ouvert de A. Donc il existe $\epsilon > 0$ tel que $B(x,\epsilon) \subset \Omega \subset A$. □

3. Continuité

3.1. Limite

Définition

Définition - Limite (et continuité)
Soit $f : E \to F$, une application entre deux espaces vectoriels normés.
On dit que f admet en $x_0 \in E$, une limite égale à $f(x_0)$ si l'une des propriétés suivantes (équivalentes) est vérifiée :

$$\forall\, \epsilon > 0, \exists\, \eta > 0 \mid \forall\, x \in E, \|x - x_0\|_E \leqslant \eta \Longrightarrow \|f(x) - f(x_0)\|_F \leqslant \epsilon$$

$$\forall\, \epsilon > 0, \exists\, \eta > 0 \mid f\big(B(x_0,\eta)\big) \subset B(f(x_0),\epsilon)$$

$$\forall\, (x_n) \in E^{\mathbb{N}} \text{ telle que } (x_n) \to x_0, \quad \big(f(x_n)\big) \to f(x_0)$$

On note alors $f(x_0) = \lim\limits_{x \to x_0} f(x)$.

Il faudrait montrer l'équivalence entre ces définitions. La première et la seconde sont évidemment semblables, il s'agit juste d'une réécriture en terme de boules (les implications et les inégalités deviennent des inclusions).
Nous étudierons l'équivalence avec la troisième définition dans la partie suivante.

Définition - Continuité en un point
Soit a un point adhérent de $A := \mathscr{D}_f$. Si f admet une limite au point a, on dit que :
— f *est continue en* a si $a \in A$ et que $\lim_{x \to a} f(x) = f(a)$.
— f *se prolonge par continuité en* a si $a \notin A$ mais a est adhérent à A.
on *définit* alors $f(a) := \lim_{x \to a} f(x)$.

Définition - Continuité sur une partie
On dit que f *est continue sur une partie* A de E,
si f est continue en tout $a \in A$

Remarque - Indépendance par rapport à la norme
On rappelle que sur E et F, en **dimension finie**, les normes sont équivalentes, donc les définitions de limite, continuité en un point, continuité sur une partie sont indépendantes des normes choisies.

Exemple - Exemples
Les applications linéaires (en dimension finie), les applications polynomiales (algèbre?), les normes, les applications bilinéaires (en dimension finie) sont continues.
La composition de deux fonctions continues est continue.

Exercice
La fonction $f : \mathbb{R}^2 \to \mathbb{R}$, $(x,y) \mapsto \dfrac{xy}{x^2+y^2}$ est-elle continue sur $[-1,1] \times [-1,1]$?

Correction
Elle n'est pas continue en 0. Aucune valeur particulière ne peut être donnée à $f(0,0)$
En effet, $f(x,0) = 0 = f(0,y)$, mais $f(x,x) = \frac{1}{2}\ldots$

Caractérisation par coordonnées

Proposition - Caractérisation par coordonnées
Soit E et F deux espaces vectoriels de dimension finie, normés.
Supposons que $(e_1, e_2, \ldots e_p)$ est base de F. Soit A une partie de E. Soit a un point adhérent de A
Soit f une application de A dans F. Soit $b = \sum_{i=1}^{p} b_i e_i \in F$.

On suppose que $f = \sum_{i=1}^{p} f_i e_i$.
Alors : f admet b comme limite au point a,
si et seulement si, $\forall\, i \in \mathbb{N}$, f_i admet b_i comme limite au point a.

Démonstration
En fait la seconde proposition correspond à la convergence de la norme uniforme $\|b\|_\infty = \max_{i\in\mathbb{N}_p} |b_i|$.
Comme on se trouve sur des espaces vectoriels de dimension finie, les normes sont équivalentes.
□

On ne s'intéressera maintenant qu'aux situations où $F = \mathbb{R}$.

Continuité et topologie

La continuité est la meilleure façon de transformer des fermés en fermés, des ouverts en ouverts… : d'étudier les topologies d'ensembles.

Proposition - Image réciproque
Soit $f : E \to F$, continue, alors :
— si $B \subset F$ est ouvert, alors $f^{-1}(B)$ est un ouvert.
— si $B \subset F$ est fermé, alors $f^{-1}(B)$ est un fermé.

Application - Sous-espace vectoriel de dimension finie
Soit $B_1 = (e_1, \cdots e_p)$ une base de F, complétée en $B = (e_1, \cdots e_p, \cdots e_n)$ base de E.
Soit $h : E \to \mathbb{R}^n$, $u \mapsto (u_1, \cdots u_n)$.
Alors $F = h^{-1}(\mathbb{R}^p \times \{0\}^{n-p})$. Ce dernier ensemble est un fermé de $\mathbb{R}^n$.

Attention - Image directe ?
Ce résultat est vraie pour les images réciproque, mais pas les images directes.
On a par ailleurs une équivalence : f est continue, si et seulement si l'image réciproque de tout ouvert (resp. fermé) de F est un ouvert (resp. fermé) de E.

Démonstration
Supposons que B est un ouvert de F.
Soit $x \in f^{-1}(B)$, i.e. $f(x) \in B$.
B est un ouvert, donc il existe $\epsilon > 0$ tel que $B(x,\epsilon) \subset B$.
Puis f est continue en x, donc $\exists\, \eta > 0$ tel que $f(B(x,\eta)) \subset B(f(x),\epsilon) \subset B$.
Donc tout élément de $B(x,\eta)$ a une image par f dans B, ie $B(x,\eta) \subset f^{-1}(B)$.
Ainsi $f^{-1}(B)$ est un ouvert de E.
Supposons que B est un fermé de F.
Soit (x_n) suite d'éléments de $f^{-1}(B)$ convergente.
pour tout $n \in \mathbb{N}$, $f(x_n) \in B$ et $(x_n) \to x$.
Puis par continuité de f, $(f(x_n))$ converge et $\lim f(x_n) = f(x)$.
Mais B est fermé donc $f(x) \in B$ et ainsi $x \in f^{-1}(B)$. Ainsi $f^{-1}(B)$ est un fermé de E.
□

Exercice
Soit $B = \{(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \mid \frac{x+y}{x^2+y^2} > 1\}$. B est-il ouvert ?
Soit $C = \{(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \mid \frac{x+y}{x^2+y^2} \geqslant 1\}$. C est-il ouvert ? C est-il fermé ?

Correction
Le premier réflexe (normalement…) pour résoudre cet exercice est de considérer $\varphi : (x,y) \mapsto \frac{x+y}{x^2+y^2}$.
On a alors, $B = \varphi^{-1}(]1,+\infty[)$, image réciproque d'un ouvert ; alors que $C = \varphi^{-1}([1,+\infty[)$, image réciproque d'un fermé.
Ainsi, sous réserve de continuité de φ, on doit pouvoir conclure que B et C sont respectivement un ouvert et un fermé de $\mathbb{R}^2$.

Etudions donc la continuité de φ. Cela commence toujours par l'ensemble de définition.
$\mathscr{D}_\varphi = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 \neq 0\} = \mathbb{R}^2 \setminus \{(0,0)\}$
Ensuite, on se concentre sur la continuité :
- $(x,y) \mapsto x+y$ est polynomiale donc continue sur $\mathbb{R}^2$
- $(x,y) \mapsto x^2+y^2$ est polynomiale donc continue sur $\mathbb{R}^2$
- $t \mapsto \frac{1}{t}$ est continue sur son ensemble de définition ($\mathbb{R}^*$)
- Par composition $(x,y) \mapsto \frac{1}{x^2+y^2}$ est continue sur son ensemble de définition.
- Par produit φ est continue sur son ensemble de définition : $\mathscr{D}_\varphi = \mathbb{R}^2 \setminus \{(0,0)\}$.

MAIS ceci est faux (en tout cas la conclusion).
Le théorème ne s'applique pas tout à fait. Le théorème énonce :
Si $\varphi : E \to F$ continue et si $B = \varphi^{-1}(O)$, avec O ouvert de F, alors B est un ouvert.
SOUS-ENTENDU : un ouvert de E.
Dans l'exemple précédent, on a $E = \mathbb{R}^2 \setminus \{(0,0)\}$, donc B est un ouvert de E et C est un fermé de E.
Mais $E \neq \mathbb{R}^2$ et la question est : est-ce que B et C sont ouvert/fermé de $\mathbb{R}^2$?
On peut méditer l'exemple qui suivra.
1. B est donc un ouvert relatif à $\mathbb{R}^2 \setminus \{(0,0)\}$,
donc il existe O ouvert de $E := \mathbb{R}^2$ tel que $B = O \cap (\mathbb{R}^2 \setminus \{(0,0)\}$.
mais $\mathbb{R}^2 \setminus \{(0,0)\}$ est un ouvert de $\mathbb{R}^2$ (complémentaire d'un fermé),
donc B est l'intersection de deux ouverts, il s'agit donc d'un ouvert de $\mathbb{R}^2$.
Si Y est ouvert dans X, tout ouvert de Y est un ouvert de X : cela découle du fait que l'intersection de deux ouverts est ouverte.
(De même, si Y est fermé dans X, tout fermé de Y est un fermé de X.).
2. C est un fermé relatif à $\mathbb{R}^2 \setminus \{(0,0)\}$, mais celui-ci n'est pas un fermé de $\mathbb{R}^2$.
Il y a donc un peu de fermé (lié à C) et un peu d'ouvert (lié à $\mathbb{R}^2 \setminus \{(0,0)\}$…
Soit, pour $n \in \mathbb{N}^*$, $u_n = (\frac{1}{n}, \frac{1}{n})$, alors $\varphi(u) = \frac{\frac{2}{n}}{\frac{2}{n^2}} = n \geqslant 1$.
donc $u_n \in C$ et la suite (u_n) converge vers $(0,0) \notin C$. Donc C n'est pas fermé (de $\mathbb{R}^2$).
Soit $v = (1,0)$, alors $v \in C$ car $\varphi(v) = 1$.
Soit $\epsilon > 0$, $v_\epsilon = (1, -\frac{\epsilon}{2})$, alors $\varphi(v_\epsilon) = \frac{1-\frac{\epsilon}{2}}{1+\frac{\epsilon}{4}} < 1$ car $-\frac{\epsilon}{2} < 0 < \frac{\epsilon^2}{4}$.
Donc $v_\epsilon \notin C$, alors que $v_\epsilon \in B(v,\epsilon)$ (pour $\|\cdot\|_\infty$). Donc C n'est pas un ouvert.

Savoir faire - Contournement du problème pour exploiter l'image réciproque
Pour éviter le problème en $(0,0)$, on peut aussi considérer les équivalences :
$$\frac{x+y}{x^2+y^2} > 1 \iff x+y > x^2+y^2 \,\&\, (x,y) \neq (0,0) \iff \psi(x,y) := x^2+y^2-x-y > 0 \,\&\, (x,y) \neq (0,0)$$

3.2. Critère de continuité (ou non) à l'aide de suites

Proposition - Caractérisation séquentielle
Soit E et F deux espaces vectoriels de dimension finie, normés.
Soit A une partie de E. Soit a un point adhérent de A
Soit f une application de A dans F. Soit $b \in F$.
Alors : f admet b comme limite au point a,
si et seulement si, $\forall\, (x_n) \to a \Rightarrow f(x_n) \to b$.

Démonstration
Supposons que f admet b comme limite en a.
Soit $\epsilon > 0$.
Il existe $\delta > 0$ tel que $\forall\, x \in A$, $\|x-a\| \leqslant \delta \Rightarrow \|f(x)-b\| \leqslant \epsilon$.
Soit (x_n) convergente vers a. Donc $\exists\, N \in \mathbb{N}$ tel que $\forall\, n \geqslant N$, $\|x_n - a\| \leqslant \delta$.
Donc $\exists\, N \in \mathbb{N}$ tel que $\forall\, n \geqslant N$, $\|f(x_n) - f(a)\| \leqslant \epsilon$.
Cela signifie bien que $(f(x_n))$ converge vers b.
Pour la réciproque, on fait un raisonnement en contraposée.
Si f n'admet pas de limite en a, alors il est possible de créer une suite (u_n) qui converge vers a, mais telle que $f(u_n)$ ne converge pas vers b.
□

Savoir faire - Un bon critère de non continuité

Si une fonction est telle que $f(u_n)$ et $f(v_n)$ admettent deux limite différentes alors que (u_n) et (v_n) ont même limite, c'est qu'elle n'est pas continue.

Ainsi avec $f:\mathbb{R}^2\to\mathbb{R}$, $(x,y)\mapsto\dfrac{xy}{x^2+y^2}$, on a :

— avec $(u_n)=(\frac{1}{n},0)$ qui converge vers $(0,0)$, $f(u_n)=0$ qui converge vers 0.

— avec $(v_n)=(\frac{1}{n},\frac{1}{n})$ qui converge vers $(0,0)$, $f(v_n)=\dfrac{\frac{1}{n^2}}{2\frac{1}{n^2}}=\dfrac{1}{2}$ qui converge vers $\frac{1}{2}$.

Donc f ne peut pas être continue en 0.

Une autre méthode qui marche souvent est d'étudier le terme dominant en rendant unidimensionnel les variables, c'est-à-dire en considérant $y=\lambda x$.

Alors $f(x,y)=f_\lambda(x)$, on étudie alors les limites possibles de $f_\lambda(x)$, pour x tendant vers 0, selon λ.

Si les limites dépendent de λ, alors f ne peut pas être continue.

Ici : $f_\lambda(x)=f(x,\lambda x)=\dfrac{\lambda x^2}{(1+\lambda^2)x^2}=\dfrac{\lambda}{1+\lambda^2}$, limite qui dépend de λ.

Donc $f(0,0)$ n'a pas de valeur unique…

Remarque - Autre utilisation : $u_{n+1}=f(u_n)$

Si (u_n) est une suite vectorielle définie par récurrence par $u_{n+1}=f(u_n)$,
et si (u_n) converge et que f est continue,
alors la limite ℓ de (u_n) vérifie $\ell=f(\ell)$, même si f dépend de plusieurs variables.

3.3. Exemple d'applications continues

Proposition - Application lipschitzienne
Soit $f:A\subset E\to F$ une application k-lipschitzienne.
Alors f est continue

Puisque $\|\cdot\|$ est 1-lipschitzienne :

Savoir faire - Continuité de $\|\cdot\|$

L'application $E\to\mathbb{R}$, $x\mapsto\|x\|$ est continue sur E.
Soit $x_0\in A$, alors $\forall\, x\in A$, $\|f(x)-f(x_0)\|\leqslant k\|x-x_0\|$.
Soit $\epsilon>0$, alors avec $\delta=\frac{\epsilon}{k}$, on a :
$\forall\, x\in A$, $\|x-x_0\|\leqslant\delta\Rightarrow\|f(x)-f(x_0)\|\leqslant k\delta=\epsilon$.
Ceci étant vrai pour tout x_0, f est continue sur A en entier

Proposition - Applications composées
Soient E,F,G trois espaces vectoriels de dimension finie et normés.
Soient $f:A\subset E\to F$, $g:B\subset F\to G$ continues et telles que $f(A)\subset B$.
Alors : $g\circ f:A\subset E\to G$ est continue.

Démonstration
Soit $x_0\in A$. Notons $y_0=f(x_0)$. Soit $\epsilon>0$. Alors,
1. il existe δ_1 tel que $\forall\, y\in B$, $\|y-y_0\|\leqslant\delta_1\Rightarrow\|g(y)-g(y_0)\|\leqslant\epsilon$.
2. il existe δ_2 tel que $\forall\, x\in A$, $\|x-x_0\|\leqslant\delta_2\Rightarrow\|f(x)-f(x_0)\|\leqslant\delta_1$.

Donc, $\forall\, x\in A$, $\|x-x_0\|\leqslant\delta_2\Rightarrow\|f(x)-f(x_0)\|\leqslant\delta_1\Rightarrow\|g\circ f(x)-g\circ f(x_0)\|\leqslant\epsilon$ ($f(x)=y$ et $f(x_0)=y_0$.
Ceci est vrai pour tout $x_0\in A$) □

Proposition - (et définition)Polynômes de plusieurs variables
On appelle fonctions polynomiales de n variables, les applications de la forme :
$f:\mathbb{K}^n\to\mathbb{K}$, $(x_1,x_2,\dots x_n)\mapsto\sum_{k=1}^{p}a_k x_1^{\alpha_{1,k}}\times x_2^{\alpha_{2,k}}\cdots\times x_n^{\alpha_{n,k}}$,
où $a_k\in\mathbb{K}$ et $\alpha_{i,j}\in\mathbb{N}$.
Il s'agit de combinaison linéaire de puissances des x_i.
Cette définition étend celle des fonctions polynomiales à une seule variable.
Les fonctions polynomiales de n variables sont continues sur $\mathbb{K}^n$

Exemple - Déterminant

Le déterminant est obtenu par un calcul de type polynomiale à partir des coefficients de la matrice. Par exemple

$$\det\begin{pmatrix}x_1&x_2&x_3\\x_4&x_5&x_6\\x_7&x_8&x_9\end{pmatrix}=1x_1x_5x_9+1x_4x_8x_3+1x_7x_2x_6-1x_1x_8x_6-1x_4x_2x_9-1x_7x_5x_3$$

Donc en tant que fonctions des coefficients de la matrice, det est une application continue de $\mathbb{K}^{n^2}$

Exercice

Montrer que $f:(x,y,z)\mapsto(\ln(xy^2),\frac{x+y}{z},x^2y+y^2z+z^2x)$ est continue sur une partie A de $\mathbb{R}^3$ à préciser

Correction
Le plus important est la question de l'ensemble de définition.
Pour la première coordonnée, il faut que $x>0$ et $y\neq0$.
Pour la deuxième coordonnée, il faut que $z\neq0$.
Pour la troisième coordonnée, il n'y a pas de contrainte.
Donc $D_f=\{(x,y,z)\mid x>0,y\neq0,z\neq0\}$ Par composition les applications $f_1:(x,y,z)\mapsto\ln(xy^2)$, $f_2:(x,y,z)\mapsto\frac{x+y}{z}$ et $f_3:(x,y,z)\mapsto x^2y+y^2z+z^2x$ sont continues sur D_f.
Par conséquent, les applications coordonnées étant continues, f est continue sur D_f.

Savoir faire - Montrer qu'une application est continue

Lorsqu'il faut montrer qu'une fonction de plusieurs variables est continue il faut :

1. bien étudier l'ensemble de définition
2. montrer par composition de fonctions continue de $\mathbb{R}$ dans $\mathbb{R}$ et de fonctions polynomiales que f est continue sur une grande partie de l'ensemble de définition
3. terminer par l'étude aux points frontières.
   En règle générale, il faut chercher les ordres maximaux et les comparer (cf. exercice suivant)

Exemple - $f:(x,y)\mapsto\dfrac{\ln(1+xy)}{\sqrt{x^2+y^2}}$

Ainsi pour l'étude de la continuité de $f:(x,y)\mapsto\dfrac{\ln(1+xy)}{\sqrt{x^2+y^2}}$, cela donne :

1. Pour que $f(x,y)$ soit bien définie, il faut et il suffit que $x^2+y^2>0$ donc $(x,y)\neq(0,0)$ et que $1+xy>0$, donc $y>-\frac{1}{x}$ si $x>0$ et $y<-\frac{1}{x}$ si $x<0$.
   Finalement on a $\mathscr{D}_f=\left\{(x,y)\mid\left(x>0\text{ et }y\in]-\frac{1}{x},0[\cup]0,+\infty[\right)\text{ ou }\left(x<0\text{ et }y\in]-\infty,0[\cup]0,-\frac{1}{x}[\right)\right\}$
2. Les applications $(x,y)\mapsto x^2+y^2$ et $(x,y)\mapsto1+xy$ sont continues de $\mathbb{R}^2$ sur $\mathbb{R}$.
   Les applications $z\mapsto\ln z$ et $z\mapsto\frac{1}{\sqrt{z}}$ sont continue sur leur $\mathbb{R}_+^*$.
   Par composition et multiplication, f est continue sur son ensemble de définition $\mathscr{D}_f$.
3. Ensuite il s'agit d'élargir l'ensemble de définition/continuité en voyant si l'on peut faire un prolongement.
   — En $y\to-\frac{1}{x}$, on a clairement $f(x,y)\to-\infty$ et donc f n'est pas prolongeable au voisinage de $(x,-\frac{1}{x})$.

— En $(0,0)$.
Au numérateur, $(x,y)\to(0,0)$ *un équivalent est* $x\times y$ *d'ordre* 2,
alors qu'au dénominateur, $\sqrt{x^2+y^2}$ *est d'ordre* 1 *(c'est la racine d'un ordre* 2*),*
donc f *est d'ordre* 1 *(i.e.* x *ou* y*) et tend donc vers* 0 *pour* $(x,y)\to(0,0)$.
On a $\ln(1+xy)=xy+o(\|(x,y)\|_\infty)$ pour (x,y) au voisinage de $(0,0)$.
Puis $\min(x,y)\leqslant\sqrt{x^2+y^2}\leqslant\max(x,y)$, alors que $x\times y=\max(x,y)\times\min(x,y)$.
donc $\min(x,y)\leqslant\dfrac{xy}{\max(x,y)}\leqslant f(x,y)\leqslant\dfrac{xy}{\min(x,y)}\leqslant\max(x,y)$ au voisinage de $(0,0)$.
et comme $\lim\limits_{(x,y)\to(0,0)}\min(x,y)=\lim\limits_{(x,y)\to(0,0)}\max(x,y)=0$,
alors f admet une limite en $(0,0)$ et $\lim\limits_{(x,y)\to(0,0)}f(x,y)=0$.

Finalement, nous pouvons élargir l'ensemble de définition à $\mathscr{D}'_f$ sur lequel f est continue,
où $\mathscr{D}'_f=\{(x,y)\mid\left(x\geqslant0\text{ et }y\in]-\frac{1}{x},+\infty[\right)\text{ ou }\left(x\leqslant0\text{ et }y\in]-\infty,-\frac{1}{x}[\right)\}$

3.4. Continuité sur un compact

Proposition - Image d'un compact par une fonction continue
Si f est continue de E sur F et K est un compact de E,
alors $f(K)$ est un compact de F.

Démonstration
Si (y_n) est une suite de $f(K)$, on considère $(x_n)\in K^{\mathbb{N}}$ telle que $\forall\ n\in\mathbb{N}$, $y_n=f(x_n)$.
alors $\exists\ \varphi\nearrow$ telle que $x_{\varphi(n)}\to x\in K$.
On a donc $y_{\varphi(n)}=f(x_{\varphi(n)})\to f(x)\in f(K)$ par continuité de f.
D'où $f(K)$ est compact. □

Comme $f(K)$ est fermé et borné :

Proposition - Optimalité
Si f est continue sur un compact de E,
Alors f est bornée et atteint ses bornes

Démonstration
En effet, $f(K)$ est compact donc borné.
Et $f(K)$ est fermé donc égal à son adhérence. □

3.5. Représentation graphique

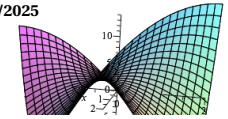
Il faut entendre ici surface au sens large : courbe, surface, volume, hypersphère…

Représentation des fonctions de plusieurs variables. « Dimension » p

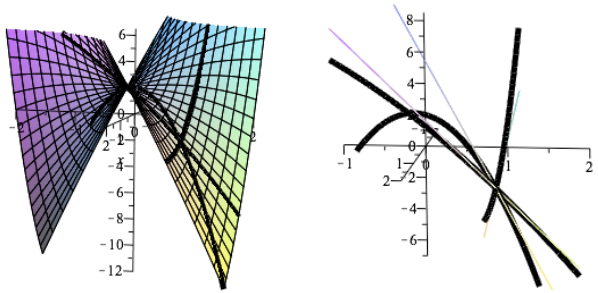
Analyse - Représentation de fonctions de deux variables
On s'intéresse dans ce petit point aux fonctions $f:\mathbb{R}^2\to\mathbb{R}$ car leur représentation se fait dans un espace $\mathbb{R}^2\times\mathbb{R}$, ce qui peut se visualiser avec un peu de géométrie projective.
Représentons donc la fonction simple polynomiale : $f:(x,y)\mapsto x^2-\frac{1}{2}y^2-4xy+2$
A quoi servent les traits et la couleur indiqués par Maple?
— Les traits montre le ligne $x=C^{ste}$ et $y=C^{ste}$ sur la figure.
— Les nuance de couleur indique les différentes altitudes de $z=f(x,y)$.
Une même couleur indique donc une « ligne de niveau ».
(il y a également un effet sous-sur la courbe)

Exemple - Sur la nappe S d'équation $z=x^2-\frac{1}{2}y^2-4xy+2$
Considérons le point $a=(1,1,f(1,1))=(1,1,-\frac{3}{2})\in S$ et trois vecteurs :

Représentation - Représentations graphiques de la nappe $z=x^2-\frac{1}{2}y^2-4xy+2$



— $u_1=(1,0)$.
Alors $\varphi_1(h)=\frac{1}{h}\big(f(1+h,1)-f(1,1)\big)=\frac{1}{h}\big(2h+h^2-4h\big)=-2+h$.
Donc f admet une dérivée en $(1,1)$ selon le vecteur $(1,0)$ égale à -2.
Qu'est-ce que cela signifie graphiquement?
si l'on suit la ligne $y=1$, on a la dérivée égale à -2.
— $u_2=(0,1)$.
Alors $\varphi_2(h)=\frac{1}{h}\big(f(1,1+h)-f(1,1)\big)=\frac{1}{h}\big(-h-\frac{1}{2}h^2-4h\big)=-5-\frac{1}{2}h$.
Donc f admet une dérivée en $(1,1)$ selon le vecteur $(0,1)$ égale à -5.
Qu'est-ce que cela signifie graphiquement?
si l'on suit la ligne $x=1$, on a la dérivée égale à -5.



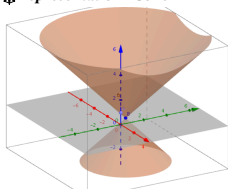
LIGNES DE REPRÉSENTATION DE $\varphi_{\vec{u}}$ ET DÉRIVÉES PARTIELLES

Ligne de niveau. « Dimension » $p-1$

Remarque - Courbe des équipotentiels
On peut s'intéresser au ligne de niveau : $\{(x_1,\dots x_p)\mid f(x_1,\dots x_p)=C^{ste}\}$. Il s'agit de l'ensemble décrit par les variables pour lesquels la fonction ne change de valeur.
Si la fonction est une grandeur physique, par exemple un potentiel, il s'agit des points d'équipotentialité. Quitte à étudier $g:(x_1,\dots x_p)\mapsto f(x_1,\dots x_p)-C^{ste}$, on peut même faire l'étude sur des équipotentiels nuls.

Définition - Ligne de niveau zéro
Soit f une application définie sur un ouvert U de $\mathbb{R}^p$ à valeur dans $\mathbb{R}$.
On appelle ligne de niveau zéro la courbe d'équation $f(x_1,\dots x_p)=0$.
Il s'agit en fait de l'ensemble $\{(x_1,x_2,\dots x_p)\in\mathbb{R}^p\mid f(x_1,\dots x_p)=0\}$.

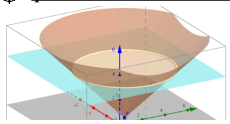
Représentation - Cône



Exemple - Cône
Considérons la fonction $g:\mathbb{R}^2\mapsto\mathbb{R}$, $(x,y,z)\mapsto(x+1)^2+(y-1)^2-z$.
Alors l'ensemble $\mathscr{C}=\{(x,y,z)\mid g(x,y,z)=0\}$ est le cône de sommet $(-1,1,0)$ et de courbe représentatif le cercle de centre $(-1,1,1)$ et de rayon 1.
C'est une courbe de dimension locale égale à 2 (surfacique, pour employer le vocabulaire de physique).

Exemple - Cercle
Considérons la fonction $f:\mathbb{R}^2\mapsto\mathbb{R}$, $(x,y)\mapsto(x+1)^2+(y-1)^2-4$.
Alors l'ensemble $\mathscr{C}=\{(x,y)\mid f(x,y)=0\}$ est le cercle de centre $(-1,1)$ et de rayon 2.
C'est une courbe de dimension locale égale à 1 (linéique, pour employer le vocabulaire de physique).
C'est aussi l'ensemble que l'on obtient lorsqu'on fait l'intersection entre le cône précédent et le plan $z=4$.

Représentation - Cercle



Bilan des représentation

Finalement, il y a à croiser différents objets selon les dimension : courbe, surface, volume par rapport au mode de (re)présentation : explicite ($y = f(x)$, $z = f(x,y)\ldots$), implicite (par une équation type ligne de niveau) et paramétrique ($(x(t),y(t))$, vu au chapitre précédent).
Ce qui donne

Proposition - « Surface »
On a les objets géométriques suivants, selon les types suivants :

	Courbe (dans $\mathbb{R}^2$)	Surface (dans $\mathbb{R}^3$)
Explicite	$M(x,y)\in\mathbb{R}^2$ tq $y=h(x)$ où $h:\mathbb{R}\to\mathbb{R}$ soit $\mathscr{C}^0$	$M(x,y,z)\in\mathbb{R}^3$ tq $z=g(x,y)$ où $g:\mathbb{R}^2\to\mathbb{R}$ soit $\mathscr{C}^0$
Implicite	$M(x,y)\in\mathbb{R}^2$ tq $g(x,y)=0$ où $g:\mathbb{R}^2\to\mathbb{R}$ soit $\mathscr{C}^0$	$M(x,y,z)\in\mathbb{R}^3$ tq $f(x,y,z)=0$ où $f:\mathbb{R}^3\to\mathbb{R}$ soit $\mathscr{C}^0$
Paramétrique	$M(x(t),y(t))\in\mathbb{R}^2$ où $x:\mathbb{R}\to\mathbb{R}$, $y:\mathbb{R}\to\mathbb{R}$	$M(x(u,v),y(u,v),z(u,v))\in\mathbb{R}^3$ où $x,y,z:\mathbb{R}^2\to\mathbb{R}$

Evidemment, il possible d'envisager une généralisation de ces définitions.

Remarque - Comment coder une courbe (un chemin ou un arc) dans $\mathbb{R}^3$?
Cela peut être une intersection de variétés (deux surfaces de $\mathbb{R}^3$), ou de manière plus pratique sous forme de arc paramétré : $t\mapsto(x(t),y(t),z(t))$.

Pour aller plus loin - Variété
Cet ensemble n'est en règle générale pas un espace vectoriel, mais localement il est comparable à un sous-espace vectoriel de dimension $p-1$.
(On parle de variété de dimension $p-1$).

4. Calcul différentiel

4.1. Développement limité. Différentiabilité

Heuristique - Comment définir alors une dérivée de f ?
Si notre motivation est de généraliser la démarche de dérivation d'une fonction à une variable : le signe de f' indique les variations de f, alors il faut se demander ce que signifie que la fonction est croissante?
Dans $\mathbb{R}^2$, cela n'a plus aucun sens.
Il ne faut donc pas s'attacher à cette approche des choses : dérivée = variations, mais plutôt à l'autre approche beaucoup plus essentielle : dérivée=DL$_1$.

Pour aller plus loin - Petit guide de calcul différentiel
Dans le petit et magnifique livre de F. Rouvière : petit guide de calcul différentiel, on voit décliner des milliers de fois une seule idée : « A ϵ près, une fonction quelconque se ramène à une fonction linéaire »
A lire absolument!

Définition - Différentielle
Soient $a\in U$ ouvert de E et $f:U\to F$.
On dit que f est différentiable en a si il existe une application linéaire $L_a:E\to F$ tel que

$$\forall\ h \text{ tel que } a+h\in U,\ f(a+h)=f(a)+L_a(h)+o(\|h\|)$$

Remarque - Sens du $o(\|h\|)$
On rappelle que $o(\|h\|)$ signifie une fonction η (ici $\eta:h\mapsto f(a+h)-f(a)-L_a(h)$) tel que $\dfrac{\|\eta(h)\|}{\|h\|}\underset{h\to0}{\longrightarrow}0$.
On peut aussi considérer la fonction ϵ telle que $\eta(h)=\|h\|\times\epsilon(h)$ avec $\epsilon(h)\to0_F$.

Proposition - Unicité de la différentielle
Si $f:U\subset E\to F$ est différentiable en a, alors la différentielle est unique. On note alors $\mathrm{d}f(a)(h)$, le vecteur $L_a(h)$.

Attention - Nature des objets
Que sont ∂f, $\partial f(a)$ et $\partial f(a)(h)$?
Dans l'ordre inverse : $\partial f(a)(h)$ un vecteur de l'espace (affine) F.
$\partial f(a)$ une application linéaire de E dans F.
∂f : une application de E dans $\mathscr{L}(E,F)$.

Application - Fonction f linéaire. Exemple de la trace
On a pour tout $A,H\in\mathscr{M}_n(\mathbb{R})$, $\mathrm{Tr}(A+H)=\mathrm{Tr}(A)+\mathrm{Tr}(H)$.
Donc $\partial tr(A)(H)=\mathrm{Tr}(H)$, qui est bien linéaire et est constante (par rapport à A).

Exemple - Fonction $f:\mathbb{R}\to\mathbb{R}$
Si f est dérivable en a et $a+h\in U$,
$f(a+h)=f(a)+h\times f'(a)+o(h)$.
Donc $\partial f(a)(h)=f'(a)\times h$, qui est bien linéaire (de la fonction $h:f'(a)(\lambda_1h_1+\lambda_2h_2)=\lambda_1f'(a)h_1+\lambda_2f'(a)h_2$).

Exemple - $f:\mathbb{R}^2\to\mathbb{R}$, $(x,y)\mapsto xy^2+3\ln x+\frac{x}{y}$.
Soient $(x,y)\in\mathbb{R}_+^*\times\mathbb{R}^*$, ouvert et (h,k) tel que $(x,y)+(h,k)\in\mathbb{R}_+^*\times\mathbb{R}^*$.

$$\begin{aligned}f\big((x,y+(h,k)\big) &= (x+h)(y+k)^2+3\ln(x+h)+\tfrac{x+h}{y+k}=xy^2+hy^2+2kxy+2hky+hk^2+3\ln x+3\ln(1+\\ &= f(x,y)+(y^2+\tfrac{3}{x}+\tfrac{1}{y})h+(2xy-\tfrac{x}{y^2})k+o(\|(h,k)\|)\end{aligned}$$

En utilisant les formules de $DL_1(0)$. Rappelons que $h^2=o(\|(h,k)\|)$, $k^2=o(\|(h,k)\|)$ et $hk=o(\|(h,k)\|)$.
Donc ici, $\partial f(x,y)(h,k)\mapsto(y^2+\frac{3}{x}+\frac{1}{y})h+(2xy-\frac{x}{y^2})k$ qui est bien linéaire.
Il reste à faire la démonstration de l'unicité.

Démonstration
Supposons que f admet deux différentielles en $a\in U$.
Alors pour tout $h\in E$ tel que $a+h\in U$, $f(a+h)-f(a)=L_a^1(h)+\underbrace{\epsilon_1(h)}_{o(\|h\|)}=L_a^2(h)+\underbrace{\epsilon_2(h)}_{o(\|h\|)}$ pour $h\to0$.

Fixons $h\in E$ tel $a+h\in U$.
Soit $t\in\mathbb{R}^*$ (corps), on a alors, par linéarité de $L^1(a)$ et $L^2(a)$:

$$\|L_a^1(h)-L_a^2(h)\|=\frac{1}{t}\|L_a^1(th)-L_a^2(th)\|\leqslant\frac{1}{t}\|\epsilon_1(th)\|+\|\epsilon_2(th)\|\underset{t\to0}{\to}0$$

Donc $\|L_a^1(h)-L_a^2(h)\|=0$, car indépendant de t. Donc $L_a^1(h)=L_a^2(h)$ □

4.2. Dérivées partielles

On se concentre uniquement ici sur des fonctions de $\mathbb{R}^p$ à valeurs dans $\mathbb{R}$ ($E=\mathbb{R}^p$, $F=\mathbb{R}$)

Remarque - Fonctions de $\mathbb{R}^p$ dans $\mathbb{R}^n$
Pour des fonctions $f:\mathbb{R}^p\to\mathbb{R}^n$, on peut décomposer $f=(f_1,f_2,\ldots f_n)$.
où pour tout $i\in\mathbb{N}_n$, $f_i:\mathbb{R}^p\to\mathbb{R}$. Selon ce que l'on a déjà vu en sciences physiques :

Définition - Dérivée partielle (d'ordre 1)
Soit $f:U\subset\mathbb{R}^p\to\mathbb{R}$. Soit $\vec{a}\in U$.
Notons $(e_1,e_2,\ldots e_p)$, la base canonique orthonormée de $\mathbb{R}^p$.
On appelle dérivées partielles de f la famille : $(\partial_1f(\vec{a}),\partial_2f(\vec{a}),\ldots,\partial_pf(\vec{a}))$:

$$\forall\ i\in\mathbb{N}_p,\qquad \partial_if(\vec{a})=\lim_{h\to0}\frac{f(\vec{a}+h\vec{e_i})-f(\vec{a})}{h}$$

Pour tout $i\in\mathbb{N}_p$, on peut noter également ce nombre $\dfrac{\partial f}{\partial x_i}(\vec{a})$

Exemple - $f:\mathbb{R}^3\to\mathbb{R},(x,y,z)\mapsto x^2+(y-z)x+y^z$
Soit $\vec{a}=(x_0,y_0,z_0)$. On a :

$$\frac{\partial f}{\partial x}(\vec{a})=\lim_{h\to 0}\frac{f(\vec{a}+h\vec{e}_i)-f(\vec{a})}{h}=\lim_{h\to 0}\frac{(x_0+h)^2+(y_0-z_0)(x_0+h)+y_0^{z_0}-x_0^2+(y_0-z_0)x_0+y_0^{z_0}}{h}$$

On retrouve exactement le calcul de la dérivée de la fonction $f_{y_0,z_0}:x\mapsto f(x,y_0,z_0)$ en $x=x_0$.
Ce résultat s'obtient donc comme si on considérait les variables y_0 et z_0, comme des constantes et que l'on dérivait par rapport à x.
On a donc

$$\frac{\partial f}{\partial x}(\vec{a})=2x_0+(y_0-z_0)$$

Truc & Astuce pour le calcul - Calculer les dérivées partielles
La dérivée partielle selon le vecteur de base $\vec{e}_i$ s'obtient en calculant la dérivée de $f_i:\mathbb{R}\to\mathbb{R}^n$, $t\mapsto f(\vec{a}+t\vec{e}_i)$.
Cela consiste donc souvent, lorsque les variables associés aux $(\vec{e}_j)$ sont clairement définissables, à dériver la fonction f en **tenant pour constante** toutes les variables x_j associés aux vecteurs $\vec{e}_j\neq\vec{e}_i$.

Exemple - Calcul des dérivées partielles de $f:(x,y)\mapsto\dfrac{xy^2}{x^2+y^2}$ **en** $(1,2)$**.**

$\frac{\partial f}{\partial x}(x,y)=\frac{y^2(x^2+y^2)-xy^2(2x)}{(x^2+y^2)^2}=\frac{y^2(y^2-x^2)}{(x^2+y^2)^2}$.
x est la variable, y est considérée ici comme une constante.
$\frac{\partial f}{\partial y}(x,y)=\frac{2yx(x^2+y^2)-xy^2(2y)}{(x^2+y^2)^2}=\frac{2x^3y}{(x^2+y^2)^2}$.
y est la variable, x est considérée ici comme une constante.
On a alors $\frac{\partial f}{\partial x}(1,2)=\frac{4(4-1)}{(1+4)^2}=\frac{12}{25}$ et $\frac{\partial f}{\partial y}(1,2)=\frac{2\times1^3\times2}{(1+4)^2}=\frac{4}{25}$.

Exercice
Calculer les dérivées partielles de la fonction f précédentes par rapport à la seconde et la troisième variable en $\vec{a}$.

Correction
$\frac{\partial f}{\partial y}(\vec{a})=x_0+z_0y_0^{z_0-1}$ et $\frac{\partial f}{\partial z}(\vec{a})=-x_0+\ln y_0\times y_0^{z_0}$

Remarque - Si $f:U\subset\mathbb{R}^p\to\mathbb{R}$ **est différentiable**
Si $(e_1,\dots e_p)$ est la base canonique de $\mathbb{R}^p$,
Alors $\partial f(a)(he_i)=\dfrac{\partial f}{\partial x_i}(a)\times h_i$.
Donc si f est différentiable, alors f admet des dérivées partielles.
Il semble donc qu'il y ait bien une implication et une relation entre les deux notions.

Attention - Nature des objets
Supposons que $f:\mathbb{R}^p\to\mathbb{R}$.
Alors $\dfrac{\partial f}{\partial x_k}(a)$ est un nombre (a est un vecteur) et donc $\dfrac{\partial f}{\partial x_k}$ est une application de $\mathbb{R}^p\to\mathbb{R}$.

4.3. Application de classe $\mathscr{C}^1$

Définition

Nous cherchons un critère réciproque : l'existence des dérivées partielles implique-t-elle la différentiabilité?
Un critère suffisant à ce que « tout se passe bien » est le fait que l'application soit de classe $\mathscr{C}^1$ sur U. Un exemple illustrera ce qui peut (mal) se passer lorsque la fonction n'est pas de classe $\mathscr{C}^1$.

Définition - Fonction de classe $\mathscr{C}^1$
Soit $f:U\subset\mathbb{R}^p\to\mathbb{R}$.
On dit que f est de classe $\mathscr{C}^1$ ou continûment différentiable sur U (ouvert), si toutes les fonctions dérivées partielles $\dfrac{\partial f}{\partial x_i}$ existent et sont continues de U dans $\mathbb{R}$.

Nous admettons déjà le résultat suivant (les explications suivront, ainsi que le critère de composition)

Proposition - Exemples de fonctions de classe $\mathscr{C}^1$
— Les fonctions polynomiales (à p variables) sont de classe $\mathscr{C}^1$ sur $\mathbb{R}^p$.
— Toute combinaison linéaire de fonctions de classe $\mathscr{C}^1$ sur U est de classe $\mathscr{C}^1$ sur U *donc* $\mathscr{C}^1(U)$, *l'ensemble des fonctions de classe* $\mathscr{C}^1$ *sur* U *est un espace vectoriel*

Cas pathologiques

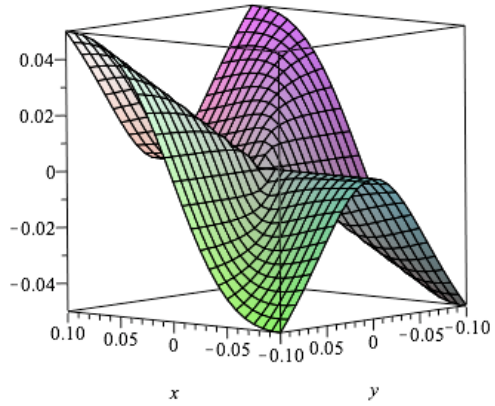
La dérivabilité n'implique pas la continuité!

Attention - Fonction différentiable mais non continûment
La condition de continuité des dérivées de f est nécessaire comme le montre le contre-exemple suivant :
Soit $f:(x,y)\mapsto\dfrac{xy^2}{x^2+y^2}$ prolongé en $f(0,0)=0$.
Ici, les dérivées partielles en $\vec{0}=(0,0)$ donnent :
$\frac{\partial f}{\partial x}(x,y)=\frac{y^2(y^2-x^2)}{(x^2+y^2)^2}$ et $\frac{\partial f}{\partial x}(0,0)=\lim_{h\to0}\frac{f(h,0)-f(0,0)}{h}=0$
de même $\frac{\partial f}{\partial y}=\frac{2xy^3}{(x^2+y^2)^2}$ et $\frac{\partial f}{\partial y}(0,0)=0$
Et plus généralement, pour tout $\vec{u}=(a,b)$,

$$\varphi_{\vec{u}}(h)=\frac{1}{h}\left(f(\vec{0}+h\vec{u})-f(\vec{0})\right)=\frac{h^3ab^2}{h(h^2(a^2+b^2)}=\frac{ab^2}{a^2+b^2}\neq0$$

Donc on a $D_{\vec{u}}(f)(0,0)\neq a\frac{\partial f}{\partial x_1}(0,0)+b\frac{\partial f}{\partial x_1}(0,0)$.
Ici les dérivées partielles ne sont pas continues en $(0,0)$.
La représentation graphique montre que la fonction f n'est pas « totalement lisse » mais semble comme froissée.

Remarque - Représentation d'une fonction dérivable mais pas continûment



Développement limité (retour)

Théorème - Développement limité
Soit f est de classe $\mathscr{C}^1$ sur un ouvert U de $\mathbb{R}^p$.
Alors :

1. f est continue sur U.
2. f admet en tout point $\vec{a}$ de U de $\mathbb{R}^p$ un développement limité :

$$f(\vec{a}+\vec{u}) = f(\vec{a}) + \sum_{i=1}^{p} u_i \times \frac{\partial f}{\partial x_i}(\vec{a}) + \|u\| \times \epsilon(u)$$

où le vecteur $\vec{u} = (u_1, u_2, \dots u_p)$ et $\epsilon : U \to \mathbb{R}$, tel que $\epsilon(u) \underset{u\to 0}{\longrightarrow} 0$.

Démonstration
On fait la démonstration dans le cas $p = 2$. Dans la marge figurent les idées de généralisation.
Supposons $\vec{a} = (x_0, y_0)$ et $\vec{u} = (h_1, h_2)$

$f(\vec{a}+\vec{u}) - f(\vec{a}) = f(x_0+h_1, y_0+h_2) - f(x_0, y_0) = f((x_0+h_1, y_0+h_2) - f(x_0+h_1, y_0) + f(x_0+h_1, y_0) - f(x_0, y_0)$

Or f est dérivable par rapport à la seconde variable en $(x_0 + h_1, y_0)$ (on applique la formule du DL pour une fonction de $\mathbb{R}$ dans $\mathbb{R}$) :

$$f(x_0+h_1, y_0+h_2) = f(x_0+h_1, y_0) + h_2 \frac{\partial f}{\partial x_2}(x_0+h_1, y_0) + |h_2|\epsilon_2(h_2)$$

Or f est dérivable par rapport à la première variable en (x_0, y_0) :

$$f(x_0+h_1, y_0) = f(x_0, y_0) + h_1 \frac{\partial f}{\partial x_1}(x_0, y_0) + |h_1|\epsilon_1(h_1)$$

Donc

$$f(\vec{a}+\vec{u}) = f(\vec{a}) + h_1 \frac{\partial f}{\partial x_1}(x_0, y_0) + h_2 \frac{\partial f}{\partial x_2}(x_0+h_1, y_0) + |h_2|\epsilon_2(h_2)|h_1|\epsilon_1(h_1)$$

Enfin, il faut exploiter la continuité de $\frac{\partial f}{\partial x_2}$ en (x_0, y_0) :

$$h_2 \frac{\partial f}{\partial x_2}(x_0+h_1, y_0) = h_2\left(\frac{\partial f}{\partial x_2}(x_0, y_0) + \epsilon_3(h_1)\right)$$

$$f(\vec{a}+\vec{u}) = f(\vec{a}) + h_1 \frac{\partial f}{\partial x_1}(x_0, y_0) + h_2 \frac{\partial f}{\partial x_2}(x_0, y_0) + \underbrace{(|h_2|\epsilon_2(h_2) + |h_1|\epsilon_1(h_1) + |h_2|\epsilon_3(h_1))}_{\|u\|\epsilon(u)}$$

□

Pour aller plus loin - Démonstration
Considérons $\vec{u}$, un vecteur quelconque de norme petite.
On utilise un télescopage :

$$\vec{a}+\vec{u} = (\vec{a}+u_1\vec{e_1}) + [(\vec{a}+u_1\vec{e_1}+u_2\vec{e_2}) - (\vec{a}+u_1\vec{e_1}] + \dots [(\vec{a}+\vec{u}) - (\vec{a}+u_1\vec{e_1}+\dots+u_{n-1}\vec{e_{n-1}})]$$

Formellement :

$$\vec{a}+\vec{u} = (\vec{a}+u_1\vec{e_1}) + \sum_{j=2}^{p}\left(\left(\vec{a}+\sum_{h=1}^{j}\vec{u}\right) - \left(\vec{a}+\sum_{h=1}^{j-1}\vec{u}\right)\right)$$

Et donc en f, on appliquant des développements limités d'ordre 1 :

$$f(\vec{a}+\vec{u}) - f(\vec{a}) = f(\vec{a}+u_1\vec{e_1}) - f(\vec{a}) + \sum_{j=2}^{p}\left(f\left(\vec{a}+\sum_{h=1}^{j}\vec{u}\right) - f\left(\vec{a}+\sum_{h=1}^{j-1}\vec{u}\right)\right)$$
$$= u_1\frac{\partial f}{\partial x_1}(\vec{a}) + u_2\frac{\partial f}{\partial x_2}(\vec{a}+u_1\vec{e_1}) + \dots + u_j\frac{\partial f}{\partial x_j}(\vec{a}+\sum_{h=1}^{j-1}u_h\vec{e_h}) + \dots \frac{\partial f}{\partial x_p}(\vec{a}+\vec{u}-u_n\vec{e_n})$$

Puis par continuité des dérivées partielles et en faisant tendre $\|u\|_\infty$ vers 0, on retrouve le résultat annoncé

Remarque - Notation physique
Nous rencontrons parfois en physique l'équation (sans travail extérieur) :
$\mathrm{d}U = T\mathrm{d}S - p\mathrm{d}V$.
Que signifie-t-elle?

1. Que l'énergie libre ne dépend que de deux variables : l'entropie S et le volume occupé V.
   (*localement, l'énergie peut dépendre d'autres couples de variable thermodynamique, mais nous ne sommes pas assurés que ces autres couples ne puissent pas donner plusieurs valeurs de U... (surtout si ce sont des variables intensives)*).
   Donc $U = U(S, V)$
2. On a les dérivées exactes (et définition) : $\frac{\partial U}{\partial S}(S,V) = T_{(S,V)}$ et $\frac{\partial U}{\partial V}(S,V) = -p_{(S,V)}$
3. Puis la formule d'approximation de premier ordre :

$$\Delta U = U(S_0+\delta S, V_0+\delta V) - U(S_0, V_0) \approx \frac{\partial U}{\partial S}(S,V)\delta S + \frac{\partial U}{\partial V}(S,V)\delta V = T_{(S_0,V_0)}\delta S - p_{(S_0,V_0)}\delta V$$

Gradient

Remarque - Pourquoi $\mathrm{d}f(\vec{a}) : u \mapsto \dots$ est-ce bien une application linéaire?
En fait on a par définition : $\mathrm{d}f(\vec{a}) : \vec{u} = (u_1, \dots u_p) \longmapsto \sum_{j=1}^{p} u_j \frac{\partial f}{\partial x_j}(\vec{a})$.
Il s'agit du produit scalaire canonique de $\vec{u}$ par le vecteur $\left(\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \dots \frac{\partial f}{\partial x_n}\right)$ dans la base canonique de $\mathbb{R}^p$.
C'est pourquoi on note plutôt $\mathrm{d}f(\vec{a})\cdot\vec{u}$ que $\mathrm{d}f(\vec{a})(\vec{u})$.
Cela explique aussi la linéarité de la différentielle. Mais nous avons plus largement intérêt à étudier ce dernier vecteur.
C'est ce qu'on appelle le gradient de f en $\vec{a}$.
D'après le théorème de représentation de Riesz en dimension finie :

Définition - Gradient
Soit $f : U \subset \mathbb{R}^p \to \mathbb{R}$ de classe $\mathscr{C}^1$ sur U.
On appelle gradient de f, l'application vectorielle :

$$\nabla f : \mathbb{R}^p \to \mathbb{R}^p,\ \vec{a} \mapsto \begin{pmatrix} \frac{\partial f}{\partial x_1}(\vec{a}) \\ \frac{\partial f}{\partial x_2}(\vec{a}) \\ \vdots \\ \frac{\partial f}{\partial x_p}(\vec{a}) \end{pmatrix}$$

On a alors, pour tout $\vec{u} \in \mathbb{R}^p$, $\mathrm{d}f(\vec{a})\cdot\vec{u} = \langle \nabla f(\vec{a}); \vec{u}\rangle$.
Et aussi (approximation au 1er ordre) : $f(\vec{a}+h\vec{u}) = f(\vec{a}) + h\langle \nabla f(\vec{a}); \vec{u}\rangle + o(h)$

4.4. Règle de la chaine

Dérivation d'une composition

Il s'agit ici d'étudier l'impact de la composition dans le calcul différentiel.
Voici le cas classique d'un arc à valeur sur une (hyper)-surface ($\mathbb{R}$ sur $\mathbb{R}^p$ puis $\mathbb{R}^p$ sur $\mathbb{R}$).
Analyse - Composition : $\mathbb{R} \to \mathbb{R}^p \to \mathbb{R}$
Supposons le schéma suivant :

$$\begin{array}{ccccc} \mathbb{R} & \xrightarrow{\varphi} & \mathbb{R}^p & \xrightarrow{f} & \mathbb{R} \\ t & \longmapsto & (x_1(t), x_2(t), \dots x_p(t)) & \longmapsto & f(x_1(t), x_2(t) \dots x_p(t)) \end{array}$$

Finalement, $g = f\circ\varphi : \mathbb{R}\to\mathbb{R}$, classique.
La question qui se pose est : que vaut $g'(t_0)$?
Pour répondre à cette question, on exploite les développements limités pour lesquels les compositions deviennent des produits.

$$g(t_0+h) = f(\varphi(t_0+h)) = f\big(\varphi(t_0)+h\cdot\varphi'(t_0)+o(h)\big) = f(\varphi(t_0))+h\mathrm{d}(f)(\varphi(t_0))\cdot\varphi'(t_0)+o(h)$$

Notons que $\varphi(t_0)$ ainsi que $\varphi'(t_0)$ sont des vecteurs.
On a donc $g'(t_0) = \mathrm{d}(f)(\varphi(t_0))\cdot\varphi'(t_0)$.
Or ici :

- le vecteur $\mathrm{d}(f)(\varphi(t_0))$ a pour coordonnées : $\left(\dfrac{\partial f}{\partial x_1}(\varphi(\vec{t}_0)), \dfrac{\partial f}{\partial x_2}(\varphi(\vec{t}_0)),\dots \dfrac{\partial f}{\partial x_p}(\varphi(\vec{t}_0))\right)$
- le vecteur $\varphi'(t_0)$ a pour coordonnées $\left(x_1'(t_0), x_2'(t_0),\dots x_p'(t_0)\right)$

Proposition - Règle de la chaîne
Soit $f : U\subset\mathbb{R}^p\to\mathbb{R}$, de classe $\mathscr{C}^1$ sur l'ouvert U. Soit $\varphi : \mathbb{R}\mapsto\mathbb{R}^p$ de classe $\mathscr{C}^1$ sur I ouvert de $\mathbb{R}$, avec $\varphi(I)\subset U$.
Alors $g : f\circ\varphi$ est une fonction numérique de classe $\mathscr{C}^1$ sur I et

$$\forall\ t\in I \qquad g'(t) = \sum_{j=1}^{p} x_j'(t)\times\frac{\partial f}{\partial x_j}(\varphi(\vec{t}))$$

L'application physique suivante explique le nom donné à cette règle :

Exemple - Fondamental!
Considérons la fonction $\Phi : \mathbb{R}\to\mathbb{R}$, $u\mapsto F\big(x(u), y(u)\big)$, où $F : \mathbb{R}^2\to\mathbb{R}$.
Alors $\Phi(u) = (F\circ G)(u)$ avec $G : \mathbb{R}\to\mathbb{R}^2$, $u\mapsto(x(u), y(u))$ (on appelle cette fonction un arc paramétré).
Et donc $\dfrac{\mathrm{d}\Phi}{\mathrm{d}u}(u) = \dfrac{\partial F}{\partial x}(x(u), y(u))\times\dfrac{\mathrm{d}x}{\mathrm{d}u}(u) + \dfrac{\partial F}{\partial y}(x(u,y(u))\times\dfrac{\mathrm{d}y}{\mathrm{d}u}(u)$.

Truc & Astuce pour le calcul - Comment dériver des fonctions composées?
Si vous devez dériver la suite de composition $f\circ\varphi$:

$$t\xrightarrow{\varphi}(x_1, x_2,\dots x_n)\xrightarrow{f} f\circ\varphi(t)$$

- t a une influence sur tout $x_k = \varphi_k(t)$ égale à $\varphi_k'(t) = \dfrac{\mathrm{d}x_k}{\mathrm{d}t}$
- Puis, tout x_k a une influence sur tout f égale à $\dfrac{\partial f}{\partial x_k}$

Puis on regarde tous les chemins possibles!! (sommation)

$$\frac{\mathrm{d}(f\circ\varphi)}{\mathrm{d}t} = \sum_{j=1}^{p}\frac{\partial f}{\partial x_j}(\varphi(t))\times\frac{\mathrm{d}x_j}{\mathrm{d}t}(t)$$

C'est la formule générale, mais penser à l'appliquer directement.

Attention - Autour de la formule de la chaîne
Même si en physique on a tendance à oublier le point (vecteur) pour lequel on effectue le calcul de la différentielle, il ne faut pas l'oublier ici!! Noter également qu'il est préférable (au moins mnémnotechniquement) d'écrire d'abord les dérivée de f (à gauche), puis celles des x_k à droite. Cela correspond bien à l'écriture de la dérivation. C'est aussi avec cette écriture qu'on peut faire des vraies/fausses simplifications rapides par $\partial x_j\dots$

Pour aller plus loin - Règle de la chaîne - multiple
Et si g est à plusieurs valeurs? Si φ s'exprime elle-même sous la forme : $\varphi : (t_1,\dots t_m)\mapsto\big(x_1(t_1,\dots t_m),\dots x_p(t_1,\dots t_m)\big)$.
On applique exactement la même règle pour chacune des dérivations par rapport à t_h.
Soit $f : U\subset\mathbb{R}^p\to\mathbb{R}^n$, de classe $\mathscr{C}^1$ sur l'ouvert U. Soit $\varphi : \mathbb{R}^m\mapsto\mathbb{R}^p$ de classe $\mathscr{C}^1$ sur O ouvert de $\mathbb{R}^m$, avec $\varphi(O)\subset U$.
Alors $g : f\circ\varphi$ est une fonction numérique de classe $\mathscr{C}^1$ sur O et

$$\forall\ \vec{t} = (t_1,\dots t_m)\in O, \forall\ k\in\mathbb{N}_m,$$

$$\frac{\partial g}{\partial t_k}(\vec{t}) = \sum_{j=1}^{p}\frac{\partial f_k}{\partial x_j}(\varphi(\vec{t}))\times\frac{\partial x_j}{\partial t_k}(\vec{t})$$

Exercice
Exprimer la dérivée de $f : (x, y)\mapsto f(x, y)$ en fonction de r et de θ si l'on admet le paramétrage : $x = r\cos\theta$ et $y = r\sin\theta$

Correction
$\dfrac{\partial f}{\partial r} = \dfrac{\partial f}{\partial x}\dfrac{\partial x}{\partial r} + \dfrac{\partial f}{\partial y}\dfrac{\partial y}{\partial r} = \cos\theta\dfrac{\partial f}{\partial x} + \sin\theta\dfrac{\partial f}{\partial y}$ et $\dfrac{\partial f}{\partial\theta} = \dfrac{\partial f}{\partial x}\dfrac{\partial x}{\partial\theta} + \dfrac{\partial f}{\partial y}\dfrac{\partial y}{\partial\theta} = -r\sin\theta\dfrac{\partial f}{\partial x} + r\cos\theta\dfrac{\partial f}{\partial y}$

Règle de la chaîne et sciences physiques

Nous nous appuyons sur le document *Rapprochements didactiques entre trois disciplines scientifiques dans la continuité [bac-3,bac+3].*

Remarque - Relation numérique. Différence entre la fonction mathématique et la loi physique.
En mathématiques, la fonction est une application d'un ensemble dans un autre. En informatique, la notion de fonction est équivalente.
En science physique, on s'intéresse aux grandeurs physiques et non aux fonctions. Celle-là sont reliées entre elles par des lois modélisant des phénomènes. Par exemple, la notation $G(g_1, g_2,\dots g_N)$ traduit le fait que la grandeur G dépend des autres grandeurs physiques $g_1,\dots g_N$.
Mais, mathématiquement, ce choix s'interprète par l'existence d'une fonction G de plusieurs variables $G : (g_1, g_2,\dots g_N)\mapsto G(g_1, g_2,\dots g_N)$.
Une difficulté majeure (voire LA difficulté majeure) réside dans le fait que le physicien note avec la même lettre G toutes les fonctions quoique différentes, servant à exprimer la même grandeur G en fonction de jeux de variables différentes.

Exemple - Thermodynamique
En thermodynamique, on utilise à la fois l'expression $S(T, V)$ de l'entropie en fonction de la température T et le volume V et son expression $S(T, P)$ en fonction de la température T et de la pression P.
Ici le physicien donne le même nom S (celui de la grandeur physique) aux deux fonctions mathématiques : $(T, V)\mapsto f(T, V)$ et $(T, P)\mapsto g(T, P)$ qui sont en fait différentes.

Remarque - Notation de dérivation
La même notation, de Leibniz, sert pour exprimer en mathématiques la dérivation de fonction de plusieurs variables et en physique la dérivation d'une grandeur. Dans les deux cas, une confusion (maladresse) peut poindre…

- En mathématiques, écrire $\dfrac{\partial f}{\partial x}(x, y)$ est assez maladroit car x apparait ici deux fois mais dans deux sens distinctes : une fois comme variable muette pour indiquer par rapport à quelle variable on calcule la dérivée, l'autre fois comme valeur de la variable.
  On a préféré ainsi dans le cours la notation $\dfrac{\partial f}{\partial x}(x_0, y_0)$, intéressante lorsqu'on se place en un point précis, mais ce n'est pas toujours le cas… On pourrait aussi noter, sans ambiguité en mathématiques : $\partial_1 f(x, y)$
- En physique, lorsque les grandeurs de référence sont toujours les mêmes cela ne pose pas trop de problème. C'est le cas en électromagnétisme : les variables sont x, y, z, t. Quoiqu'un premier doute peut apparaître lorsqu'on écrit $\dfrac{\partial E}{\partial r}$. Que le contexte associe à r les coordonnées cylindrique ou sphérique change le résultat.
  C'est encore plus dramatique en thermodynamique. Reprenons l'exemple précédent, que signifie $\dfrac{\partial S}{\partial T}$. Est-ce la dérivée de la variable $S(T, V)$ ou $S(T, P)$?
  Pour répondre à cette question, en physique on note $\left(\dfrac{\partial S}{\partial T}\right)_V$ et $\left(\dfrac{\partial S}{\partial T}\right)_P$, ce qu'on aurait noté mathématiquement $\dfrac{\partial f}{\partial T}$ et $\dfrac{\partial g}{\partial T}$ respectivement (avec les conventions de l'exemple précédent)

Exemple - Formule de la chaîne physicienne
Nous avons vu que mathématiquement, avec $\Phi : \mathbb{R}\to\mathbb{R}$, $u\mapsto F\big(x(u), y(u)\big)$, où $F : \mathbb{R}^2\to\mathbb{R}$.
Alors $\Phi(u) = (F\circ G)(u)$ avec $G : \mathbb{R}\to\mathbb{R}^2$, $u\mapsto(x(u), y(u))$ (on appelle cette fonction un arc paramétré).

Et donc $\frac{\mathrm{d}\Phi}{\mathrm{d}u}(u) = \frac{\partial F}{\partial x}(x(u),y(u)) \times \frac{\mathrm{d}x}{\mathrm{d}u}(u) + \frac{\partial F}{\partial y}(x(u),y(u)) \times \frac{\mathrm{d}y}{\mathrm{d}u}(u)$.
Comment s'écrit cette formule physiquement.
On note en fait de la même façon Φ et F, car elles expriment une même grandeur, par exemple l'énergie interne U.
Supposons qu'on ait ainsi $U = U(S,V)$, donc $U(T) = U(S(T),V(T))$ (convention en physique) alors

$$\frac{\partial U}{\partial T} = \frac{\partial U}{\partial S}\frac{\partial S}{\partial T} + \frac{\partial U}{\partial V}\frac{\partial V}{\partial T}\cdots$$

5. Visualisation et optimisation

5.1. Tangente à une courbe, à une surface

Commençons par la tangente à une surface : il s'agit d'un plan.
Pour la courbe, nous ferons une analogie et retrouverons les résultats déjà connus…

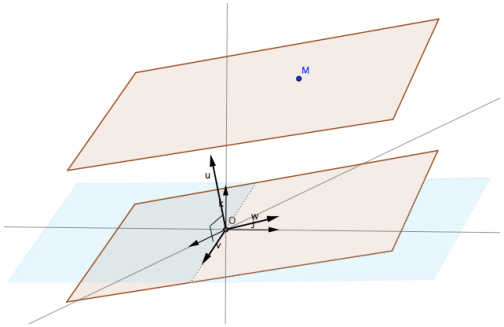
Plan de l'espace

Pour les courbe de $\mathbb{R}$ dans $\mathbb{R}$, localement une courbe ressemble à un segment de droite. Comme pour ces cas simples, localement, une surface ressemble (de près donc) à une surface plane.
Voyons comme décrire une surface plane.

Heuristique - Décrire un plan de $\mathbb{R}^3$

Comment peut-on décrire un plan dans $\mathbb{R}^3$ (espace affine) ?

1. et en donnant un point du plan .
2. en décrivant sa pente, c'est-à-dire le plan parallèle qui passe par O, ou encore le plan de l'espace vectoriel parallèle.
   - celui-ci est donné soit par une équation explicite : $ax+by+cz=0$.
     Ou de manière équivalente, mais plus géométrique, par un vecteur orthogonal au plan en question (ici $\vec{u}=(a,b,c)$).
     Cela correspond à *l'écriture implicite du plan.*
   - ou enfin, par la donnée de deux vecteurs formant une famille génératrice du plan (ici $\vec{v},\vec{w}$).
     Cela correspond à *l'écriture paramétrique du plan.*



Proposition - Surface plane
L'écriture **explicte** d'un plan de $\mathbb{R}^3$ est de la forme : $z = ax+by+c$
(ou dans certain cas particuliers $x = x_0$ (plan perpendiculaire à (Ox)),

Pour aller plus loin - Nature de $\frac{\partial f}{\partial x_i}$

Si $f:\mathbb{R}^p \to \mathbb{R}^n$, alors $\frac{\partial f}{\partial x_i}$ est également une fonction de $\mathbb{R}^p$ dans $\mathbb{R}^n$, puisque $\frac{\partial f}{\partial x_i} : \vec{a} \mapsto \left(\frac{\partial f_1}{\partial x_i}(\vec{a}), \frac{\partial f_2}{\partial x_i}(\vec{a}), \dots \frac{\partial f_n}{\partial x_i}(\vec{a})\right)$.
On peut donc tenter de dériver également ces fonctions-là.
Soit $f: U \subset \mathbb{R}^p \to \mathbb{R}$ de classe $\mathscr{C}^1$ sur U.
Si pour tout $i \in \mathbb{N}_p$, $\frac{\partial f}{\partial x_i}$ est dérivable, on dit que f admet des dérivées partielles d'ordre 2 notées $\frac{\partial^2 f}{\partial x_j \partial x_i}$ (pour la dérivée $\frac{\partial}{\partial x_j}\frac{\partial f}{\partial x_i}$)

ou bien $y = y_0$ (plan perpendiculaire à (Oy)),
ou bien $y = ax+c$ (plan perpendiculaire à la droite $y = ax+c$ de (Oxy)))
L'écriture **implicite** d'un plan de $\mathbb{R}^3$ est de la forme : $ax+by+cz+d=0$
plan orthogonal à $\vec{u}=(a,b,c)$ passant par $(0,0,-\frac{d}{c})$
L'écriture **paramétrique** d'un plan de $\mathbb{R}^3$ est de la forme :

$$\begin{cases} x(u,v) &= a_1u+b_1v+c_1 \\ y(u,v) &= a_2u+b_2v+c_2 \\ z(u,v) &= a_3u+b_3v+c_3 \end{cases}$$

plan dirigé par $\vec{e}=(a_1,a_2,a_3)$ et $\vec{f}=(b_1,b_2,b_3)$ et passant par (c_1,c_2,c_3).

Démonstration
Soit $\vec{u}=(a,b,c)$,
Supposons $c\neq 0$. Notons $D=(0,0,-\frac{d}{c})$. Soit $M=(x,y,z)$.
$\overrightarrow{DM}=(x,y,z+\frac{d}{c})$ est orthogonal à $\vec{u}$ ssi $\overrightarrow{DM}\cdot\vec{u}=0$
$\overrightarrow{DM}$ est orthogonal à $\vec{u}$ ssi $ax+by+cz+d=0$
Considérons $\vec{e}=(a_1,a_2,a_3)$ et $\vec{f}=(b_1,b_2,b_3)$,
le plan (passant par O) engendré par $\vec{e}$ et $\vec{f}$ est donné par $u\vec{e}+v\vec{f}$.
$M(x,y,z)$ un point du plan parallèle à celui-ci passant $D=(c_1,c_2,c_3)$ vérifie $\overrightarrow{DM} \in \mathrm{vect}(\vec{e},\vec{f})$,
ce qui donne exactement le système paramétrique précédent.
(Il faudrait faire des réciproques ici…) □

Remarque - Point de vue et nature de la définition
On voit que selon le point de vue adopté pour définir un plan, la définition de ce plan change de nature :
- si l'on considère le plan comme un ensemble engendré par deux vecteurs (et un point) alors on aboutit à une définition paramétrique,
- si l'on considère le plan comme u ensemble orthogonal à un vecteur (et passant par un point) alors on aboutit à une définition implicite.

Plan tangent à une surface

Heuristique - Regarder au voisinage d'un point

Pour pouvoir regarder une surface au voisinage de point $M_0(x_0,y_0,z_0)$, il faut que l'on puisse maîtriser l'ensemble des $M(x,y,z)$, voisin de M_0 et qui se trouve sur la surface Σ.
Il faut donc que le vecteur $\lim_{M(\in\Sigma)\to M_0} \frac{\overrightarrow{M_0M}}{\|M_0M\|}$ ait un sens.
Or $f(x,y,z)-f(x_0,y_0,z_0)=0$ (cas implicite)
donc $\frac{\partial f}{\partial x}(x,y,z)\times(x-x_0)+\frac{\partial f}{\partial y}(x,y,z)\times(y-y_0)+\frac{\partial f}{\partial z}(x,y,z)\times(z-z_0)=0$
donc $\langle \nabla f(x,y,z)\cdot\overrightarrow{M_0M}\rangle = 0$.
Il est donc nécessaire, dans le cas des surfaces implicites, que $\nabla f(x,y,z)$ soit non nul pour pouvoir définir, alors, un plan tangent.
Le cas paramètre est hors programme La surface va ressembler à un plan, localement, si le point au voisinage duquel nous faisons l'étude est régulier :

Définition - Point régulier
Un point $M(x,y,z)$ d'une surface Σ est dit **régulier** si :
- dans le cas d'une surface définie explicitement $z=g(x,y)$:
  $\frac{\partial g}{\partial x}(x,y)$ et $\frac{\partial g}{\partial y}(x,y)$ sont finis,
- dans le cas d'une surface définie implicitement $f(x,y,z)=0$:
  $\nabla f(x,y,z)\neq 0$.
- dans le cas d'une surface définie paramétriquement $\big(x(u,v),y(u,v),z(u,v)\big)$:
  $\left(\frac{\partial\varphi}{\partial u}(u,v),\frac{\partial\varphi}{\partial v}(u,v)\right)$ forment une famille libre,

Un point non régulier est dit critique, nous le verrons plus tard.
Et selon ces cas :

Proposition - Plan tangent
Considérons une surface Σ et $M(x_0,y_0,z_0)$ un point régulier de cette surface.
Alors : Σ admet en M un plan tangent (affine) :
- dans la cas où Σ a pour équation explicite $z=g(x,y)$, ce plan tangent a pour équation :
$$z-z_0=\frac{\partial g}{\partial x}(x_0,y_0)\times(x-x_0)+\frac{\partial g}{\partial y}(x_0,y_0)\times(y-y_0)$$
ou $z-z_0=\langle\nabla g(x_0,y_0)\cdot(x-x_0,y-y_0)\rangle$.
- dans la cas où Σ a pour équation implicite $f(x,y,z)=0$, ce plan tangent a pour équation :
$$\langle\nabla f(x_0,y_0,z_0)\cdot\overrightarrow{M_0M}\rangle=0$$
ou $\frac{\partial f}{\partial x}(x_0,y_0,z_0)\times(x-x_0)+\frac{\partial f}{\partial y}(x_0,y_0,z_0)\times(y-y_0)+\frac{\partial f}{\partial z}(x_0,y_0,z_0)\times(z-z_0)=0$
- dans le cas où Σ est définie paramétriquement par $\big(x(u,v),y(u,v),z(u,v)\big)$, le plan tangent à cette surface en $M_0(x(u_0,v_0),y(u_0,v_0),z(u_0,v_0))$ a pour équation :
$$M_0+\text{vect}\left(\frac{\partial\varphi}{\partial u}(u_0,v_0),\frac{\partial\varphi}{\partial v}(u_0,v_0)\right).$$

Exercice
Montrer que $M(1,1,1)$ est un point régulier de la surface Σ d'équation $x^2+y^2-z^2=1$.
Donner une équation du plan tangent à Σ en M

Correction
Notons $f:(x,y,z)\mapsto x^2+y^2-z^2-1$, alors $M(x,y,z)\in\Sigma$ ssi $f(x,y,z)=0$.
Or $f(1,1,1)=1+1-1-1=0$, donc $M\in\Sigma$.
L'équation de la surface Σ est implicite, on regarde $\overrightarrow{\text{grad}}f(1,1,1)$, or $\overrightarrow{\text{grad}}f(x,y,z)=(2x,2y,-2z)$.
Donc $\overrightarrow{\text{grad}}f(1,1,1)=(2,2,-2)$ et donc M est un point régulier de Σ.
Le plan tangent à Σ en M a pour équation : $2(x-1)+2(y-1)-2(z-1)=0$ i.e. $2x+2y-2z-2=0$

Droite tangente à une courbe

Remarque - Droite tangente à une courbe
Par analogie, on adapte ces définitions (points réguliers) et propriétés (droites tangentes à une courbe) au cas d'une courbe du plan.
L'exercice suivant nous donne une application.
Exercice
On considère l'ellipse $\mathscr{E}$ d'équation $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$.
Soit $M(x_0,y_0)$ un point de $\mathscr{E}$, donner l'équation de la droite tangente en M.

Correction
Notons $g:(x,y)\mapsto\frac{x^2}{a^2}+\frac{y^2}{b^2}-1$, alors $M(x_0,y_0)\in\mathscr{C}$ ssi $g(x_0,y_0)=0$.
Puis $\nabla g(x_0,y_0)=\left(\frac{\partial g}{\partial x}(x_0,y_0),\frac{\partial g}{\partial y}(x_0,y_0)\right)=\left(\frac{2x_0}{a^2},\frac{2y_0}{b^2}\right)$.
Donc $\langle\nabla g(x_0,y_0)\cdot(x-x_0,y-y_0)\rangle=\frac{2x_0}{a^2}(x-x_0)+\frac{2y_0}{b^2}(y-y_0)=2\left(\frac{xx_0}{a^2}+\frac{yy_0}{b^2}-1\right)=0$ puisque $M\in\mathscr{E}$.
C'est donc l'équation de la tangente à l'ellipse : $\frac{xx_0}{a^2}+\frac{yy_0}{b^2}=1$

Courbes implicites

On admet :

Théorème - Paramétrage
Considérons une courbe $\mathscr{C}$ et $M(x_0,y_0)$ un point régulier de cette courbe.
On suppose que $\mathscr{C}$ a pour équation implicite $f(x,y)=0$.

Alors : si $\frac{\partial f}{\partial y}(x_0,y_0)\neq0$, il existe un paramétrage de classe $\mathscr{C}^1$ de la courbe $\mathscr{C}$.
Autrement écrit : il existe $\epsilon>0$, $x,y:]-\epsilon,\epsilon[\to\mathbb{R}$ tels que
- $x(0)=x_0$ et $y(0)=y_0$.
- La courbe paramétrée $(x(t),y(t))$ a la même représentation localement que $\mathscr{C}$

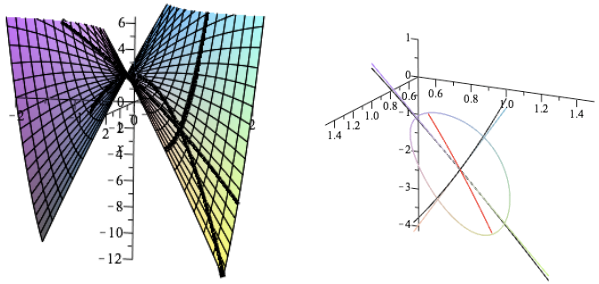
Analyse - Fonctions implicites
La tangente à la courbe paramétrée a pour coefficient directeur en $t=0$: $\frac{y'(0)}{x'(0)}$,
mais, comme également la tangente a pour équation $y=y_0-\frac{\frac{\partial f}{\partial x}(x_0,y_0)}{\frac{\partial f}{\partial y}(x_0,y_0)}\times(x-x_0)$,
elle a aussi pour coefficient directeur : $-\frac{\frac{\partial f}{\partial x}(x_0,y_0)}{\frac{\partial f}{\partial y}(x_0,y_0)}$.
Si le coefficient directeur n'est pas infini, la fonction $t\mapsto x$ est localement bijective (voisinage de 0).
Ainsi, en considérant $h=y\circ x^{-1}$, on a $h(x)=y(x^{-1}(x))=y$, soit une relation directe entre y et x.
et dont la dérivée est $h'(x)=y'(x^{-1}(x))\times(x^{-1})'(x)=y'(t)\times\frac{1}{x'(t)}$ avec $t=x^{-1}(x)$.
Et donc la dérivée $h'(x_0)$ est égale à $-\frac{\frac{\partial f}{\partial x}(x_0,y_0)}{\frac{\partial f}{\partial y}(x_0,y_0)}$.

Application - Thermodynamique
En physique, comme les fonctions sont les grandeurs, on fera quelques assimilations bien pratique.
Ainsi supposons une transformation qui conserve l'énergie : $U(P,T)=C^{ste}=U(P_0,T_0)$.
On a donc une relation entre les grandeurs P et T (ie. il existe h tel que $T=h(P)$ avec $h(P_0)=T_0$).
On a alors $h'(P_0)=-\frac{\frac{\partial U}{\partial P}(P_0,T_0)}{\frac{\partial U}{\partial T}(P_0,T_0)}$.
Ce qui avec la convention physicienne s'écrit : $\frac{\partial T}{\partial P}=-\frac{\frac{\partial U}{\partial P}}{\frac{\partial U}{\partial T}}$.
Une trop rapide simplification par ∂U n'expliquerait pas la présence du signe $-$.

5.2. Interprétation physique du gradient

Heuristique - Interprétation géométrique du gradient
Soit $\vec{a}\in U$. Dans la direction donnée par $\vec{u}$, la variation donnée par f est
$$f(\vec{a}+h\vec{u})-f(\vec{a})=h\langle\nabla f(\vec{a});\vec{u}\rangle$$
Nous savons que le produit scalaire est maximale lorsque les deux vecteurs multiplié sont colinéaires (optimisation de l'inégalité de Cauchy-Schwarz).
Donc pour h donné, la variation $f(\vec{a}+h\vec{u})-f(\vec{a})$ est extrémale si u est colinéaire à $\nabla f(\vec{a})$.
Par conséquent, $\nabla f(\vec{a})$ indique la plus forte pente (variation) de f en a.

Exemple - Retour sur la fonction $f(x,y)\to x^2-\frac{1}{2}y^2-4xy+2$
On a vu $\frac{\partial f}{\partial x}(x,y)=2x-4y$ et $\frac{\partial f}{\partial y}(x,y)=-y-4x$.
Donc $\nabla f(1,1)=\begin{pmatrix}-2\\-5\end{pmatrix}$.
La variation la plus forte de f au voisinage de $\vec{a}=(1,1)$ a pour direction $\begin{pmatrix}-2\\-5\end{pmatrix}$.



REPRÉSENTATION DU GRADIENT EN ROUGE,
DIRECTION DE L'ACCROISSEMENT MAXIMALE DE f

On peut dire encore mieux :

Proposition - Gradient
Soit $\vec{a}$ un point régulier de f.
Supposons que $f(\vec{a}) = C$.
Alors : $\nabla f(\vec{a})$ est orthogonal à la ligne de niveau $f(\vec{x}) = C$,
dans le sens des lignes de valeurs croissantes.

5.3. Optimum libre

Point critique

Heuristique - Etude des extremum
Dans le cadre des fonctions de $\mathbb{R}^p$ dans $\mathbb{R}$, il est légitime de chercher des extremums, puisque l'ensemble d'arrivée est $\mathbb{R}$ muni d'une relation d'ordre.
Nous allons essayer de répondre à cette question. Souvenons que pour les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ de classe $\mathscr{C}^1$, la nullité de la dérivée en x_0 est un critère nécessaire pour affirmer que $f(x_0)$ est un maximum (ou minimum) local de f.
Attention ce n'est pas une condition suffisante : penser à $x \mapsto x^3$ dont la dérivée s'annule en 0…

Définition - Extremum
Soit $f : U \subset \mathbb{R}^p \to \mathbb{R}$. Soit $\vec{a} \in U$
On dit que f admet un maximum (resp. mninimum) global sur U en $\vec{a}$
ssi $\forall\ \vec{x} \in U$, $f(\vec{a}) \geqslant f(\vec{x})$ (resp. $f(\vec{a}) \leqslant f(\vec{x})$)
On dit que f admet un maximum (resp. mninimum) local en $\vec{a}$
ssi $\exists\ \epsilon > 0$ tel que $\forall\ \vec{x} \in U \cap B_\epsilon(\vec{a})$, $f(\vec{a}) \geqslant f(\vec{x})$ (resp. $f(\vec{a}) \leqslant f(\vec{x})$).
Un maximum (resp. minimum) global est un maximum (resp. minimum) local.

Remarque - Extrema
On parle d'extremum pour parler de minimum ou de maximum.
Le pluriel est plutôt extrema,maxima,minima, mais on tolère extremums, maximums, minimums.

Définition - Points critiques
Soit $f : U \subset \mathbb{R}^p \to \mathbb{R}$ de classe $\mathscr{C}^1$ sur U.
On dit que $\vec{a}$ est un point critique de f si $\nabla f(\vec{a}) = \vec{0}$

Remarque - Les dérivées partielles en $\vec{a}$
Comme pour tout i, $\dfrac{\partial f}{\partial x_i}(\vec{a} = \mathrm{D}_i f(\vec{a}) = \langle \overrightarrow{\mathrm{grad}}(f)(\vec{a}); \vec{e}_i \rangle = \langle \vec{0}, \vec{e}_i \rangle = 0$, on en déduit que si $\vec{a}$ est un point critique de f, alors toutes les dérivées partielles de f sont nulles en $\vec{a}$.
La réciproque est vraie.

Proposition - Point critique et optimalité
Soit $f : U \subset \mathbb{R}^p \to \mathbb{R}$ de classe $\mathscr{C}^1$ sur U.
Supposons que f possède un extremum local en $\vec{a}$.
Alors : $\vec{a}$ est un point critique de f

Attention - La condition n'est que nécessaire
Penser un point-col (comme sur la figure 1 de ce chapitre), qui admet au point col un point critique (maximal selon x et minimal selon y), mais pas d'extremum

Démonstration
Soit $i \in \mathbb{N}_p$. Supposons que $\vec{a}$ est un maximum.

$$\forall\ t \quad f(\vec{a} + t\vec{e}_i) - f(\vec{a}) \leqslant 0$$
$$\forall\ t > 0 \quad \frac{f(\vec{a} + t\vec{e}_i) - f(\vec{a})}{t} \leqslant 0$$

En passant à la limite, on a donc $\dfrac{\partial f}{\partial x_i}(\vec{a}) \leqslant 0$.

$$\forall\ t < 0 \quad \frac{f(\vec{a} + t\vec{e}_i) - f(\vec{a})}{t} \geqslant 0$$

En passant à la limite, on a donc $\dfrac{\partial f}{\partial x_i}(\vec{a}) \geqslant 0$.

Et par continuité de la dérivée partielle, on a nécessairement : $\dfrac{\partial f}{\partial x_i}(\vec{a}) = 0$.
Ceci est vrai pour tout $i \in \mathbb{N}_p$, donc $\nabla f(\vec{a}) = 0$ □

Méthode de recherche d'optimalité

Remarque - Ouvert, fermé et compact
Remarquons bien que la proposition présentée ici concerne **un ouvert** U.
Par contre souvenons-nous que toute application sur un partie fermée et bornée (compact) de $\mathbb{R}^p$ admet une borne supérieure et une borne inférieure, et que celles-ci sont atteintes par la fonction continue.

Savoir faire - Recherche d'extremum
Considérons f dont on recherche un extremum.

1. On montre l'existence de cet extremum en appliquant le théorème de continuité sur un compact K de E, donc un fermé borné si $E = \mathbb{R}^n$.
2. (a) On considère ensuite son intérieur. C'est un ouvert et on recherche les points critiques.
   Localement, on regarde s'il s'agit d'un maximum ou d'un minimum.
   On étudie donc $f(\vec{x}) - f(\vec{a})$.
   Directement ou bien avec l'aide d'un DL d'ordre 2 (si pos-

sible) :

$$f(\vec{x}) = f(\vec{a}) + \underbrace{0}_{\text{point critique}} + \frac{1}{2}\sum_{i=1}^{p}\sum_{j=1}^{p}\frac{\partial^2 f}{\partial x_i \partial x_j}(\vec{a})(x-a_i)(x-a_j) + o(\|\vec{x}-\vec{a}\|^2)$$

qu'on étudie…

(b) On recherche les points sur la frontière.
Souvent ce sera un ensemble où chaque x_i est bloqué sauf un.

Remarque - Système d'équations, non linéaires
Il arrive souvent que le système soit associé à des équations non linéaires.
La méthode du pivot de Gauss est alors vouée à l'échec.
Dans ce cas, on n'a pas mieux que la substitution. Seulement ici, vous êtes tolérés à l'employer…

Exercice
Etudier les extremums globaux de $f : (x,y) \mapsto x^2+y^2-2x-4y$ sur $U = [0,3]\times[1,5]$.

Correction

1. U est fermé, borné ; f est polynomiale donc continue.
Donc f admet sur U un maximum global et un minimum global.

2. (a) Si ces point sont à l'intérieur de U, ils sont nécessairement des points critiques.
Leurs coordonnées (x_0,y_0) vérifient donc $\nabla f(x_0,y_0)$.
$$\begin{cases} 2x_0-2 &= 0\\ 2y_0-4 &= 0\end{cases} \iff \begin{cases} x_0 &= 1\\ y_0 &= 2\end{cases}$$
On a alors :
$$f(1+h,2+k) = (1+h)^2+(2+k)^2-2(1+h)-4(2+k) = \underbrace{-5}_{=f(1,2)} + \underbrace{0\times h+0\times k}_{\text{point critique}} + h^2+k^2$$
Donc pour tout $h,k\in\mathbb{R}$, $f(1+h,2+k)\geqslant -5 = f(1,2)$.
Ainsi f possède un minimum global sur U en $(1,2)$.

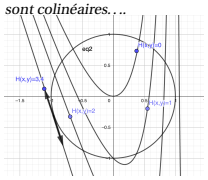
(b) Il faut compléter l'étude avec l'étude à la frontière pour trouver le maximum global sur U.
Il n'y a pas de maximum local à l'intérieur de U La frontière de U se décompose en quatre parties : $\{0\}\times[1,5]$, $\{3\}\times[1,5]$, $[0,3]\times\{1\}$ et $[0,3]\times\{5\}$.
Sur ces ensembles, on est amené à étudier :
— $g_1 : [1,5]\to\mathbb{R}$, $y\mapsto y^2-4y = y(y-4)$, maximale sur $[1,5]$ en $y=5$ avec pour valeur 5.
— $g_2 : [1,5]\to\mathbb{R}$, $y\mapsto 3+y^2-4y = y(y-4)$, maximale sur $[1,5]$ en $y=5$ avec pour valeur 8.
— $f_1 : [0,3]\to\mathbb{R}$, $x\mapsto x^2-2x-3 = x(x-2)-3$, maximale sur $[0,3]$ en $x=3$ avec pour valeur 0.
— $f_2 : [0,3]\to\mathbb{R}$, $x\mapsto x^2-2x+5 = x(x-2)+5$, maximale sur $[0,3]$ en $x=3$ avec pour valeur 8.

Ainsi f admet un minimum global en $(1,2)$, et un maximum global en $(3,5)$. Puis
$$\forall (x,y)\in U,\qquad -5 = f(1,2)\leqslant f(x,y)\leqslant f(3,5) = 8$$

5.4. Optima liés

Analyse - Problèmatique
Il arrive plutôt de chercher le maximum d'une fonction H sous certaines contraintes $\vec{u}\in C$.
Par exemple, on peut chercher le maximum de $H:\mathbb{R}^2\to\mathbb{R}$ sous la contrainte $x^2+y^2=1$.
• Première stratégie :
On définit, $h:\mathbb{R}\to\mathbb{R}$, $x\mapsto H(x,\sqrt{1-x^2})$, on a réduit le nombre de variables en fonction des contraintes qui lie finalement les variables entre elle.
Il reste ensuite à étudier la première cette fonction h.
$$h'(x) = \frac{\partial H}{\partial x}(x,\sqrt{1-x^2}) + \frac{-x}{\sqrt{1-x^2}}\frac{\partial H}{\partial y}(x,\sqrt{1-x^2})$$
x_0 est un point critiique de h ssi $\vec{u_0} = (x_0,\sqrt{1-x_0^2})$ est un point qui vérifie : $\frac{\partial H}{\partial x}(\vec{u}) + \frac{dy}{dx}(x_0)\frac{\partial H}{\partial y}(\vec{u})$ (avec la notation physicienne).

Représentation - Optima llié : colinéarité…
On a représenté $H(x,y) = 3x^2+xy-y$, sous la forme de ligne de niveau $H(x,y)=0$, … $H(x,y)=3.4$.
On notera pour la cas maximal : le dérivées partielles de H et de C au même point maximal sont colinéaires. …



Si on note $\varphi : (x,y)\mapsto x^2+y^2-1$, il faut lire $\frac{dy}{dx}(x_0)$ comme $\frac{\frac{\partial\varphi}{\partial x}}{\frac{\partial\varphi}{\partial y}}(\vec{u})$.
Et donc on a la condition : (en $\vec{u}$) : $\frac{\partial\varphi}{\partial y}\times\frac{\partial H}{\partial x} - \frac{\partial\varphi}{\partial x}\times\frac{\partial H}{\partial y} = 0$.
• Ainsi, (et cela conduit à la seconde stratégie) : les vecteur ∇H et $\nabla\varphi$ sont colinéaires.
On a le théorème suivant, dont on donnera une démonstration l'année prochaine.
On notera qu'il s'agit d'un critère nécessaire et non suffisant :

Théorème - Extrema lié. Optimisation sous contrainte
Soient f et $g_1,\dots g_r$ sont des fonctions numériques définies et de classe $\mathscr{C}^1$ sur l'ouvert U de E,
Notons X l'ensemble des zéros de g_1, $g_2\dots g_r$.
Si $\vec{x}\in X$, avec $\forall\, i\in\mathbb{N}_r$, $\mathrm{d}g_i(\vec{x})\neq 0$ et si $f_{|g_1,\dots g_r}$ admet un extremum en $\vec{x}$, alors $\nabla f(\vec{x})\in \mathrm{vect}\big(\nabla g_1(\vec{x}),\dots\nabla g_r(\vec{x})\big)$.

Remarque - Si $r=1$
Cela signifie simplement que $\nabla f(x)$ et $\nabla g(x)$ sont colinéaires.

Application - Maximum d'entropie $H:(x,y)\mapsto -x\ln x - y\ln y - z\ln z$ sous les contraintes $x+y+z=1$ et $xE_1+yE_2+zE_3=E$
Selon la première méthode, on a $y = \frac{E-E_3+(E_3-E_1)x}{E_2-E_3}$ et $z = \frac{E-E_2+(E_2-E_1)x}{E_3-E_2}$, puis $h(x) = -x\ln x - \dots$ à optimiser.
Avec la seconde méthode, on garde les symétries du problème.
$$\exists\,\lambda_1,\lambda_2\in\mathbb{R}\text{ tel que }\left(\frac{\partial f}{\partial x},\frac{\partial f}{\partial y},\frac{\partial f}{\partial z},\right) = \lambda_1\left(\frac{\partial g_1}{\partial x},\frac{\partial g_1}{\partial y},\frac{\partial g_1}{\partial z},\right) + \lambda_2\left(\frac{\partial g_2}{\partial x},\frac{\partial g_2}{\partial y},\frac{\partial g_2}{\partial z},\right)$$
Ce qui donne trois équations (chacune des trois coordonnées) :
$$\frac{\partial}{\partial x}(f-\lambda_1 g_1-\lambda_2 g_2)=0 \qquad \frac{\partial}{\partial y}(f-\lambda_1 g_1-\lambda_2 g_2)=0 \qquad \frac{\partial}{\partial z}(f-\lambda_1 g_1-\lambda_2 g_2)=0$$

Savoir faire - Multiplicateurs de Lagrange
Soit à optimiser f sous les contraintes $g_1,\dots g_r$ sur le domaine U, ouvert de $\mathbb{R}^p$.
On considère $H:\mathbb{R}^p\times\mathbb{R}^r\to\mathbb{R}$, $(x_1,\dots x_p,\lambda_1,\dots\lambda_r)\mapsto f(x_1,\dots x_p) - \lambda_1 g_1(x_1,\dots x_p)+\cdots\lambda_r g_r(x_1,\dots x_p)$.
Alors si $\vec{x}$ est un optimum sous contrainte (« optimum lié »), nécessairement $\vec{x}$ est (la première partie d')un point critique de H.

Application - Distribution de Boltzmann
On considère donc $U:(x,y,z,\lambda_1,\lambda_2)\mapsto H(x,y,z)-\lambda_1(x+y+z-1)-\lambda_2(E_1x+E_2y+E_3z-E)$.
On a $\frac{\partial U}{\partial x}(x,y,z,\lambda_1,\lambda_2) = \ln x - 1-\lambda_1-\lambda_2E_1 = 0$
$\frac{\partial U}{\partial y}(x,y,z,\lambda_1,\lambda_2) = \ln y-1-\lambda_1-\lambda_2E_2$ et $\frac{\partial U}{\partial z}(x,y,z,\lambda_1,\lambda_2) = \ln z-1-\lambda_1-\lambda_2E_3$
et les deux conditions de contraintes.
Donc $x=\exp(A+\lambda_2E_1) = C\exp(-BE_1)$, $y = C\exp(-BE_2)$ et $z = C\exp(-BE_3)$ avec $C=\exp(1+\lambda_1)$ et $B=-\lambda_2$.
Et par ailleurs les équations $x+y+z=1$ et $E_1x+E_2y+E_3z=E$ donnent des valeurs précises à C et B.

6. Bilan

Synthèse

⇝ Avec la notion de norme, on généralise les valeurs absolues sur les espaces vectoriels.

Sur les espaces de dimension finie (comme $\mathbb{R}^2$), toutes les normes étant équivalentes, nous n'avons aucune difficulté à définir les limites de suite et de fonctions.
On profite de ce petit passage sur des questions de topologie pour définir à l'aide de boule (généralisation sur E d'intervalles de $\mathbb{R}$), les ouvertes, fermés, l'adhérence et l'intérieur d'un ensemble.

⇝ Puis, nous nous concentrons sur les fonctions f de $\mathbb{R}^p$ sur $\mathbb{R}$. Démontrer la continuité n'est pas une chose facile, il faut voir si le calcul qui définit f est continue (souvent polynomial) sinon, on n'a pas de moyen d'étudier cette continuité.
En revanche à l'aide de suite, on peut démontrer la non-continuité de certaines fonctions.

⇝ On cherche alors à dériver/différentier ces fonctions, ce qui donne une formule de type développement limité. Malheureusement, la dérivation n'assure pas la continuité.
Quand les fonctions étudiées sont obtenues par composition, il est nécessaire d'exploiter la formule de la chaine, sorte de généralisation de la formule de dérivation d'une composée de fonctions.

⇝ Représenter de telles fonctions n'est pas facile. On voit, qu'en science, on alterne entre trois modes de représentations de fonctions (sous forme de surface) : explicite - $z = f(x,y)$, implicite - $f(x,y,z) = 0$ ou paramétré - $(x,y) = (x(t,u), y(t,u))$.
Pour bien comprendre ce que l'on fait, il est important de bien faire la différence entre ces représentations.
C'est en particulier le cas, lorsqu'on cherche un plan tangent ou à optimiser un certain problème.
D'ailleurs pour résoudre ce problème d'optimisation, on a deux stratégies selon que l'on soit sans ou avec contrainte(s).

Savoir-faire et Truc & Astuce du chapitre

229. Savoir-faire - Renverser l'inégalité triangulaire
230. Savoir-faire - Montrer qu'une partie est un ouvert. Avec des voisinage !
231. Savoir-faire - Montrer qu'une partie est un fermé. Avec des suites !
232. Savoir-faire - Caractérisation de $x \in \overline{A}$
233. Savoir-faire - Caractérisation de $x \in A^0$
234. Savoir-faire - Contournement du problème pour exploiter l'image réciproque
235. Savoir-faire - Un bon critère de non continuité
236. Savoir-faire - Continuité de $\|\cdot\|$.
237. Savoir-faire - Montrer qu'une application est continue
238. Truc & Astuce pour le calcul - Calculer les dérivées partielles
239. Truc & Astuce pour le calcul - Comment dériver des fonctions composées
240. Savoir-faire - Recherche d'extremum
241. Savoir-faire - Multiplicateur de Lagrange

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\partial f(a)(\cdot)$	Différentielle de f en a, élément de $\mathscr{L}(E,F)$	Fonction linéaire, égale à $\epsilon(h)$ près à $f(a+h)-f(a)$	
∂f	(Fonction) différentielle de f de $E \to \mathscr{L}(E,F)$	(voir ligne précédente)	Ne pas oublier des arguments…
$\frac{\partial f}{\partial x_k}$	(Fonction) dérivée partielle de f selon la k^e variable (dans la base canonique, orthonormée)	$\frac{\partial f}{\partial x_k}(\vec{x}) = \lim h \to 0 \frac{f(\vec{x}+he_k)-f(\vec{x})}{h}$	Il existe d'autres notations : $D_k f$…
∇f	Gradient de f (c'est une fonction à valeurs vectorielles)	Vecteur dont la coordonnée k est $\frac{\partial f}{\partial x_k}(\vec{x})$	$\mathrm{DL}_1 : \mathrm{d}f(\vec{x})(\vec{h}) = \langle \nabla f(x); \vec{h}\rangle + \|h\| \times \epsilon(h)$ avec $\epsilon(h) \to 0$

Retour sur les problèmes

164. La notion de norme généralise la valeur absolue.
165. Les normes équivalentes sont la solutions au problème. Dans un espace vectoriel de dimension finie, toutes les normes sont équivalentes.
166. On exploite la définition de la limite (dans tout le voisinage), pour définir la continuité.
167. $\sqrt{4,001} \approx 2 + 0,001 \times \frac{\partial \sqrt{}}{\partial x}(4) = 2 + 0,00025 = 2,00025$
168. Non. Contre-exemple vu dans le cours.
169. Cours

Annexes

Annexe A

Suite de variable aléatoire. Convergence (HP)

Résumé -

Totalement hors-programme (sauf la loi faible des grands nombres, au programme de seconde année, mais sans le vocabulaire bien adapté), on peut considérer cette partie comme une application des deux chapitres précédents.
Ce qui unit les différents résultats ici, est la notion de suite de variables aléatoires. Et en particulier, la question de la convergence associée.
Plusieurs modes de convergence sont assez naturels, nous en proposons trois ici. En seconde année, les différents modes de convergence de suites de fonctions sont également un morceau important. On peut faire un parallèle entre ces deux parties.
C'est aussi l'occasion de revenir sur un résultat parachuté en terminale : le théorème de Moivre-Laplace, conséquence d'un sommet des mathématiques : le théorème limite central, mais qui nécessite, à notre avis de passer par un certain nombre d'étapes intermédiaires (définition, vocabulaire, démonstration…), pour vraiment comprendre ce que l'on manipule.
Quelques vidéos :

- *Maths en tête : Alexandre Morgan - La dynastie des Bernoulli / Maths C qui ? #10 - https ://www.youtube.com/watch ?v=jWut-6jBl3U*
- *Sur le Chemin des Maths - Histoire des Mathématiques 03 : Abraham de Moivre de la loi binomiale à la loi normale - https ://www.youtube.com/watch ?v=uLbPKe3LT28*
- *Statoscope - Convergence en loi vs convergence en probabilité - https ://www.youtube.com/watch ?v=9O1ves_L2eM*

Sommaire

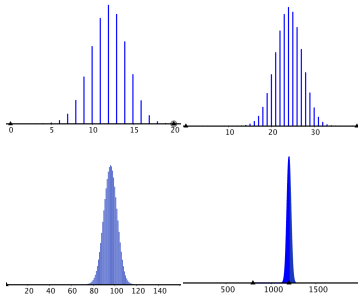
1. Problèmes 864
2. Suite de variable aléatoire 865
2.1. Suite de variables aléatoires 865
2.2. Exemples de convergence de variable aléatoire . . . 865
3. Différents modes de convergence 866
3.1. convergence presque sûre 866
3.2. Convergence en probabilité 869
3.3. Lien entre ces deux convergences de variables aléatoires 869
3.4. Convergence en loi 870
4. Loi (faible) des grands nombres et estimateurs 872
4.1. Lois des grands nombres 872
4.2. Estimateurs 872
5. Théorème limite central 874

5.1. Rappels sur la loi normale 874
5.2. Enoncé 875
5.3. Intervalle de confiance 876
6. Bilan 877

1. Problèmes

? Problème A1 - $\frac{S_n}{n} \to$?

On a fait la représentation pour $p = 0,6$ et $n = 20$, $n = 40$, $n = 160$ et $n = 2000$:



L'expérience montre que M_n devrait tendre vers p, ce qu'illlustre le resserrement du pic.
Qu'en penser?

? Problème A2 - Convergence (en loi)

En point d'orgue du programme de mathématique en terminale, figure le théorème de Moivre-Laplace.
Quel est sa sginification? Et comment se démontre-t-il?
Il s'agit d'une limite pour des variables aléatoires. Que signifie qu'une suite de variables aléatoires convergent?

? Problème A3 - Estimateur

Quel rapport entre l'espérance mathématique et l'estimateur d'une expérience?
Lorsqu'on répète un grand nombre de fois une même expérience, quels sont les résultats qu'on obtient? Comment faire le lien entre

- la probabilité d'une variable aléatoire, souvent choisis comme modèle selon les symétries de l'expérience,
- son espérance mathématique
- la moyenne expérimentale des résultats obtenus, lors de la répétition un grand nombre de fois de l'expérience associée?

2. Suite de variable aléatoire

2.1. Suite de variables aléatoires

La définition suivante est un rappel :

Définition - Indépendance pour une suite de v.a.
Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires définies sur $(\Omega,\mathbf{P})$.
$(X_n)_{n\in\mathbb{N}}$ est une suite de variables aléatoires mutuellement indépendantes si, pour tout $n\in\mathbb{N}^*$, les variables aléatoires $X_1,\dots,X_n$ sont mutuellement indépendantes.

Heuristique - Cas classique
Très souvent, n représente le temps.
On répète un certain nombre de fois une même expérience élémentaire. On note X_k, le résultat d'une certaine mesure sur l'expérience k.
On obtient ainsi une suite de variable aléatoire.
Très souvent, les expériences répétées sont indépendantes. On a alors une suite (X_k) de variable aléatoire indépendante, identiquement distribué (notée « *v.a.i.i.d.* » dans la littérature probabiliste).
C'est le cas par exemple lorsqu'on répète une même expérience en science physique. Le résultat est d'une certaine façon une variable aléatoire (même si son espérance est très précise…)

Remarque - Cas classique (2). Ω infini (dénombrable)
Il n'est pas rare que Ω soit en fait infini, même si pour tout n, X_n est définie sur Ω_n, un ensemble fini.
On aurait alors $\Omega_n=\pi_n(\Omega)$, où pour $\omega=(\omega_i)_{i\in\mathbb{N}}\in\Omega$, $\pi_n\big((\omega_i)_{i\in\mathbb{N}}\big)=(\omega_1,\omega_2,\dots\omega_n)$.
C'est hors programme de première année, mais pas de seconde année (donc au programme des concours).

2.2. Exemples de convergence de variable aléatoire

Remarque - Différents modes de convergence
Une des difficultés est qu'il existe des modes de convergence variés pour les variables aléatoires. Ils sont plus ou moins « forts » … Pour aborder ces différentes notions, nous allons considérer une famille d'exemple.

Exemple - Variable de Bernoulli répétée
Considérons une première suite (X_i) de variable aléatoire indépendante et de même loi $\mathscr{B}(p)$.
Notons alors $S_n=\sum_{k=1}^{n}X_k$. On sait que $S_n\hookrightarrow\mathscr{B}(n,p)$.
Représentons différentes valeurs de S_n (pour différentes valeurs de n). Le bon mode de représentation est l'histogramme.
Mais « trichons un peu », de manière à ce que chaque représentation soit comparable. Donc comme $S_n(\Omega)=[\![1,n]\!]$, on représente plutôt (et finalement assez naturellement) $M_n=\frac{1}{n}S_n$.

Heuristique - Convergence de variable aléatoire
Comment interpréter ce « devrait tendre » :
- Interprétation déterministe : pour toute réalisation ω du hasard, on a $M_n(\omega)\to p$.
  Ceci est clairement faux. Dans Ω, on a par exemple ω tel que $X_i(\omega)=\frac{1}{2}(1+(-1)^i)$ (une fois sur 2 X vaut 0 ou 1).
- Interprétation forte : avec une probabilité égale à 1, la suite $M_n(\omega)\to p$.
  $$\mathbf{P}(\{\omega\mid M_n(\omega)\to p\})=1$$
  Il s'agit de la convergence presque sûree que nous verrons plus loin.
  Elle conduit à la loi forte des grands nombres.
- Interprétation faible : l'ensemble des moyennes qui reste écartées de p de plus de ϵ (quelconque) tend vers 0.
  $$\forall\,\epsilon>0,\qquad \mathbf{P}(\{\omega\mid|M_n(\omega)-p|>\epsilon\})\longrightarrow 0$$
  Il s'agit de la convergence en probabilité que nous verrons plus loin.
  Elle conduit à la loi faible des grands nombres.

Remarque - On notera l'interversion des ϵ (et plus) entre les convergences p.s. et en probabilité
Pour une convergence presque sûre, on a :
$$\mathbf{P}\big(\{\omega\mid\forall\,\epsilon,\exists\,N_\epsilon(\omega)\mid\forall\,n\geqslant N_\epsilon(\omega),|M_n(\omega)-p|<\epsilon\}\big)=1$$
ou en passant au complémentaire :
$$\begin{aligned}0&=\mathbf{P}\left(\overline{\{\omega\mid\forall\,\epsilon,\exists\,N_\epsilon(\omega)\text{ tq }\forall\,n\geqslant N_\epsilon(\omega),|M_n(\omega)-p|<\epsilon\}}\right)\\&=\mathbf{P}\big(\{\omega\mid\exists\,\epsilon>0\text{ tq}\forall\,n\in\mathbb{N},\exists\,N>n\text{ tq }|M_N(\omega)-p|>\epsilon\}\big)\end{aligned}$$
Ce qui peut s'écrire avec des suites extraites :
$$\mathbf{P}(\{\omega\mid\exists\,\epsilon>0,\exists\,\varphi:\mathbb{N}\to\mathbb{N}\nearrow\nearrow\text{ tq}\forall\,n\in\mathbb{N},|M_{\varphi(n)}(\omega)-p|>\epsilon\}=0$$
Pour une convergence en probabilité, on a :
$$\forall\,\epsilon>0,\qquad u_n(\epsilon):=\mathbf{P}(\{\omega\mid|M_n(\omega)-p|>\epsilon\}\longrightarrow 0$$
$$\forall\,\epsilon>0,\forall\,\alpha>0,\exists\,N_\alpha\text{ tq }\forall\,n\geqslant N_\alpha,|u_n(\epsilon)|\leqslant\alpha$$

Heuristique - Convergence de loi (de var) (» convergence en loi »)
On peut s'intéresser à plus que la limite de M_n. En effet, on peut s'intéresser aux fluctuations autour de p. L'échelle de fluctuations de M_n autour de sa valeur est de l'ordre de l'écart-type : $\sigma(M_n)=\frac{\sigma(X_i)}{\sqrt{n}}$.
Pour comparer ces M_n, on s'intéresse donc à sa version centrée réduite : $M_n^*=\frac{S_n-np}{\sqrt{n}\sqrt{p(1-p)}}$.
On ne peut pas espérer une convergence de variable, car les fluctuations restent importantes : de l'ordre de l'unité.
Mais on peut espérer une estimation de la répartition, ou encore une loi (limite) de probabilité de la variable aléatoire de répartition.
On a donc besoin d'une nouvelle notion de convergence : la convergence en loi. Le théorème clé est alors le théorème limite centrale.

3. Différents modes de convergence

On considère dans cette section des variables aléatoires réelles $X_1,X_2,\dots X_n\dots$ et X, toutes définies sur un même espace de probabilité.

3.1. convergence presque sûre

La première convergence dérive d'une convergence d'événements

Pour aller plus loin - Convergence naturelle simple
Evidement la convergence la plus naturelle, mais également trop rare pour être rencontrée est donnée par :
$$\forall\,\omega,X_n(\omega)\to X(\omega)$$

Définition - convergence presque sûre
La suite (X_n) **converge presque sûrement** vers X si
$$\mathbf{P}(\lim_{n\to\infty}X_n=X)=\mathbf{P}\big(\{\omega\mid\lim_{n\to\infty}X_n(\omega)=X(\omega)\}\big)=1$$
On note alors $X_n\xrightarrow{ps}X$.

Dans une remarque précédente, on a vu que l'étude de la convergence par suite extraite pourrait être intéressante.

Définition - Infiniment souvent
Soit $\omega \in \Omega$, $\epsilon > 0$ et une suite Y_n de v.a.
On dit que $|Y_n(\omega)| > \epsilon$ infiniment souvent,
si il existe $\varphi : \mathbb{N} \to \mathbb{N}$ ↗↗ telle que pour tout $n \in \mathbb{N}$ $|Y_{\varphi(n)}(\omega)| > \epsilon$.
si $\{n \in \mathbb{N} \mid |Y_n(\omega)| > \epsilon\}$ n'est pas borné.
L'événement associé se note : $[|Y_n| > \epsilon$ i.s.$]$

Proposition - Événement équivalent
Pour tout $\omega \in \Omega$, et tout $\epsilon \in \mathbb{R}_+^*$

$$|Y_n(\omega)| > \epsilon \text{ i.s.} \iff \forall\, n \in \mathbb{N}, \exists\, p \geqslant n \text{ tel que } |Y_p(\omega)| > \epsilon$$

Ainsi :

$$\{\omega \in \Omega \mid |Y_n(\omega)| > \epsilon \text{ i.s.}\} = \bigcap_{n\in\mathbb{N}} \left(\bigcup_{p \geqslant n} \{\omega \mid |Y_p(\omega)| > \epsilon\} \right)$$

Démonstration
Il s'agit simplement de mettre en forme ensembliste les quantificateurs : $\exists \leftrightarrow \cup$ et $\forall \leftrightarrow \cap$ □

Heuristique - Réunion décroissante. Passage à la limite
Si on note A_n, l'événement $\bigcup_{p\geqslant n} \{\omega \mid |Y_p(\omega)| > \epsilon\}$.
Alors $\omega \in A_{n+1} \Rightarrow \exists\, p \geqslant n+1 (\geqslant n)$ tel que $|Y_p(\omega)| > \epsilon \Rightarrow \omega \in A_n$.
Donc $A_{n+1} \subset A_n$, i.e. la suite (A_n) est décroissante.
Donc pour tout $N \in \mathbb{N}$, $\bigcap_{n=1}^{N} A_n = A_N$. Pour passer à la limite, on utilise le théorème de convergence décroissante :

$$\mathbf{P}\left(\bigcap_{n\in\mathbb{N}} A_n\right) = \lim_{N\to+\infty} \mathbf{P}(A_N)$$

Proposition - Critère équivalent à la convergence presque sûre
La suite (X_n) **converge presque sûrement** vers X
si et seulement si $\forall\, \epsilon > 0$, $\mathbf{P}(|X_n - X| > \epsilon, \text{infiniment souvent}\} = 0$
si et seulement si $\forall\, \epsilon > 0$, $\lim\limits_{N\to\infty} \mathbf{P}(\exists\, n \geqslant N \mid |X_n - X| > \epsilon) = 0$.

Démonstration
Avec des suites extraites, dire que $X_n(\omega)$ ne tend pas vers $X(\omega)$ c'est dire :

$$\exists\, \epsilon > 0, \exists\, \varphi : \mathbb{N} \to \mathbb{N} \nearrow\nearrow \text{ tq } |X_{\varphi(n)}(\omega) - X(\omega)| > \epsilon$$

Donc en terme d'événement (ou d'ensemble)

$$\overline{[X_n \to X]} = \bigcup_{\epsilon>0} [|X_n - X| > \epsilon, \text{infiniment souvent}]$$

Donc on a équivalence entre :
— $X_n \xrightarrow{ps} X$
— $\mathbf{P}([X_n \to X]) = 1$
— $\mathbf{P}(\overline{[X_n \to X]}) = 0$
— $\mathbf{P}\left(\bigcup_{\epsilon>0} [|X_n - X| > \epsilon, \text{infiniment souvent}]\right) = 0$

On a donc les équivalences :

$$X_n \xrightarrow{ps} X \iff \mathbf{P}\left(\bigcup_{\epsilon>0} [|X_n - X| > \epsilon, \text{infiniment souvent}]\right) = 0$$

Sens direct.
On fixe $\epsilon_0 > 0$.
, $[|X_n - X| > \epsilon_0, \text{infiniment souvent}] \subset \bigcup\limits_{\epsilon>0} [|X_n - X| > \epsilon, \text{infiniment souvent}]$,
on a donc $\forall\, \epsilon_0 > 0$, $\mathbf{P}(|X_n - X| > \epsilon_0, \text{infiniment souvent}) = 0$.
Réciproquement : si $\forall\, \epsilon > 0$, $\mathbf{P}(|X_n - X| > \epsilon, \text{infiniment souvent}) = 0$,

alors $\forall\, \epsilon_0 > 0$, $\mathbf{P}\left(\bigcup\limits_{\epsilon<\epsilon_0} [|X_n - X| > \epsilon, \text{infiniment souvent}]\right) = \mathbf{P}(|X_n - X| > \epsilon_0, \text{infiniment souvent}) = 0$.

Il s'agit d'une suite décroissante d'événements : $\epsilon_1 < \epsilon 2$, $\bigcup\limits_{\epsilon>\epsilon_2} [|X_n - X| > \epsilon, \text{infiniment souvent}] \subset \bigcup\limits_{\epsilon>\epsilon_1} [|X_n - X| > \epsilon, \text{infiniment souvent}]$.

On peut passer à la limite dans la probabilité : $\lim_\epsilon \mathbf{P}(A_\epsilon) = \mathbf{P}(\lim\limits_\epsilon A_\epsilon)$.

Donc $\mathbf{P}(\bigcup\limits_{\epsilon>0} [|X_n - X| > \epsilon, \text{infiniment souvent}]) = 0$.

Enfin, si l'on souhaite préciser cet événement : Dire qu'infiniment souvent, $|X_n - X| > \epsilon$, cela signifie que pour tout N que l'on se fixe, il existe toujours $n > N$ tel que $|X_n - X| > \epsilon$.
En faisant tendre N vers l'infini, on retrouve le critère précédent. □

Savoir faire - Démontrer une convergence presque sûre
On exploite souvent le lemme de Borel-Cantelli.
En effet, il donne un argument de convergence infiniment souvent d'une probabilité

Pour aller plus loin - Réciproque?
Est-ce que la réciproque est vraie : si $\mathbf{P}(A_n, \text{ i.s.}) = 0$, alors $\sum\limits_{n\geqslant n_0} \mathbf{P}(A_n)$ converge?
On a une condition suffisante : la suite (A_p) est une suite d'événements indépendants. On étudie les événements contraires

$$\begin{aligned}\mathbf{P}\left(\bigcup_{p\geqslant N} A_p\right) &= 1 - \mathbf{P}\left(\overline{\bigcup_{p\geqslant N} A_p}\right)\\ &= 1 - \mathbf{P}\left(\bigcap_{p\geqslant N} \overline{A_p}\right)\\ &= 1 - \prod_{p\geqslant N} \mathbf{P}(\overline{A_p})\end{aligned}$$

Puis on compose par le ln*, comme on compare série et produit infini*

Théorème - Borel-Cantelli
Soit (A_n) une suite d'événements.
Si $\sum\limits_{n\geqslant n_0} \mathbf{P}(A_n)$ converge, alors $\mathbf{P}(A_n, \text{ i.s.}) := \mathbf{P}(\{\omega \mid \omega \in A_n \text{ i.s.}\}) = 0$

Démonstration
On a vu que $[A_n \text{ i.s.}] = \bigcap\limits_{n\in\mathbb{N}} \left(\bigcup\limits_{p\geqslant n} A_p\right)$.
On note $B_n = \cup_{p\geqslant n} A_p$. Il s'agit d'une suite d'événements décroissants.
Donc $\mathbf{P}(\bigcap\limits_{n\in\mathbb{N}} B_n) = \lim\limits_{N\to+\infty} \mathbf{P}(B_N)$.
Or $\mathbf{P}(B_N) = \mathbf{P}\left(\bigcup\limits_{p\geqslant N} A_p\right) \leqslant \sum\limits_{p\geqslant N} \mathbf{P}(A_p) = R_N$.
Mais la série $\sum\limits_{n\geqslant n_0} \mathbf{P}(A_n)$ converge, donc les restes tendent vers 0.
On trouve donc bien : $\lim_{N\to+\infty} \mathbf{P}(B_N) = 0$ et donc $\mathbf{P}(\bigcap\limits_{n\in\mathbb{N}} B_n) = 0$ i.e. $\mathbf{P}(A_n, \text{ i.s.}) = 0$.
□

L'exercice suivant donne une application directe.
Exercice
Soit (X_i) une suite de variables aléatoires indépendantes identiquement distribuée admettant un moment d'ordre 4.
On note $S_n = \frac{1}{n}\sum\limits_{k=1}^{n} X_k$.
En exploitant l'inégalité de Markov pour $\mathbf{P}((S_n - p)^4 > \epsilon^4)$, puis le lemme de Borel-Cantelli, montrer que S_n converge presque sûrement vers $p = \mathbf{E}(X_i)$

Correction
On applique l'inégalité de Markov à $(S_n - p)^4$ qui admet une espérance :

$$\forall\, \epsilon > 0, \qquad \mathbf{P}\left((S_n - p)^4 > \epsilon^4\right) \leqslant \frac{\mathbf{E}((S_n - p)^4)}{\epsilon^4}$$

Or $[S_n - p]^4 > \epsilon^4 \iff [S_n - p] > \epsilon$.
Puis $S_n - p = \frac{1}{n}\sum\limits_{i=1}^{n} (X_i - p)$.
Par linéarité de l'espérance et indépendance des X_i :

$$\begin{aligned}\mathbf{E}\left((S_n - p)^4\right) &= \mathbf{E}\left(\frac{1}{n^4}[\sum_{i=1}^{n}(X_i - p)]^4\right)\\ &= \frac{1}{n^4}\mathbf{E}\left(\sum_{i=1}^{n} X_i^{*4} + \sum_{i\neq j} 4X_iX_j^3 + 6X_i^2X_j^2 + \sum_{i\neq j\neq k} 12X_iX_jX_k^2 + \sum_{i\neq j\neq k\neq h} 24X_iX_jX_hX_k\right)\\ &= \frac{1}{n^3}\mu_4(X) + \frac{n-1}{2n^3}4\mu_1(X)\mu_3(X) + \frac{n-1}{2n^3}6\mu_2^2(X)\\ &\quad + \frac{(n-1)(n-2)}{6n^2}12\mu_1^2(X)\mu_2(X) + \frac{(n-1)(n-2)(n-3)}{24n^3}24\mu_1^4(X)\\ &= \frac{1}{n^3}\mu_4(X) + \frac{3(n-1)}{n^3}\mu_2^2(X)\end{aligned}$$

où $X_i^* = X_i - p$, donc $\mathbf{E}(X_i^*) = \mu_1(X)0$.

Donc, pour tout $\epsilon > 0$, $\mathbf{P}(|S_n - p| > \epsilon) \leqslant \frac{1}{\epsilon^4}\left(\frac{1}{n^3}\mu_4(X) + \frac{3(n-1)}{n^3}\mu_2^2(X)\right)$.

Donc la série $\sum_{n\geqslant 1} \mathbf{P}(|S_n - p| > \epsilon)$ converge (comparaison à une série de Riemann).

On applique le Lemme de Borel-Cantelli à $A_n = [|S_n - p| > \epsilon]$.

Ainsi, $\mathbf{P}([S_n - p > \epsilon \text{ i.s.})] = 0$. Ceci est vrai pour tout $\epsilon > 0$

3.2. Convergence en probabilité

Définition - Convergence en probabilité

La suite (X_n) **converge en probabilité** vers X si

$$\forall\, \epsilon > 0, \qquad \lim_{n\to+\infty} \mathbf{P}(|X_n - X| \geqslant \epsilon) = 0$$

On note alors $X_n \xrightarrow{\mathbf{P}} X$.

Savoir faire - Démontrer la convergence en probabilité

Très fréquemment, on emploie les inégalités de Markov ou de Bienaymé-Tchebychev pour démontrer qu'une suite de variable aléatoire converge en probabilité vers une constante.

Proposition - Stabilité

Si $X_n \xrightarrow{\mathbf{P}} X$ et $Y_n \xrightarrow{\mathbf{P}} Y$, respectivement $X_n \xrightarrow{ps} X$ et $Y_n \xrightarrow{ps} Y$.

Alors pour tout $\alpha, \beta \in \mathbb{R}$, $\alpha X_n + \beta Y_n \xrightarrow{\mathbf{P}} \alpha X + \beta Y$ resp. : $\xrightarrow{ps} \alpha X + \beta Y$.

Si $g : \mathbb{R} \to \mathbb{R}$ est continue alors $g(X_n) \xrightarrow{\mathbf{P}} g(X)$ resp. : $g(X_n) \xrightarrow{ps} g(X)$

La linéarité est assez simple à démontrer.

La composition par une fonction continue est plus compliquée… On l'admet. (On pourrait utiliser l'image réciproque de tout ouvert est un ouvert…).

Pour aller plus loin - Lien entre convergence

Si (X_n) converge presque sûrement vers X, alors (X_n) converge en probabilité vers X.

Si (X_n) converge en probabilité vers X, alors il existe $\varphi \nearrow\nearrow$, $(X_{\varphi(n)})$ converge presque sûrement vers X.

3.3. Lien entre ces deux convergences de variables aléatoires

Commençons par analyser un exemple.

Analyse - Une suite de variable aléatoire qui converge en probabilité mais pas presque sûrement.

On note $T_n = \frac{n(n+1)}{2} = \sum_{k=1}^{n} k$.

Pour tout $k \in \mathbb{N}$, $\exists\, n(k) \in \mathbb{N}$ tel que $T_{n(k)-1} < k \leqslant T_n(k)$.

Considérons alors $X_k = \mathbb{1}_{\left[\frac{k-T_{n(k)-1}-1}{n(k)}, \frac{k-T_{n(k)-1}}{n(k)}\right]}$, indicatrice Pour bien comprendre ce que signifie cette suite, on peut résumer sa construction de la façon suivante :

1. On coupe l'intervalle $[0,1]$ en un morceau et on considère $X_1 = \mathbb{1}_{[0,1]}$
2. On coupe l'intervalle $[0,1]$ en deux morceaux et on considère $X_2 = \mathbb{1}_{\left[0,\frac{1}{2}\right]}$ et $X_3 = \mathbb{1}_{\left[\frac{1}{2},1\right]}$
3. On coupe l'intervalle $[0,1]$ en trois morceaux et on considère $X_4 = \mathbb{1}_{\left[0,\frac{1}{3}\right]}$, $X_5 = \mathbb{1}_{\left[\frac{1}{3},\frac{2}{3}\right]}$ et $X_6 = \mathbb{1}_{\left[\frac{2}{3},1\right]}$
4. n On coupe l'intervalle $[0,1]$ en n morceaux et on considère $X_{T_{n-1}+1} = \mathbb{1}_{\left[0,\frac{1}{n}\right]}$, $X_{T_{n-1}+2} = \mathbb{1}_{\left[\frac{1}{n},\frac{2}{n}\right]}$,… et $X_{T_n} = \mathbb{1}_{\left[\frac{n-1}{n},1\right]}$
5. …

Alors pour la plupart des ω, $X_h(\omega) = 0$, mais régulièrement, $X_h(\omega) = 1$ (une et une seule fois entre chaque T_n et T_{n+1}).

Ainsi on peut considérer $X = 0$. Soit $\epsilon > 0$ et $\epsilon < 1$.

$$[|X_k - X| > \epsilon] = \{\omega \in \Omega \mid X_k(\omega) = 1\} \qquad \mathbf{P}(|X_k - X| > \epsilon) = \mathbf{E}\left(\mathbb{1}_{\left[\frac{k-T_{n(k)-1}-1}{n(k)}, \frac{k-T_{n(k)-1}}{n(k)}\right]}\right) = \frac{1}{n(k)} \xrightarrow[n\to\infty]{} 0$$

Donc X_n converge en probabilité vers $X = 0$.

En revanche, pour tout $\omega \in \Omega$, il existe une suite (ν_n) strictement croissante (infinie) tel que $X_{\nu_n}(\omega) = 1$.

Donc pour tout $\epsilon > 0$ (et inférieur à 1), on n'a pas $\lim_{N\to\infty} \mathbf{P}([\exists\, n \geqslant N \mid |X_n - X| > \epsilon) = 0$.

Ainsi X_n ne tend pas presque sûrement vers $X = 0$

Proposition - Implication des convergences

Si $(X_n) \xrightarrow{ps} X$, alors $(X_n) \xrightarrow{\mathbf{P}} X$.

Attention - Réciproque fausse

La réciproque est fausse comme le montre le contre-exemple vu en analyse

Démonstration

Notons $Y_n = |X_n - X|$. Soit $\epsilon > 0$ et pour tout $N \in \mathbb{N}$, $B_N(\epsilon)$ l'événement « il existe $n \geqslant N$ tel que $Y_n \geqslant \epsilon$ » La convergence presque sûre de (Y_n) vers 0 montre que $\lim_{N\to+\infty} \mathbf{P}(B_N(\epsilon)) = 0$.

Or pour tout entier n, $[Y_n > \epsilon] \subset B_n(\epsilon)$ ce qui prouve que par majoration que $\mathbf{P}([Y_n > \epsilon]) \to 0$ □

Toutefois, il y a presqu'équivalence ;

Proposition - Condition suffisante pour l'implication réciproque

Si $(X_n) \xrightarrow{\mathbf{P}} X$,

alors on peut extraire de X_n une sous-suite convergent presque sûrement vers X. Autrement écrit :

$$\exists\, \varphi \nearrow\nearrow \mid (X_{\varphi(n)}) \xrightarrow{ps} X$$

On ne fait pas la démonstration.

3.4. Convergence en loi

Comme son nom l'indique, la convergence en loi indique que la suite des lois de X_n converge vers la loi de X.

L'objet n'est plus directement la variable aléatoire…

Définition - Convergence en loi (variable discrète)

On note $E = \bigcup_{n\in\mathbb{N}^*} X_n(\Omega) \cup X(\Omega)$.

La suite (X_n) **converge en loi** vers X si

$$\forall\, x \in E, \qquad \lim_{n\to+\infty} \mathbf{P}(X_n = x) = \mathbf{P}(X = x)$$

Si $x \notin X_n(\Omega)$, on note $\mathbf{P}(X_n = x) = 0$ et de même si $x \notin X(\Omega)$, on note $\mathbf{P}(X = x) = 0$

On note alors $X_n \xrightarrow{\mathscr{L}} X$.

convergence pas tout à fait convergences

Remarque - Cas des variables continues
Lorsque $X(\Omega)$ n'est pas dénombrable, mais un ensemble compact dans $\mathbb{R}$ (comme en terminale), on ne calcule pas $\mathbf{P}(X=x)$, celle-ci est toujours nul.
Le calcul qui joue le rôle équivalent est donnée par la fonction de répartition : $\mathbf{P}(X \leqslant x) = \int_{-\infty}^{x} f(t)\mathrm{d}t$.
Ainsi le calcul d'espérance de X est $\mathbf{E}(X) = \int_{-\infty}^{+\infty} tf(t)\mathrm{d}t$ au lieu de $\sum_{k\in\mathbb{N}} k\mathbf{P}(X=k)$.
Et de même pour la définition de la convergence en loi :

Définition - Convergence en loi (variable continue)
On note $E = \bigcup_{n\in\mathbb{N}^*} X_n(\Omega) \cup X(\Omega)$.
La suite (X_n) **converge en loi** vers X si

$$\forall\, x \in E \text{ (non discontinuité)}, \quad \lim_{n\to+\infty} \mathbf{P}(X_n \leqslant x) = \mathbf{P}(X \leqslant x)$$

Il s'agit de la convergence simple des fonctions de répartition. On note alors $X_n \xrightarrow{\mathscr{L}} X$.

Attention - Pas de structure algébrique
Considérons X et Y indépendantes qui suivent la même loi binomiale $\mathscr{B}(n,p)$.
Considérons pour tout $n\in\mathbb{N}$, $X_n = X$ et $Y_n = n - X$.
Alors $X_n \hookrightarrow \mathscr{B}(n,p)$ et $Y_n \hookrightarrow \mathscr{B}(n,p)$.
Donc la convergence en loi de $\lim_{\mathscr{L}}(X_n) + \lim_{\mathscr{L}}(Y_n) \hookrightarrow \mathscr{B}(2n,p)$.
Alors que $X_n + Y_n = n$ alors donc $\lim_{\mathscr{L}}(X_n + Y_n) \hookrightarrow n$.

Proposition - Stabilité
Si $g : \mathbb{R} \to \mathbb{R}$ est continue alors $g(X_n) \xrightarrow{\mathscr{L}} g(X)$

Proposition - Convergence en probabilité implique la convergence en loi
Supposons que la suite (X_n) converge en probabilité vers X.
Alors (X_n) converge en loi vers X

On fait la démonstration dans le cas discret.

Démonstration
Soit (X_n) qui converge en probabilité vers X.
Soit $\epsilon > 0$. Soit $x \in X(\Omega)$,

$$[X_n = x] = [X_n = x, X < x-\epsilon] \cup \left[X_n = x, X \in [x-\epsilon, x+\epsilon]\right] \cup [X_n = x, X > x+\epsilon]$$

$$\mathbf{P}(X_n = x) = \mathbf{P}(X_n = x, X_n - X > \epsilon) + \mathbf{P}(X_n = x, X \in [x-\epsilon, x+\epsilon]) + \mathbf{P}(X_n = x, X - X_n > \epsilon)$$

$$\mathbf{P}(X_n = x) \leqslant \mathbf{P}(X \in [x-\epsilon, x+\epsilon]) + \mathbf{P}(|X - X_n| > \epsilon)$$

Comme $X(\Omega)$ est fini, l'ensemble $\{|x_i - x_j|\}$ est fini, il existe donc η tel que $\forall\ i,j, |x_i - x_j| > \eta$.
Donc avec $\epsilon < \eta$:

$$\mathbf{P}(X_n = x) \leqslant \mathbf{P}(X = x) + \mathbf{P}(|X - X_n| > \epsilon)$$

De même, on trouve :

$$\mathbf{P}(X = x) \leqslant \mathbf{P}(X_n = x) + \mathbf{P}(|X_n - X| > \epsilon)$$

Donc

$$|\mathbf{P}(X_n = x) - \mathbf{P}(X = x)| \leqslant \mathbf{P}(|X - X_n| > \epsilon)$$

On achève la démonstration en exploitant la convergence en probabilité. □

Un exemple très classique :

Proposition - Approximation poissonnienne
Notons X_n une variable aléatoire qui suit une loi binomiale de paramètre $(n, \frac{\lambda}{n})$.
Alors $X_n \xrightarrow{\mathscr{L}} X$, où $X \hookrightarrow \mathscr{P}(\lambda)$ la loi de Poisson de paramètre λ, c'est-à-dire :

$$X(\Omega) = \mathbb{N} \qquad \mathbf{P}(X=k) = e^{-\lambda}\frac{\lambda^k}{k!}$$

Démonstration
Soit $k\in\mathbb{N}$. Pour $n \geqslant k$, $k \in X_n(\Omega)$.

$$\begin{aligned}\mathbf{P}(X_n = k) &= \frac{n!}{k!(n-k)!}\frac{\lambda^k}{n^k}\left(1-\frac{\lambda}{n}\right)^{n-k} = \frac{\lambda^k}{k!}\frac{n\times(n-1)\dots(n-k+1)}{n\times n\times\dots n}\left(1-\frac{\lambda}{n}\right)^{n-k}\\ &= \frac{\lambda^k}{k!}\prod_{h=0}^{k-1}\left(1-\frac{h}{n}\right)\left(1-\frac{\lambda}{n}\right)^{n-k} = \frac{\lambda^k}{k!}\left(1-\frac{\lambda}{n}\right)^n\prod_{h=0}^{k-1}\left((1-\frac{h}{n})(1-\frac{\lambda}{n})^{-1}\right)\end{aligned}$$

Or k est fixé, le produit est fini et pour $n\to+\infty$: $\prod_{h=0}^{k-1}\left((1-\frac{h}{n})(1-\frac{\lambda}{n})\right)^{-1} \to 1$.

Donc $\mathbf{P}(X_n = k) \underset{n\to+\infty}{\longrightarrow} \frac{\lambda^k}{k!}e^{-\lambda}$. □

4. Loi (faible) des grands nombres et estimateurs

4.1. Lois des grands nombres

Théorème - Loi faible des grands nombres
Soit (X_n) une suite de variables aléatoires indépendantes de même espérance m et variance σ^2.
Alors la suite $M_n = \frac{1}{n}\sum_{k=1}^{n} X_k$ converge en probabilité vers la variable constante égale à m

Exercice
Ecrire ce résultat avec des ϵ

Correction
$\forall\,\epsilon > 0,\ \lim_{n\to+\infty} \mathbf{P}(|M_n - m| > \epsilon) = 0$

Démonstration
On exploite l'inégalité de Bienaymé-Tchebychev : car par linéarité de l'espérance $\mathbf{E}(M_n) = \frac{1}{n}\sum_{k=1}^{n}\mathbf{E}(X_k) = m$

$$\mathbf{P}(|M_n - m| > \epsilon) = \mathbf{P}(|M_n - \mathbf{E}(M_n)| > \epsilon) \leqslant \frac{\mathbf{V}(M_n)}{\epsilon^2}$$

Or $\mathbf{V}(M_n) = \frac{1}{n^2}n\sigma^2$, par indépendance des X_i.

$$\mathbf{P}(|M_n - m| > \epsilon) \leqslant \frac{\sigma^2}{n\epsilon^2} \to 0$$

□

Histoire - La loi des grands nombres et l'histoire des probabilités
On pourrait faire un cours de probabilité en suivant le fil de l'histoire et comment les mathématiciens ont, depuis Jacques Bernoulli, eu comme unique mission d'alléger les hypothèses de ce théorème ou de le rendre plus fort

La loi forte des grands nombres existe (Kolmogorov) avec quasiment aucune hypothèse supplémentaire (mais avec une démonstration plus costaud !).

4.2. Estimateurs

Heuristique - Faire la moyenne
Ce théorème est essentiel. Il affirme que si on fait une moyenne des résultats obtenus en répétant une même expérience aléatoire (des mesures après une répétition d'une même expérience), alors celle-ci va converger vers l'espérance de la loi.
Une autre application est la suivante. On réalise un très grand nombre de simulations informatiques (avec Python), on fait la moyenne des résultats, et on obtient un résultat

, mathématique précis. C'est la philosophie des méthodes dites de Monte-Carlo

Voilà enfin démontrer la raison pour laquelle nous calculons les moyennes des élèves… Mais il peut y avoir d'autres estimateurs.

Heuristique - Contexte

On considère un phénomène aléatoire et on s'intéresse à une variable aléatoire réelle X qui lui est liée, dont on suppose que la loi de probabilité n'est pas complètement spécifiée et appartient à une famille de lois dépendant d'un paramètre θ décrivant un sous-ensemble $\Theta \in \mathbb{R}$. Le paramètre θ est une quantité inconnue, fixée dans toute l'étude, que l'on cherche à déterminer ou pour laquelle on cherche une information partielle.
Le problème de l'estimation consiste alors à estimer la vraie valeur du paramètre θ (ou de $g(\theta)$ -fonction à valeurs réelles du paramètre θ), à partir d'un échantillon de données $x_1,\dots,x_n$ obtenues en observant n fois le phénomène. Cette fonction du paramètre représentera en général une valeur caractéristique de la loi inconnue comme son espérance, sa variance, son étendue...

Définition - Estimateur de $g(\theta)$
Un estimateur de $g(\theta)$ est une variable aléatoire de la forme $T_n = \Phi(X_1,\dots,X_n)$.
La réalisation $\Phi(x_1,\dots,x_n)$ de l'estimateur T_n est l'estimation de $g(\theta)$. Cette estimation ne dépend que de l'échantillon $(x_1,x_2,\dots,x_n)$ observé.

Exemple - Moyenne
Si $X_1,\dots X_n$ sont des variables aléatoires indépendantes de même espérance m.
Alors la moyenne de $X_1,\dots X_n$ est un estimateur (empirique) de m.

Définition - Biais et estimateur sans biais
Si pour tout $\theta \in \Theta$, l'estimateur T_n admet une espérance, on appelle **biais de T_n en** $g(\theta)$ le réel
$$b_\theta(T_n) = \mathbf{E}_\theta(T_n) - g(\theta)$$
L'estimateur T_n de $g(\theta)$ est dit estimateur sans biais si pour tout $\theta \in \Theta$, $\mathbf{E}_\theta(T_n) = g(\theta)$.

Définition - Estimateur convergent
Une suite d'estimateurs $(T_n)_{n\geqslant 1}$ de $g(\theta)$ est convergente si pour tout θ, la suite $(T_n)_{n\geqslant 1}$ converge en probabilité vers $g(\theta)$.
Par abus de langage on dit rapidement que l'estimateur est convergent.

Exercice
On considère une suite (X_i) de variables aléatoires indépendantes qui suivent toute la même loi de Benoulli de paramètre p.
Et l'on cherche un estimateur de la variance V de cette loi.

1. On considère $M_n = \dfrac{1}{n}\sum_{k=1}^{n} X_k$.
   Montrer que M_n est un estimateur sans biais de p.
   Est-il convergent ?
2. On considère $V_n = \dfrac{1}{n}\sum_{k=1}^{n} (X_k - M_n)^2$.
   V_n est-il un estimateur sans biais de V ? Sinon calculer biais.
   Est-il convergent ?
3. On considère $W_n = \dfrac{1}{n-1}\sum_{k=1}^{n} (X_k - M_n)^2$.
   W_n est-il un estimateur sans biais de V ? Sinon calculer le biais.

Correction

1. $\mathbf{E}(M_n) = \dfrac{1}{n}\sum_{k=1}^{n} \mathbf{E}(X_k) = m$.
   Donc M_n est un estimateur sans biais de p. D'après la loi faible des grands nombres, il est convergent (en probabilité) vers p.
2. On considère $V_n = \dfrac{1}{n}\sum_{k=1}^{n} (X_k - M_n)^2$.
   $$\mathbf{E}(V_n) = \frac{1}{n}\sum_{k=1}^{n} \mathbf{E}((X_k - M_n)^2)$$
   Or
   $$(X_k - M_n)^2 = X_k^2 + M_n^2 - 2X_kM_n = \left(1-\frac{2}{n}\right)X_k^2 + M_n^2 - \frac{2}{n}\sum_{i\neq k} X_kX_i$$
   Donc
   $$\mathbf{E}(V_n) = \frac{1}{n}\sum_{k=1}^{n}\left[\left(1-\frac{2}{n}\right)\left(\mathbf{V}(X_k)+[\mathbf{E}(X_k)]^2\right)+\left(\mathbf{V}(M_n)+[\mathbf{E}(M_n)]^2\right)-\frac{2}{n}\sum_{i\neq k}\mathbf{E}(X_k)\mathbf{E}(X_i)\right]$$
   $$= \left[\frac{n-2}{n}\left(pq+p^2\right)\right)+\left(\frac{1}{n}pq+p^2\right)-\frac{2(n-1)}{n}p^2\Big] = \frac{1}{n}\left((n-2)p+pq+np^2-2(n-1)p^2\right)$$
   $$= \frac{1}{n}\left((n-1)p-(n-1)p^2\right) = \frac{n-1}{n}pq = \frac{n-1}{n}V$$
   Donc V_n est un estimateur avec biais égal à $\mathbf{E}(V_n) - V = \dfrac{-1}{n}V$.
   $\forall\, \epsilon > 0$
   $$|V_n - V| > \epsilon = |V_n - \frac{n-1}{n}V + \frac{1}{n}V| > \epsilon \Longrightarrow |V_n - \mathbf{E}(V_n)| + \frac{1}{n}V > \epsilon$$
   $$\mathbf{P}(|V_n - V) > \epsilon) \leqslant \mathbf{P}(|V_n - \mathbf{E}(V_n)| > \epsilon - \frac{1}{n}V) \leqslant \frac{\mathbf{V}(V_n)}{(\epsilon - \frac{1}{n}V)^2}$$
   d'après l'inégalité de Bienaymé-Tchebychev : Il reste à calculer la variance de V_n, ce n'est pas aisé…
3. L'espérance étant linéaire, comme $W_n = \dfrac{n}{n-1}V_n$, on a donc $\mathbf{E}(W_n) = \dfrac{n}{n-1}\mathbf{E}(V_n) = V$.
   Donc W_n est-il un estimateur sans biais de V.

5. Théorème limite central

5.1. Rappels sur la loi normale

On a besoin de quelques rappels de terminale sur la loi normale : Lorsque $X(\Omega)$ est un intervalle de $\mathbb{R}$, nous devons penser autrement les lois de probabilité. On exploite les fonctions de répartition et non les lois ; la notion de densité devient alors importante.

Définition - Variable aléatoire à densité
Une variable aléatoire continue X est définie à partir d'une densité f vérifiant :
— $f : \mathbb{R} \to \mathbb{R}^+$
— f est continue par morceaux sur $\mathbb{R}$
— $\lim\limits_{x\to-\infty, y\to+\infty} \int_x^y f(t)\mathrm{d}t = 1$. Ce nombre est notée $\int_{-\infty}^{+\infty} f(t)\mathrm{d}t$.
On a alors
$$\mathbf{P}(X \leqslant x) = \int_{-\infty}^{x} f(t)\mathrm{d}t \qquad \mathbf{P}(X \in [a,b]) = \int_a^b f(t)\mathrm{d}t$$
Par ailleurs, si « les intégrales suivantes sont convergentes » (i.e. les limites existent) :
$$\mathbf{E}(X) = \int_{-\infty}^{+\infty} tf(t)\mathrm{d}t \qquad \mathbf{E}(\varphi(X)) = \int_{-\infty}^{+\infty} \varphi(t)f(t)\mathrm{d}t \qquad \mathbf{V}(X) = \mathbf{E}(X^2) - \mathbf{E}(X)^2$$

Exemple - Loi exponentielle
cf. Le cours de terminale
Un exemple classique de loi à densité :

Définition - Loi normale
Pour tout $\mu \in \mathbb{R}$, $\sigma^2 > 0$, la fonction

$$f_{\mu,\sigma^2} : t \mapsto \frac{1}{\sqrt{2\pi}} \exp(-\frac{(t-\mu)^2}{2\sigma^2}$$

est une fonction de densité.
On dit qu'une variable aléatoire X qui admet pour densité f_{μ,σ^2} suit une loi normale (ou gaussienne ou Laplace-Gauss).
On note $X \hookrightarrow \mathcal{N}(\mu, \sigma^2)$.
On a alors $\mathbf{E}(X) = \mu$ et $\mathbf{V}(X) = \sigma^2$

Remarque - Convergence en loi pour les variables à densité
Nous venons de l'écrire : pour des variables à densité, on exploite plus les lois mais les fonctions de répartitions.
La convergence en loi s'écrit donc autrement dans ce cas là

Définition - Convergence en loi
On suppose $X(\Omega$ et $X_n(\Omega) \subset \mathbb{R}$.
La suite (X_n) **converge en loi** vers X (à densité) si

$$\forall\ x \in \mathbb{R}, \quad \lim_{n\to+\infty} \mathbf{P}(X_n \leqslant x) = \mathbf{P}(X \leqslant x)$$

5.2. Enoncé

Il est très général, il est plus large que la loi des grands nombres mais ne donne une convergence « qu'en loi »

Proposition - Théorème central limite
Soit $(X_n)_{n\in\mathbb{N}^*}$ est une suite de variables aléatoires indépendantes et de même loi, admettant une espérance m et une variance σ^2 non nulle.
Notons $\overline{X_n} = \dfrac{X_1 + \cdots + X_n}{n}$ et $\overline{X_n}^* = \sqrt{n}\left(\dfrac{\overline{X_n} - m}{\sigma}\right)$, variable aléatoire centrée et réduite.
Alors $(\overline{X_n}^*)$ converge en loi vers une variable aléatoire suivant la loi normale centrée réduite.

$$X_n^* \xRightarrow{\mathcal{L}} \mathcal{N}(0;1)$$

Nous n'en ferons pas de démonstration. Il nous manque quelques outils…
Insistons : ce résultat est indépendant de la loi suivie par X_n !
On peut par contre l'appliquer afin d'obtenir :

Théorème - Théorème de De Moivre-Laplace
Soit $p \in]0,1[$ et S_n une suite de variables aléatoires telles que $S_n \hookrightarrow \mathcal{B}(n,p)$.
Alors pour tout réel x,

$$\mathbf{P}\left(\frac{S_n - np}{\sqrt{np(1-p)}} \leqslant x\right) \underset{n\to\infty}{\longrightarrow} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}}\,\mathrm{d}t$$

Démonstration
S_n est une somme de Bernoulli indépendante. On applique le théorème limite central. Notons $Z_n = \dfrac{S_n - np}{\sqrt{np(1-p)}}$.
Par linéarité $\mathbf{E}(Z_n) = \dfrac{1}{\sqrt{np(1-p)}}(\mathbf{E}(S_n) - np) = 0$ et $\mathbf{V}(Z_n) = \dfrac{1}{np(1-p)}\mathbf{V}(S_n) = 1$ Donc Z_n est une suite de va centrée réduite. Donc

$$Z_n \xRightarrow{\mathcal{L}} \mathcal{N}(0;1)$$

Pour des variables à densité, la convergence en loi ne s'exprime plus avec des lois de probabilités mais avec des densités.
□

5.3. Intervalle de confiance

Heuristique - Fluctuations autour d'une valeur estimée
L'estimateur théorique, basée ensuite sur des mesures, donne une estimation d'un paramètre $g(\theta)$. Mais parfois, on souhaite plutôt une connaissance des fluctuations autour de la valeur limite. La convergence en loi joue un peu ce rôle comparée à la convergence en probabilité.
On peut donc espérer élargir la notion d'estimateur à l'aide du théorème limite central ou le théorème de De Moivre-Laplace si l'on se concentre sur des variables de Bernoulli.
C'est la notion d'intervalle de confiance qui joue se rôle

On notera que l'intervalle de confiance est **une variable aléatoire**, c'est ce qui le différencie de l'intervalle de fluctuation (aux bornes fixées).
Le principe est le suivant :

Définition - Intervalle de confiance
Soit (X_n) une suite de variables aléatoires indépendants de même loi admettant un moment d'ordre 2. Notons $m = \mathbf{E}(X_1)$ et $\sigma^2 = \mathbf{V}(X_1)$.
$M_n = \dfrac{1}{n}\sum_{k=1}^{n} X_k$ est un estimateur de m.
Soit $\alpha > 0$, un risque. L'intervalle de confiance au risque α est défini comme

$$I_n(\omega) = \left[M_n - \frac{\epsilon\sigma}{\sqrt{n}}, M_n + \frac{\epsilon\sigma}{\sqrt{n}}\right]$$

où ϵ est définie par $\mathbf{P}(|N| > \epsilon) = \alpha$, avec $N \hookrightarrow \mathcal{N}(0;1)$

Remarque - ϵ ?
$\mathbf{P}(|N| > \epsilon = 1 - \int_{-\epsilon}^{\epsilon} n(t)\mathrm{d}t = 1 - 2\int_0^{\epsilon} n(t)\mathrm{d}t$, car n est paire.
Donc $\mathbf{P}(|N| > \epsilon) = \alpha \iff N(\epsilon) = \dfrac{1-\alpha}{2} \iff \epsilon = N^{-1}\left(\dfrac{1-\alpha}{2}\right)$
où N est la primitive de n, strictement croissante (car $n > 0$) et continue donc bijective

Proposition - Encadrement de m
Avec les hypothèses de la définition, on a

$$\mathbf{P}(m \in I_n) \underset{n\to\infty}{\longrightarrow} \int_{-\epsilon}^{+\epsilon} n(t)\mathrm{d}t = 1 - \alpha$$

Démonstration
On a applique le TLC (ou Moivre-Laplace dans le cas de Bernoulli).
On a donc, par convergence en loi :

$$\mathbf{P}(m \in I_n) = \mathbf{P}\left(m \in \left[M_n - \frac{\epsilon\sigma}{\sqrt{n}}, M_n + \frac{\epsilon\sigma}{\sqrt{n}}\right]\right) \underset{n\to\infty}{\longrightarrow} \int_{-\epsilon}^{+\epsilon} n(t)\mathrm{d}t = 1 - \alpha$$

□

Pour des exercices, voir le cours de terminale.

6. Bilan

Synthèse

⇝ La convergence simple des suites de fonctions (X_n) n'est pas satisfaisante (trop exigeante) pour l'étude des suites de variables aléatoires. Il suffit de se contenter de convergence sur des parties de Ω de mesure égale à 1, donc des convergence presque sûree. Voire une convergence en probabilité. Ces convergences ne sont pas sans lien.
On associe à ces convergences les convergentes fortes (p.s.) ou faibles (en $\mathbf{P}$). Par exemple les lois des grands nombres ou la convergence (faible) d'estimateurs..

⇝ On peut aussi s'intéresser aux lois des variables aléatoire et voir si ces fonctions convergent. Cela donne une convergence en loi, en réalité indépendante des variables d'une certaine façon. Une application classique est le théorème central limite dont une des conséquences est le théorème de Moivre-Laplace vu (trop rapidement) en terminale.

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Démontrer une convergence presque sûre
— Savoir-faire - Démontrer une convergence en probabilité

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$i.s.$	ω fixé. On a la propriété $\mathscr{P}(X_n(\omega))$ infiniment souvent si $\{n \in \mathbb{N} \mid \mathscr{P}(X_n(\omega))\}$ n'est pas borné	Equivalent à $\exists\, \varphi : \mathbb{N} \to \mathbb{N}$ ↗↗ tel $\forall\, n \in \mathbb{N}$, $\mathscr{P}(X_{\varphi(n)}(\omega))$	$\{\omega \mid \mathscr{P}(X_n(\omega)) \ i.s.\} = \bigcap_{n\in\mathbb{N}} \bigcup_{p\geqslant n} \{\omega \mid \mathscr{P}(X_n(\omega))\}$.
$(X_n) \xrightarrow{p.s.} X$	La suite de v.a. (X_n) converge presque sûrement vers X	$\mathbf{P}(\lim_{n\to+\infty} X_n = X) = 1$	
$(X_n) \xrightarrow{\mathbf{P}} X$	La suite de v.a. (X_n) converge en probabilité vers X	$\forall\, \epsilon > 0,\ \lim_{n\to+\infty} \mathbf{P}(\lvert X_n - X\rvert \geqslant \epsilon) = 0$	$(X_n) \xrightarrow{p.s.} X \Rightarrow (X_n) \xrightarrow{\mathbf{P}} X$. On exploite souvent l'inégalité de B.T.
$(X_n) \xrightarrow{\mathscr{L}} X$	La suite de v.a. (X_n) converge en loi vers X	(Cas au plus dénombrable) : $\forall\, x \in E$, $\lim_{n\to+\infty} \mathbf{P}(X_n = x) = \mathbf{P}(X = x)$	Utilisation pour l'approximation poissonnienne ou le TCL.

Retour sur les problèmes

A.18 Ici on a une convergence faible, comme un estimateur. C'est (au moins) la loi faible des grands nombres. Mais la loi forte peut également s'appliquer.

A.19 Gros morceau du cours hors-programme. Si les démonstrations ont échappées au lecteur, on espère au moins que les notions ont été comprises en profondeur!

A.20 Même réponse qu'à la question précédente.

Annexe B

Fonctions holomorphes

Résumé -

Dans ce complément hors-programme de CPGE, nous étudions les fonctions dérivables de la variable complexe. On qualifie ces fonctions d'holomorphes (« de forme entière »). Nous verrons d'abord que ces fonctions sont nombreuses (toutes nos fonctions usuelles sont holomorphes sur un ouvert plus ou moins grand) et qu'elles possèdent une certaine rigidité (conformes), cela leur donne des propriétés nouvelles : elles sont nécessairement analytiques et donc de classe $\mathscr{C}^\infty$, elles vérifient le principe harmonique…

Pour obtenir ces relations, nous exploiterons l'intégration sur un chemin complexe. Nous devons faire un détour par les intégrales curvilignes (et en bonus, le théorème de Green-Riemann). Nous serons armés avec les formules intégrales de Cauchy pour faire les démonstrations, dont le prolongement analytique (en gros : deux fonctions holomorphes sur un (petit) ouvert sont égales sur toute la composante connexe) et une méthode superpuissante pour calculer des intégrales immondes : le théorème de résidus.

Un chaîne youtube d'analyse complexe - https://www.youtube.com/playlist?list=PLErC88eFpes2gkbeh-RFAJqoQ5vYrwUBz

Sommaire

1. Problèmes 880
2. Holomorphie = Dérivation complexe 881
2.1. Fonctions holomorphes 881
2.2. Stabilité et premiers exemples 882
2.3. Condition de Cauchy-Riemann 883
2.4. Fonction analytique e(s)t fonction holomorphe . . . 884
3. Chemins dans le plan complexe et intégrale curviligne . . 885
3.1. Arc du plan 885
3.2. Intégration le long d'un chemin 886
3.3. Longueur d'une courbe et majoration 888
4. Théorème(s) de Cauchy 889
4.1. Indice de Cauchy 889
4.2. Lemme de Goursat et holomorphie 890
4.3. Petit détour : Formule de Green-Riemann 893
5. Théorème des résidus 894
5.1. Principe du théorème des résidus 894
5.2. Calculer les résidus 896
5.3. Applications (aux calculs d'intégrales immondes et sommes effrayantes) 896
6. Prolongement analytique 898

6.1. Zéros d'une fonction holomorphe 898
6.2. Prolongement analytique 899
6.3. Fonctions à singularités. Vers les surfaces de Riemann900
7. Bilan 901

1. Problèmes

? Problème A4 - Division par un nombre complexe et passage à la limite

Les fonctions de plusieurs ne sont pas dérivables car la division par un vecteur n'a pas de sens : $\dfrac{f(\vec{x}+\vec{h})-f(\vec{x})}{\vec{h}}$ ne signifie rien…

En revanche, la division par un nombre complexe a bien une signification. Que dire des fonctions $\mathbb{C}$-dérivable?

Et si on note $F(x,y)=f(x+iy)$, que signifie pour $\dfrac{\partial F}{\partial x}$ et $\dfrac{\partial F}{\partial y}$ le fait que $\dfrac{\partial f}{\partial z}$ existe?

? Problème A5 - Intégration complexe

Si la dérivation complexe semble avoir un sens facilement accessible : $\lim\limits_{|a|\to 0}\dfrac{f(z+a)-f(z)}{a}$, qu'en est-il de son opération réciproque.

Que signifie $\displaystyle\int_\Gamma f(z)\mathrm{d}z$ pour $f:\mathbb{U}\subset C\to\mathbb{C}$ et Γ, un chemin dans le plan complexe ou encore $\displaystyle\iint_K f(x+iy)\mathrm{d}x\mathrm{d}y$ pour K une partie de $\mathbb{C}$?

? Problème A6 - Théorème de D'Alembert-Gauss

Le corps $\mathbb{C}$ a été crée comme l'extension de $\mathbb{R}$ afin que tous les polynômes à coefficients entiers ou réels de degré n aient exactement n racines (certaines pouvant être multiples).

Comment démontrer ce résultat? Les fonctions holomorphes aident-elles pour faire cette démonstration?

? Problème A7 - Extension de ln

Pourquoi la fonction exp s'étend sans difficulté sur $\mathbb{C}$: $\exp(x+iy)=e^x(\cos y+i\sin y)$?

Et que se passe-t-il pour sa fonction réciproque $\ln z$? Est-elle bien définie, ou pourquoi ne l'est-elle pas?

Et à quoi « ressemble » la représentation graphique associée à ln?

? Problème A8 - Fonction Γ

La fonction $\Gamma:x\mapsto\displaystyle\int_0^{+\infty}t^{x-1}e^{-t}\mathrm{d}t$ est central en mathématiques. En particulier, elle interpole la factorielle (précisément : $\Gamma(n+1)=n!$), elle semble définie sur $\mathbb{R}_+^*$ entier où elle est de classe $\mathscr{C}^\infty$.

Peut-elle être prolongée sur $\mathbb{C}$, de manière unique?

Même question pour $\zeta : s \in \mathbb{R}$ ou $\mathbb{C} \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$?

2. Holomorphie = Dérivation complexe

2.1. Fonctions holomorphes

Remarque - Division par un nombre complexe : possible

Pour les fonctions de $\mathbb{R}^n \to \mathbb{R}^p$, il n'est pas possible d'étudier la limite $\frac{f(u+h)-f(u)}{h}$, pour h vecteur de $\mathbb{R}^n$ tendant vers 0. En effet, cela nécessiterait de donner un sens à la division par un vecteur.

En revanche, $\mathbb{C}$ étant un corps, il est possible d'effectuer $\frac{f(z_0+h)-f(z_0)}{h}$ et de regarder la limite pour $h \to 0 (\in \mathbb{C})$.

Définition - Fonctions holomorphes en un point (nombre complexe)

Soit $f : \mathbb{C} \to \mathbb{C}$, une fonction de la variable complexe (et à valeurs dans $\mathbb{C}$).
Soit U un ouvert de $\mathbb{C}$ (i.e. $\forall\, z \in U, \exists\, \rho > 0$ tel que $|z - z_0| < \rho \Rightarrow z \in U$.)
On dit que f est $\mathbb{C}$-dérivable ou (plutôt) holomorphe en $z_0 \in U$ si $\frac{f(z)-f(z_0)}{z-z_0}$ admet une limite (dans $\mathbb{C}$) pour $z \underset{z\in U}{\longrightarrow} z_0$.
Autrement écrit, on a les équivalences :

- f est holomorphe en z_0 de dérivée égale à $f'(z)$
- $\forall\, \epsilon > 0, \exists\, \rho > 0$ tel que $|z - z_0| < \rho \Longrightarrow \left| \frac{f(z)-f(z_0)}{z-z_0} - f'(z) \right| < \epsilon$.
- $\exists\, \epsilon : U \to \mathbb{C}$ tel que $\forall\, z \in U$, $f(z) = f(z_0) + f'(z) \times (z - z_0) + (z - z_0)\epsilon(z)$ avec $\epsilon(z) \underset{z\to z_0}{\longrightarrow} 0$.

Définition - Fonction holomorphe sur un ouvert

Soit $f : \mathbb{C} \to \mathbb{C}$, une fonction de la variable complexe (et à valeurs dans $\mathbb{C}$).
Soit U un ouvert de $\mathbb{C}$.
On dit que f est holomorphe sur U, si f est holomorphe en tout point z_0 de U.
On pourra noter $\mathscr{H}(U)$, l'ensemble des fonctions holomorphes définies sur l'ouvert U.

Pour aller plus loin - Connexe

Dans la pratique, il sera souvent nécessaire de nous restreindre à des ouverts qui sont connexes (parfois on se contentera de convexe).

Exemple - Fonction puissance entière

Soit $n \in \mathbb{N}$. On peut supposer $n \geqslant 2$ (sinon, c'est sans intérêt).
Pour $z \neq z_0 \in \mathbb{C}$:

$$\frac{z^n - z_0^n}{z - z_0} - n z_0^{n-1} = \sum_{k=0}^{n-1} z^k z_0^{n-1-k} - \sum_{k=0}^{n-1} z_0^{n-1} = \sum_{k=1}^{n-1} (z^k - z_0^k) z^{n-k-1}$$
$$= (z - z_0) \sum_{k=1}^{n-1} \sum_{h=0}^{k-1} z^h z_0^{k-h-1} z_0^{n-k-1} = (z - z_0) \sum_{h=0}^{n-2} (n-h-1) z^h z_0^{n-h-2}$$

car on peut commencer la somme à $k = 1$. Pour z suffisamment proche de z_0 (en module) i.e. $|z - z_0| < \eta$, donc $|z| < |z_0| + \eta$:

$$\left| \sum_{h=0}^{n-2} (n-h-1) z^h z_0^{n-h-2} \right| \leqslant (|z_0|+\eta)^{n-2} \sum_{h=0}^{n-2} (n-h-1) = (|z_0|+\eta)^{n-2} \sum_{j=1}^{n-1} j = \frac{n(n-1)}{2} |z_0+\eta|^{n-2}$$

Donc pour $|z - z_0| < \eta$

$$\left| \frac{z^n - z_0^n}{z - z_0} - n z_0^{n-1} \right| \leqslant \eta \frac{n(n-1)}{2} |z_0 + \eta|^{n-2} \underset{\eta \to 0}{\longrightarrow} 0$$

Ainsi $z \mapsto z^n$ est holomorphe sur $\mathbb{C}$ (entier) et sa dérivée est $z \mapsto n z^{n-1}$.

Exercice
Si $n \in \mathbb{Z}$ et $n < 0$, montrer que $f_n : z \mapsto z^n$ est également holomorphe sur $\mathbb{C} \setminus \{0\}$

Correction

On note $m = -n \in \mathbb{N}^*$. $f_n(z) - f_n(z_0) = \frac{1}{z^m} - \frac{1}{z_0^m} = \frac{-(f_m(z) - f_m(z_0))}{(zz0)^m}$. Donc

$$\frac{f_n(z) - f_n(z_0)}{z - z_0} = \frac{-1}{z^m z_0^m} \frac{f_m(z) - f_m(z_0)}{z - z_0} \underset{z\to z_0}{\longrightarrow} \frac{-1}{z_0^{2m}} f'_m(z_0) = \frac{-m z_0^{m-1}}{z_0^{2m}} = \frac{-m}{z_0^{m+1}} = n z_0^{n-1}$$

2.2. Stabilité et premiers exemples

Comme l'application de passage à la limite est linéaire, on retrouve les mêmes résultats que pour les fonctions dérivables (sur $\mathbb{R}$)

Proposition - Stabilité

Soit f et g holomorphe sur un ouvert U de $\mathbb{C}$. Alors :

- Pour tout $a, b \in \mathbb{C}$, $af + bg$ est holomorphe sur U et
  $\forall\, z \in U$, $(\lambda f + \mu g)'(z) = \lambda f'(z) + \mu g'(z)$.
- $f \times g$ est holomorphe sur U et
  $\forall\, z \in U$, $(f \times g)'(z) = f'(z)g(z) + f(z)g'(z)$.
- si g ne s'annule pas sur U, $\frac{f}{g}$ est holomorphe sur U et
  $\forall\, z \in U$, $\left(\frac{f}{g}\right)'(z) = \frac{f'(z)g(z) - f(z)g'(z)}{g^2(z)}$.

On démontre les deux premiers résultats

Démonstration
On suppose que f et g sont holomorphes sur U.
Soit $z_0 \in U$. Il existe $\epsilon_1, \epsilon_2 : U \to \mathbb{C}$ tel que $\forall\, z \in U$, $f(z) = f(z_0) + f'(z) \times (z - z_0) + (z - z_0)\epsilon_1(z)$ et $g(z) = g(z_0) + g'(z_0)(z - z_0) + (z - z_0)\epsilon_2(z)$ avec $\epsilon_1(z) \underset{z\to z_0}{\longrightarrow} 0$ et $\epsilon_2(z) \underset{z\to z_0}{\longrightarrow} 0$. Donc, pour $\lambda, \mu \in \mathbb{C}$:

$$(\lambda f + \mu g)(z) = \lambda f(z) + \mu g(z) = (\lambda f + \mu g)(z_0) + [\lambda f'(z_0) + \mu g'(z_0)](z - z_0) + (z - z_0) \times \epsilon_3(z)$$

où $\epsilon_3(z) = \lambda \epsilon_1(z) + \mu \epsilon_2(z) \underset{z\to z_0}{\longrightarrow} 0$ par addition.
Et selon le même principe :

$$(f \times g)(z) = f(z) \times g(z) = f(z_0)g(z_0) + (z - z_0)[f'(z_0)g(z_0) + f(z_0)g'(z_0)] + (z - z_0)\epsilon_4(z)$$

où $\epsilon_4(z) = \epsilon_1(z) \times g(z) + \epsilon_2(z) \times f(z) + (z - z_0) f'(z_0) g'(z_0) \underset{z\to z_0}{\longrightarrow} 0$ par addition. □

Exercice
Démontrer le dernier résultat

Correction
On rappelle qu'il est malin d'écrire : $f(z)g(z) - f(z_0)g(z_0) = f(z)(g(z) - g(z_0)) + (f(z) - f(z_0))g(z_0)\ldots$
Comme les puissances entières sont holomorphes, par combinaison linéaire :

Pour aller plus loin - Fonction analytique

On sait décrire parfaitement les fonctions holomorphes. Il s'agit des fonctions analytiques, i.e. des séries localement entière (ou polynôme de degré infini). Comme nous le verrons plus loin

Corollaire - Polynômes (et fractions rationnelles)

Les fonctions polynomiales : $p : z \mapsto \sum_{k=0}^{n} a_k z^k$ sont holomorphes sur $\mathbb{C}$ et

pour tout $z \in \mathbb{C}$, $p'(z) = \sum_{k=0}^{n} k a_k z^{k-1} = \sum_{k=1}^{n} k a_k z^{k-1} = \sum_{h=0}^{n-1} (h+1) a_{h+1} z^h$.

Les fractions rationnelles sont holomorphes sur tout ouvert de $\mathbb{C}$ ne contenant aucun pôle de la fraction.
La fonction dérivée associée est « comme on l'imagine ».

Une fonction holomorphe sur $\mathbb{C}$, en entier, est qualifiée de fonction entière.
Une fonction polynomiale est donc une fonction entière.

2.3. Condition de Cauchy-Riemann

Remarque - Bijection $\mathbb{C} \to \mathbb{R}^2$

Il existe un isomorphisme (canonique/ naturelle) entre $\mathbb{R}^2$ et $\mathbb{C} : (x,y) \mapsto x+iy$.
On peut donc considérer $F : \mathbb{R}^2 \to \mathbb{R}^2$, $(x,y) \mapsto \big(\underbrace{\mathrm{Re}(f(x+iy))}_{P(x,y)}; \underbrace{\mathrm{Im}(f(x+iy))}_{Q(x,y)}\big)$.

Est-ce équivalent de dire que f est holomorphe en $z_0 = x_0 + iy_0$ ou F est différentiable en (x_0, y_0) ?
On conserve, pour la suite, les notations de la remarque

Proposition - Condition de Cauchy-Riemann

f est holomorphe en z_0 ssi F est différentiable en (x_0, y_0) avec

$$\begin{cases} \dfrac{\partial P}{\partial x}(x_0,y_0) = \dfrac{\partial Q}{\partial y}(x_0,y_0) \\ \dfrac{\partial P}{\partial y}(x_0,y_0) = -\dfrac{\partial Q}{\partial x}(x_0,y_0) \end{cases}$$

Savoir faire - Montrer l'holomorphie (ou non) avec $H : \mathbb{R}^2 \to \mathbb{C}$, $(x,y) \mapsto f(x+iy)$

On notera l'équivalence entre le système de la proposition et :

$$\left[\frac{\partial P}{\partial x}(x,y) + i\frac{\partial Q}{\partial x}(x,y)\right] + i\left[\frac{\partial P}{\partial y}(x,y) + i\frac{\partial Q}{\partial y}(x,y)\right] = 0.$$

Ce qui est encore équivalent à $\dfrac{\partial H}{\partial x} + i\dfrac{\partial H}{\partial y} = 0_{\mathbb{C}}$, pour $H : (x,y) \mapsto f(x+iy)$ (i.e. $H : \mathbb{R}^2 \to \mathbb{C}$)

Démonstration

Si f est holomorphe, il existe $\epsilon : U \to \mathbb{C}$ tel que $\epsilon(z) \xrightarrow[z\to z_0]{} 0$, telle que $f(z) = f(z_0) + (z-z_0)f'(z) + (z-z_0)\epsilon(z)$.

$$\begin{aligned} P(x,y) - P(x_0,y_0) &= \mathrm{Re}\big(f(x+iy) - f(x_0+iy_0) + ((x-x_0)+i(y-y_0))\epsilon(x+iy)\big) \\ &= \mathrm{Re}\Big(\big((x-x_0)+i(y-y_0)\big)\times f'(x_0+iy_0) + ((x-x_0)+i(y-y_0))\epsilon(x+iy)\Big) \\ &= (x-x_0)\mathrm{Re}\big(f'(x_0+iy_0)\big) - (y-y_0)\mathrm{Im}\big(f'(x_0+iy_0)\big) + o(\|(x,y)\|) \\ Q(x,y) - Q(x_0,y_0) &= \mathrm{Im}\big(f(x+iy) - f(x_0+iy_0) + ((x-x_0)+i(y-y_0))\epsilon(x+iy)\big) \\ &= \mathrm{Im}\Big(\big((x-x_0)+i(y-y_0)\big)\times f'(x_0+iy_0) + ((x-x_0)+i(y-y_0))\epsilon(x+iy)\Big) \\ &= (x-x_0)\mathrm{Im}\big(f'(x_0+iy_0)\big) + (y-y_0)\mathrm{Re}\big(f'(x_0+iy_0)\big) + o(\|(x,y)\|) \end{aligned}$$

Donc F est différentiable en (x_0,y_0), avec $\dfrac{\partial P}{\partial x}(x_0,y_0) = \mathrm{Re}\big(f'(x_0+iy_0)\big) = \dfrac{\partial Q}{\partial y}(x_0,y_0)$.

mais aussi $\dfrac{\partial P}{\partial y}(x_0,y_0) = -\mathrm{Im}\big(f'(x_0+iy_0)\big) = -\dfrac{\partial Q}{\partial x}(x_0,y_0)$.

Réciproquement, on suppose que F est différentiable en (x_0,y_0) avec les relations de Cauchy-Riemann.

On note $A = \dfrac{\partial P}{\partial x}(x_0,y_0) + i\dfrac{\partial Q}{\partial x}(x_0,y_0) = \dfrac{\partial Q}{\partial y}(x_0,y_0) - i\dfrac{\partial P}{\partial y}(x_0,y_0)$.

Pour $z = x+iy$ proche de $z_0 = x_0+iy_0$,

$$\begin{aligned} f(z) - f(z_0) &= \big[F(x,y) - F(x_0,y_0)\big]_1 + i\big[F(x,y) - F(x_0,y_0)\big]_2 \\ &= \left[(x-x_0)\frac{\partial P}{\partial x}(x_0,y_0) + (y-y_0)\frac{\partial P}{\partial y}(x_0,y_0)\right] + i\left[(x-x_0)\frac{\partial Q}{\partial x}(x_0,y_0) + (y-y_0)\frac{\partial Q}{\partial y}(x_0,y_0)\right] \\ &\quad + ((x-x_0)+i(y-y_0))\epsilon(x+iy) \\ &= (x-x_0)\times A + i(y-y_0)\times A + ((x-x_0)+i(y-y_0))\epsilon(x+iy) = (z-z_0)\times A + (z-z_0)\epsilon(z) \end{aligned}$$

Donc f est holomorphe en z_0, avec $f'(z_0) = A$. □

Application - $z \mapsto e^z$ est holomorphe

Ici $H : (x,y) \mapsto e^x\cos y + ie^x \sin y$, différentiable sur $\mathbb{R}^2$.
Et $\dfrac{\partial H}{\partial x} + i\dfrac{\partial H}{\partial y} = (e^x\cos y + ie^x\sin y) + i(-e^x\sin y + ie^x\cos y) = 0$.
Donc $f : z \mapsto e^z$ est holomorphe sur $\mathbb{C}$.

Application - $z \mapsto \overline{z}$ n'est pas holomorphe

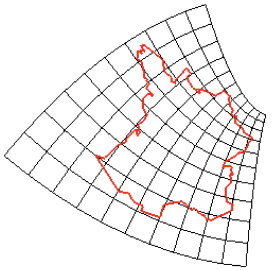
Même stratégie : ici $H : (x,y) \mapsto x - iy$, différentiable sur $\mathbb{R}^2$.
Et $\dfrac{\partial H}{\partial x} + i\dfrac{\partial H}{\partial y} = 1 + i(-i) = 2 \neq 0$.
Donc $f : z \mapsto \overline{z}$ n'est pas holomorphe sur $\mathbb{C}$

Heuristique - Du plan tangent à la similitude (locale)

Le fait que F soit différentiable nous dit, géométriquement, que P et Q sont comparables chacun à un plan au voisinage de tout (x_0,y_0), ou bien que P et Q admettent un plan tangent en (x_0,y_0).
Qu'ajoute l'information sur les relations de Cauchy-Riemann pour les fonctions holomorphes ?
Les vecteurs normaux au plan (∇P et ∇Q) sont orthogonaux : $\dfrac{\partial P}{\partial x}\dfrac{\partial Q}{\partial x} + \dfrac{\partial P}{\partial y}\dfrac{\partial Q}{\partial y} = 0$.
Ainsi la matrice jacobienne est une matrice orthogonale (à condition de la normalisée par la racine carrée de son déterminant) du plan, il s'agit donc d'une rotation.
Une fonction holomorphe est localement la composée d'une rotation et d'une homothétie (normalisation) : c'est une similitude.

Représentation - Application conforme

Une application conforme conserve les angles localement. L'image de la carte de la France par une application conforme donne quelque chose de reconnaissable.



Remarque - Application conforme

On a vu en début d'année, qu'une similitude conserve les angles ; i.e. si s est une similitude :

$$\big(\overrightarrow{s(A)s(B)}, \overrightarrow{s(C),s(D)}\big) = \arg\frac{s(d)-s(c)}{s(b)-s(a)} = \arg\frac{d-c}{b-a} = \big(\overrightarrow{AB}, \overrightarrow{C,D}\big)$$

on rappelle que $s : z \mapsto z_0 + re^{i\theta}(z-z_0)$. Donc les similitudes conservent les angles (souvent on prend $A = C$, ici). Une telle application est dite application conforme.
Une fonction holomorphe est donc (localement) une application conforme : elle conserve les formes des petites figures (mais pas les longueurs)

2.4. Fonction analytique e(s)t fonction holomorphe

Un mot sur les séries de fonctions (de référence)

Définition - Séries entières. Rayon de convergence

On appelle série entière les fonctions de la forme $S : z \in \mathbb{C} \mapsto \sum_{k=0}^{+\infty} a_n z^n$ où $(a_n) \in \mathbb{C}^{\mathbb{N}}$ est une suite de complexe.
On pose $R_S = \sup\{r \in \mathbb{R}_+ \mid (|a_n|r^n)_{n\in\mathbb{N}} \text{ bornée}\}$, appelé rayon de convergence de la série (entière).

On énonce une série de propriétés pour les séries entières, elles seront démontrées en seconde année.

Proposition - Régularité d'une série entière

La fonction $S_{\mathbb{R}}$ est définie, continue et de classe $\mathscr{C}^\infty$ sur le « disque » ouvert $]-R,R[$. On a alors

$$\forall\, n \in \mathbb{N},\ \forall\, x \in]-R,R[,\ S^{(n)}(x) = \sum_{k=n}^{+\infty} \frac{k!}{(k-n)!} a_k x^{k-n} = \sum_{h=0}^{+\infty} \frac{(h+n)!}{h!} a_{h+n} x^h.$$

Heuristique - Idées de démonstration

1. D'abord, notons que pour $|x| > R$ la série diverge grossièrement. $\mathscr{D}_{S_{\mathbb{R}}} \subset [-R,R]$.
Si $|x| < R$, alors avec $\rho \in]|x|,R[$, on a $|a_n x^n| \leqslant a_n \rho^n \times \left|\frac{|x|}{\rho}\right|^n \leqslant M\left|\frac{|x|}{\rho}\right|^n$. Et la série entière est **normalement** convergente. Tout se passera bien : continuité, dérivabilité… Ce qui se passe en R et $-R$ dépend de chaque série considérée. On peut tout avoir.
2. On calcule la dérivée, comme limite de la série des dérivées. C'est une nouvelle série entière.
3. On trouver pour $S'_{\mathbb{R}}$, le même rayon de convergence (petite manipulation).
Et on continue ainsi pour toutes les dérivées !

De la même façon, on a le théorème suivant (qui ne sera pas démontré…) :

Proposition - Série entière et fonctions holomorphes
La fonction S est définie, continue, holomorphe et de classe $\mathscr{C}^\infty$ (dérivation complexe) sur le disque ouvert $\mathscr{D}(0,R_S)=\{z\in\mathbb{C}\mid |z|<R_S\}$. Alors

$$\forall\, n\in\mathbb{N},\ \forall\, z\in\mathscr{D}(0,R_S),\ S^{(n)}(z)=\sum_{k=n}^{+\infty}\frac{k!}{(k-n)!}a_k z^{k-n}=\sum_{h=0}^{+\infty}\frac{(h+n)!}{h!}a_{h+n}z^h.$$

Définition - Fonction analytique
On dit que $f:U\subset\mathbb{C}\to\mathbb{C}$ est analytique sur l'ouvert U si
pour tout $z_0\in U$, il existe $R>0$ et $(a_n)\in\mathbb{C}^{\mathbb{N}}$ tel que :

$$\forall\, z\in\mathscr{D}(z_0,R),\qquad f(z)=\sum_{n=0}^{+\infty}a_n(z-z_0)^n$$

(Il s'agit du disque ouvert de $\mathbb{C}$ centré en z_0 et de rayon R.
Si f est analytique sur U, alors f est holomorphe sur U

On reviendra en fin de chapitre sur les propriétés analytiques (prolongement…) des fonctions holomorphes. C'est l'un des pierres précieuses des fonctions holomorphes. En attendant, mais sans pouvoir faire démonstration, on énonce le théorème suivant, dont la connaissance est importante à ce stade du chapitre :

Théorème - Holomorphie et analycité
Si f est holomorphe sur un ouvert U, alors f est analytique sur U.
Ainsi, pour tout $z_0\in U$, il existe $R>0$ et (a_n) tel que $\forall\, z\in\mathscr{D}(z_0,R)$, $f(z)=\sum_{n=0}^{+\infty}a_n(z-z_0)^n$.
Et on a, pour tout $r\in]0,R[$:

$$a_n=\frac{1}{2r^{n+1}i\pi}\int_0^{2\pi}f(z_0+re^{i\theta})e^{-i(n+1)\theta}\mathrm{d}\theta=\frac{1}{2i\pi}\oint_{\mathscr{C}(z_0,r)}\frac{f(z)}{(z-z_0)^{n+1}}\mathrm{d}z$$

Attention - Dépendance des (a_n) par rapport à z_0
On rappelle que chaque z_0 définit un rayon distinct et une suite (a_n) propre.
On aurait du noter $(a_n(z_0))_n$.

3. Chemins dans le plan complexe et intégrale curviligne

3.1. Arc du plan

On commence par beaucoup de vocabulaire dont le sens géométrique ne devrait pas échapper au lecteur.

Définition - Arc du plan complexe ou chemin
Soit $[a,b]$ un compact de $\mathbb{R}$ et $\gamma:[a,b]\to\mathbb{C}$, **continue**.
L'image du compact $[a,b]$ de $\mathbb{R}$ par γ est appelé arc de $\mathbb{C}$, noté Γ, γ est alors appelé (une) paramétrisation de Γ.
On dit que l'arc est fermé si $\gamma(a)=\gamma(b)$.
On dit que l'arc est simple si γ est injectif (i.e. $\gamma(t)\neq\gamma(s)$ dès que $s\neq t\in]a,b[$).

Si γ est de classe $\mathscr{C}^1$, on dit que γ est un chemin. Un chemin fermé est parfois qualifié de lacet.

Pour aller plus loin - Chemins continument différentiable
Pour les chemins, le cours devrait se limiter aux applications γ dérivables par morceaux.
Nous simplifions ici le cours en ne prenant que des chemins de classe $\mathscr{C}^1$. En revanche, nous couperons nos intégrales curvilignes en morceaux si l'on rencontre des coupures naturelles de chemin

Attention - Tolérance
Parfois on appelle chemin, à la fois la paramétrisation de la courbe et sa représentation géométrique.
Le contexte est en règle générale suffisant pour faire la distinction.
Mais cette tolérance peut créer une confusion pour le débutant; on essayera de bien s'en garder.

Remarque - Interprétation des contions γ de classe $\mathscr{C}^1$ et $\gamma'(t)\neq 0$
La paramétrisation γ s'appelle parfois le mobile (comme un point mobile qui se déplace). A chaque instant t il laisse sa trace sur la courbe. Le fait que γ soit dérivable signifie que le mobile a une vitesse. $\gamma'(t)\neq 0$ signifie qu'elle ne s'annule pas et comme le déplacement du mobile est continue, cela implique qu'il ne revient pas en arrière.

Exemple - Paramétrisation du cercle unité
L'application : $[0,2\pi]\to\mathbb{C}$, $t\mapsto e^{it}$ est une paramétrisation de l'arc : cercle unité.
Une autre, associée au compact $[0,1]$ est $t\mapsto e^{2i\pi t}$.

Proposition - Paramétrisation à partir de $[0,1]$
Soit Γ un chemin de $\mathbb{C}$.
Alors il existe une paramétrisation γ de Γ, à partir du compact $[0,1]$.

Démonstration
Considérons une paramétrisation $\gamma_1:[a,b]\to\mathbb{C}$ de Γ.
Considérons $\varphi:[0,1]\to[a,b]$, $t\mapsto a+(b-a)t$, alors $\gamma:t\mapsto\gamma_1\circ\varphi$ est une paramétrisation de Γ à partir du compact $[0,1]$ □

Définition - Chemins équivalents
Soient $\gamma_1:[a,b]\to\mathbb{C}$ et $\gamma_2:[c,d]\to\mathbb{C}$ deux chemins.
Si il existe une bijection $\varphi:[a,b]\to[c,d]$, de classe $\mathscr{C}^1$ et croissante telle que $\gamma_1=\gamma_2\circ\varphi$, alors on dit que les chemins sont équivalents.
Il s'agit d'une relation d'équivalence.

Exercice
intégrale curviligne

Correction
Fiche de TD

3.2. Intégration le long d'un chemin

Analyse - Intégration d'une fonction holomorphe le long d'un chemin dans $\mathbb{C}$
Comment définir $\int_\Gamma f(z)\mathrm{d}z$?
Si on exploite la même idée que pour les sommes de Riemann, on se trouve en présence de $\sum_{k=0}^{n}f(u_k)(y_{k-1}-y_k)$ où $\tau_p=\left(([y_{k-1},y_k],u_k),k\in\mathbb{N}_n\right)$ est une subdivision pointée de Γ.
Or la seule chose qu'on peut dire des points x_k et t_k de Γ, c'est qu'ils sont des images par le paramétrage γ du compact $[a,b]$.
Ainsi, en simplifiant à la condition que le paramétrage soit croissant, il existe une subdivision pointée $\sigma_p=\left(([x_{k-1},x_k],t_k),k\in\mathbb{N}_n\right)$ de $[a,b]$ telle que $\gamma(\sigma_p)=\tau_p$, i.e. $y_k=\gamma(x_k)$ et $u_k=\gamma(t_k)$.
On a donc (en exploitant l'égalité des accroissements finis) :

$$\int_\Gamma f(z)\mathrm{d}z=\lim_{\sigma_p\to 0}\sum_{k=1}^{n}f(\gamma(t_k))(\gamma(x_k)-\gamma(x_{k-1})\lim_{\sigma_p\to 0}\sum_{k=1}^{n}f(\gamma(t_k))\gamma'(c_k)(x_k-x_{k-1})=\int_a^b f(\gamma)\times\gamma'$$

La définition suivante, reste vraie pour des fonctions f non nécessairement holomorphe.

Définition - Intégration curviligne le long d'un chemin
Soit U un ouvert de $\mathbb{C}$. Soient $f : U \to \mathbb{C}$ et $\gamma : [a,b] \to U$, un chemin.
On définit l'intégrale de g sur le chemin Γ :

$$\int_\Gamma g(z)\mathrm{d}z = \int_a^b g(\gamma(t))\gamma'(t)\mathrm{d}t$$

Le résultat ne dépend pas du choix du paramétrage γ du chemin Γ.

Le résultat qui suit sera très souvent exploité !

Application - $\oint_{\mathbb{U}} z^n\mathrm{d}z$, pour $n \in \mathbb{Z}$
On note $\mathbb{U}$ le cercle trigonométrique dont une paramétrisation est $\gamma : [0,1] \to \mathbb{C}$, $t \mapsto e^{2i\pi t}$.
On a alors, pour tout entier $n \in \mathbb{Z}$:

$$\oint_{\mathbb{U}} z^n\mathrm{d}z = \int_0^1 \left(e^{2i\pi t}\right)^n \times (2i\pi)e^{2i\pi t}\mathrm{d}t = 2i\pi\int_0^1 e^{2i\pi(n+1)t}\mathrm{d}t$$

Si $n+1 \neq 0$ i.e. $n \neq -1$:

$$\oint_{\mathbb{U}} z^n\mathrm{d}z = \left[\frac{1}{n+1}e^{2i\pi(n+1)t}\right]_0^1 = \frac{1}{n+1}[1-1] = 0$$

Si $n+1 = 0$ i.e. $n = 0$:

$$\oint_{\mathbb{U}} z^n\mathrm{d}z = 2i\pi\int_0^1 \mathrm{d}t = 2i\pi$$

Reste à démontrer l'indépendance du choix du paramétrage.

Démonstration
Soient γ_1 et γ_2 deux paramétrages de Γ.
Alors il existe une bijection $\varphi : [c,d] \to [a,b]$ de classe $\mathscr{C}^1$ tel que $\gamma_2 = \gamma_1 \circ \varphi$.
On a alors $\gamma_2' = \varphi' \times \gamma_1' \circ \varphi$ et donc

$$\int_c^d f(\gamma_2(t))\gamma_2'(t)\mathrm{d}t = \int_c^d f(\gamma_1(\varphi(t))\gamma_1'(\varphi(t))\varphi'(t)\mathrm{d}t = \int_a^b f(\gamma_1(s))\gamma_1'(s)\mathrm{d}s$$

en faisant le changement de variable $s = \varphi(t)$ dans le calcul intégral. □

Proposition - Intégrale curviligne d'une dérivée
Soit f une fonction holomorphe sur U et $\gamma : [a,b] \to U$, un chemin.
Alors $\displaystyle\int_\Gamma f'(z)\mathrm{d}z = f(\gamma(b)) - f(\gamma(a))$.

Démonstration
On fait le calcul

$$\int_\Gamma f'(z)\mathrm{d}z = \int_a^b f'(\gamma(t)) \times \gamma'(t)\mathrm{d}t = \left[f(\gamma(t))\right]_a^b = f(\gamma(b)) - f(\gamma(a))$$

□

Corollaire - Intégrale d'une dérivée sur un chemin fermé
Si Γ est un chemin fermé et que f est la dérivée d'une fonction holomorphe, alors $\oint_\Gamma f = 0$.

Savoir faire - Démontrer qu'une fonction n'est pas la dérivée d'une fonction holomorphe
Si l'intégrale d'une fonction f sur un chemin fermé n'est pas nulle, alors, elle ne peut être la dérivée d'une fonction holomorphe.

Exemple - z^{-1}
Pour tout $n \in \mathbb{Z} \setminus \{-1\}$, $z \mapsto z^n$ est la dérivée d'une fonction holomorphe : $z \mapsto \dfrac{1}{n+1}z^{n+1}$.
En revanche, ce n'est pas le cas de $z \mapsto \frac{1}{z} = z^{-1}$.

Exercice

Après l'intégration, plusieurs ont eu en colle : calculer $\displaystyle\int_0^\pi \ln(a^2 - 2a\cos t + 1)\mathrm{d}t$.

Voici une nouvelle question : interpréter en terme de intégrale curviligne le calcul

Correction

Pour aller plus loin - Invariance et homotopie (marge)
Une homotopie est une déformation continue entre deux applications, notamment entre les chemins à extrémités fixées et en particulier les lacets. Cette notion topologique permet de définir des invariants algébriques utilisés pour classifier les applications continues entre espaces topologiques dans le cadre de la topologie algébrique.

3.3. Longueur d'une courbe et majoration

Analyse - Longueur d'un chemin dans $\mathbb{C}$
Considérons le chemin Γ paramétré par γ, définie sur $[a,b]$.
On note ℓ la longueur de Γ que l'on aimerait calculer.
Soit $\sigma = (x_k)_{k\in[\![0,n]\!]}$, une subdivision de $[a,b]$.
La longueur de Γ entre les points $M_{k-1} = \gamma(x_{k-1})$ et $M_k = \gamma(x_k)$ peut être approchée par $\|M_{k-1}M_k\| = |z_k - z_{k-1}| = |\gamma(x_k) - \gamma(x_{k-1})|$.
D'après l'inégalité des accroissements finis :

$$\sum_{k=1}^n \inf_{[x_{k-1},x_k]} |\gamma'|(x_k - x_{k-1}) \leqslant \sum_{k=1}^n |\gamma(x_k) - \gamma(x_{k-1})| \leqslant \sum_{k=1}^n \sup_{[x_{k-1},x_k]} |\gamma'|(x_k - x_{k-1})$$

On reconnait des sommes de Darboux, elles convergent (quand tout va bien) vers $\displaystyle\int_a^b |\gamma'(x)|\mathrm{d}x$.

Proposition - Longueur d'un chemin de $\mathbb{C}$
La longueur d'un chemin Γ de $\mathbb{C}$ paramétré par γ (de classe $\mathscr{C}^1$) est donné par

$$\ell(\Gamma) = \int_a^b |\gamma'(t)|\mathrm{d}t$$

indépendant du choix de γ.

Application - Périmètre d'une ellipse
Soient $a, b > 0$. La chemin $z : t \mapsto a\cos t + i\sin t$ décrit une ellipse, pour $t \in [0, 2\pi]$.
Sa longueur (périmétre) est

$$\ell = \int_0^{2\pi} |-a\sin t + ib\cos t|\mathrm{d}t = \int_0^{2\pi} \sqrt{a^2\sin^2 t + b^2\cos^2 t}\mathrm{d}t = b\int_0^{2\pi} \sqrt{1 + e^2\sin^2 t}\mathrm{d}t$$

où $e = \dfrac{\sqrt{a^2-b^2}}{b}$. Et on ne sait pas faire plus...

Proposition - Inégalité des accroissements finis
Soit Γ un chemin paramétré par γ de classe $\mathscr{C}^1$.
Alors, pour toute fonction f holomorphe sur U contenant Γ,

$$\left|\int_\Gamma f(z)\mathrm{d}z\right| \leqslant \sup_\Gamma |f| \times \ell(\Gamma)$$

Démonstration
Le calcul donne :

$$\left|\int_\Gamma f(z)\mathrm{d}z\right| = \left|\int_a^b f(\gamma(t))\gamma'(t)\mathrm{d}t\right| \leqslant \sup_\Gamma |f| \int_a^b |\gamma'(t)|\mathrm{d}t = \sup_\Gamma |f| \times \ell(\Gamma)$$

□

4. Théorème(s) de Cauchy

4.1. Indice de Cauchy

Définition - Indice (de Cauchy) d'un chemin par rapport à un point z_0
Soient Γ un chemin fermé de $\mathbb{C}$, de paramétrisation γ.
On note U, le complémentaire de Γ dans $\mathbb{C}$. Soit $z_0 \in \mathbb{C}$.
On appelle indice de Γ (ou Γ) par rapport à z_0, le nombre.

$$\mathrm{Ind}_\Gamma(z_0) = \frac{1}{2i\pi}\oint_\Gamma \frac{\mathrm{d}z}{z-z_0}$$

Remarque - Autre nom
On parle parfois de l'indice de z_0 par rapport à Γ (ou γ).

Exemple - $\Gamma = \mathbb{U}$, le cercle unité et $z_0 \in \mathbb{C}$
Si $z_0 = 0$, $\mathrm{Ind}_\Gamma(z_0) = \frac{1}{2i\pi}\int_0^{2\pi} \frac{ie^{i\theta}}{e^{i\theta}-0}\mathrm{d}\theta = 1$.
Si $z_0 = \frac{1}{2}$,

$$\begin{aligned}
\mathrm{Ind}_\Gamma(z_0) &= \frac{1}{2i\pi}\int_0^{2\pi} \frac{ie^{i\theta}}{e^{i\theta}-\frac{1}{2}}\mathrm{d}\theta \\
&= \frac{1}{\pi}\int_0^{2\pi} \frac{e^{i\theta}}{2e^{i\theta}-1}\mathrm{d}\theta = \frac{1}{\pi}\int_0^{2\pi} \frac{e^{i\theta}(2e^{-i\theta}-1)}{5-4\cos\theta}\mathrm{d}\theta = \frac{1}{\pi}\int_0^{2\pi} \frac{2-e^{i\theta}}{5-4\cos\theta}\mathrm{d}\theta \\
&= \frac{1}{2\pi}\int_0^{\pi} \frac{2-\cos\theta}{5-4\cos\theta}\mathrm{d}\theta - \frac{i}{\pi}\int_0^{2\pi} \frac{\sin\theta}{5-4\cos\theta}\mathrm{d}\theta \qquad t=\tan\frac{\theta}{2} \\
&= \frac{1}{2\pi}\int_0^{+\infty} \frac{1+3t^2}{(1+9t^2)(1+t^2)}\mathrm{d}t - \frac{i}{4}\left[\ln(5-4\cos(\theta))\right]_0^{2\pi} \\
&= \frac{1}{2\pi}\int_0^{+\infty} \frac{1}{1+t^2} + \frac{3}{1+9t^2}\mathrm{d}t = \frac{1}{2\pi}\left[\arctan t + \arctan 3t\right]_0^{+\infty} = 1
\end{aligned}$$

Si $z_0 = 2$,

$$\begin{aligned}
\mathrm{Ind}_\Gamma(z_0) &= \frac{1}{2i\pi}\int_0^{2\pi} \frac{ie^{i\theta}}{e^{i\theta}-2}\mathrm{d}\theta = \frac{1}{2\pi}\int_0^{2\pi} \frac{e^{i\theta}(e^{-i\theta}-2)}{5-4\cos\theta}\mathrm{d}\theta = \frac{1}{2\pi}\int_0^{2\pi} \frac{1-2e^{i\theta}}{5-4\cos\theta}\mathrm{d}\theta \\
&= \frac{1}{2\pi}\int_0^{\pi} \frac{1-2\cos\theta}{5-4\cos\theta}\mathrm{d}\theta - \frac{i}{\pi}\int_0^{2\pi} \frac{\sin\theta}{5-4\cos\theta}\mathrm{d}\theta \qquad t=\tan\frac{\theta}{2} \\
&= \frac{1}{2\pi}\int_0^{+\infty} \frac{-1+3t^2}{(1+9t^2)(1+t^2)}\mathrm{d}t - \frac{i}{4}\left[\ln(5-4\cos(\theta))\right]_0^{2\pi} \\
&= \frac{1}{4\pi}\int_0^{+\infty} \frac{1}{1+t^2} - \frac{3}{1+9t^2}\mathrm{d}t = \frac{1}{4\pi}\left[\arctan t - \arctan 3t\right]_0^{+\infty} = 0
\end{aligned}$$

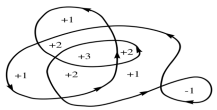
Avec les mêmes notations

Proposition - Valeur de l'indice
$\mathrm{Ind}_\Gamma(z_0)$ est à valeurs entières et constant sur chaque composante connexe de U et il est nul sur la composante connexe non bornée de U.

Démonstration
• $\mathrm{Ind}_\Gamma(z_0)$ est à valeurs entières.
Notons $\gamma : [a,b] \to \mathbb{C}$ une paramétrisation de Γ de classe $\mathscr{C}^1$, donc $\mathrm{Ind}_\Gamma(z) = \frac{1}{2i\pi}\int_a^b \frac{\gamma'(t)}{\gamma(t)-z}\mathrm{d}t$.
Considérons, pour $z \in U$ ($z \notin \Gamma$), $\varphi_z : u \mapsto \exp\left(\int_a^u \frac{\gamma'(t)}{\gamma(t)-z}\mathrm{d}t\right)$.
Par composition φ_z est dérivable sur $[a,b]$ et

$$\varphi_z'(u) = \frac{\gamma'(u)}{\gamma(u)-z}\varphi_z(u)$$

Représentation - Indice d'un point
Il s'agit du nombre de tour que la boucle effectue autour d'un point.
Cela est géométriquement facilement visible, même sans calcul :



La fonction $\Psi_z : t \mapsto \frac{\varphi_z(t)}{\gamma(t)-z}$ est dérivable également et

$$\Psi_z'(t) = \frac{\varphi_z'(t)(\gamma(t)-z) - \varphi_z(t)\gamma'(t)}{(\gamma(t)-z)^2} = 0$$

Donc Ψ est constante sur $[a,b]$. Or $\Psi(a) = \frac{\varphi_z(0)}{\gamma(0)-z} = \exp(0) = 1$, donc pour tout $t \in [a,b]$:

$$\Psi_z(t) = 1 = \frac{\varphi_z(t)}{\gamma(t)-z}$$

Ainsi $\varphi_z(t) = \gamma(t) - z$. Et donc $\varphi_z(b) = \gamma(b) - z = \gamma(a) - z = \varphi_z(a) = 1$.
Donc $\exp(2i\pi\mathrm{Ind}_\Gamma(z)) = 1$ donc $\mathrm{Ind}_\Gamma(z) \in \mathbb{Z}$.
• $\mathrm{Ind}_\Gamma(z_0)$ est constante sur les composantes connexes.

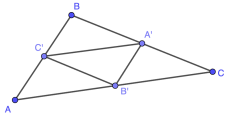
$$z \mapsto \int_a^b \frac{\gamma'(t)}{\gamma(t)-z}\mathrm{d}t = \sum_{k=0}^{+\infty}\left(\int_a^b \frac{\gamma'(t)}{\gamma^{n+1}(t)}\right)z^k$$

Donc Ind_Γ est fonction analytique, donc holomorphe donc continue.
Une fonction continue sur une partie connexe a une image connexe (T.V.I.). Mais comme Ind_Γ est à valeurs dans un ensemble à valeurs séparées, nécessairement Ind_Γ est constante sur chaque composante connexe.
• Sur la composante non bornée.
Si z est suffisamment grand, $\mathrm{Ind}_\Gamma(z)$ est un entier de valeurs absolues strictement plus petite que 1.
Donc $\mathrm{Ind}_\Gamma(z) = 0$. □

4.2. Lemme de Goursat et holomorphie

Proposition - Lemme de Goursat
Soit Δ un triangle (fermé) de U ouvert de C. Soit f une fonction holomorphe sur U.
Alors $\oint_\Delta f(z)\mathrm{d}z = 0$

Représentation - Décomposition du triangle



Démonstration
On note A, B, C les trois sommets du triangle (plein!!) $\Delta = [A \to B \to C \to A]$.
On note respectivement A', B' et C' les milieux de $[BC]$, $[AC]$ et $[AB]$ (cf figure dans la marge).
On note $\Delta_1 = [A \to C' \to B' \to A]$, $\Delta_2 = [C' \to B \to A' \to C']$, $\Delta_3 = [A' \to C \to B' \to A']$ et enfin $\Delta_4 = [C' \to A' \to B' \to C']$.
Par relation de Chasles (dans $\mathbb{R}$, avec le paramétrage) :

$$\begin{aligned}
&\oint_{\Delta_1} f(z)\mathrm{d}z + \oint_{\Delta_2} f(z)\mathrm{d}z + \oint_{\Delta_3} f(z)\mathrm{d}z = \left(\int_{A\to C'} f(z)\mathrm{d}z + \int_{C'\to B'} f(z)\mathrm{d}z + \int_{B'\to A} f(z)\mathrm{d}z\right) + \cdots \\
&= \left(\int_{A\to C'} f(z)\mathrm{d}z + \int_{C'\to B} f(z)\mathrm{d}z + \int_{B\to A'} f(z)\mathrm{d}z + \int_{A'\to C} f(z)\mathrm{d}z + \int_{C\to B'} f(z)\mathrm{d}z + \int_{B'\to A} f(z)\mathrm{d}z\right) \\
&\quad - \left(\int_{C'\to A'} f(z)\mathrm{d}z + \int_{A'\to B'} f(z)\mathrm{d}z + \int_{B'\to C'} f(z)\mathrm{d}z\right) \\
&= \oint_\Delta f(z)\mathrm{d}z - \oint_{\Delta_4} f(z)\mathrm{d}z
\end{aligned}$$

Supposons, par l'absurde que $\oint_\Delta f(z)\mathrm{d}z \neq 0$, donc $C := \left|\oint_\Delta f(z)\mathrm{d}z\right| > 0$ On a alors

$$C := \left|\oint_{\Delta_1} f(z)\mathrm{d}z + \oint_{\Delta_2} f(z)\mathrm{d}z + \oint_{\Delta_3} f(z)\mathrm{d}z + \oint_{-\Delta_4} f(z)\mathrm{d}z\right| > 0$$

Par inégalité triangulaire :

$$0 < C \leqslant \left|\oint_{\Delta_1} f(z)\mathrm{d}z\right| + \left|\oint_{\Delta_2} f(z)\mathrm{d}z\right| + \left|\oint_{\Delta_3} f(z)\mathrm{d}z\right| + \left|\oint_{-\Delta_4} f(z)\mathrm{d}z\right|$$

Notons $C' = \max\left|\oint_{\Delta_i} f(z)\mathrm{d}z\right|$, on a donc $C \leqslant 4C'$.
Donc il existe i tel que $\left|\oint_{\Delta_i} f(z)\mathrm{d}z\right| > \frac{C}{4}$.
On continue ainsi, en coupant Δ_i en 4 morceaux comme précédemment, et ainsi, par récurrence, on crée une suite $(T_i)_{i\in\mathbb{N}}$, de triangles emboités tels que :

$$\text{pour tout } n \in \mathbb{N}, \left|\oint_{T_n} f(z)\mathrm{d}z\right| > \frac{C}{4^n} \text{ et également } \ell(T_n) = \frac{1}{2}\ell(T_{n-1}) = \frac{\ell(\Delta)}{2^n}.$$

En réalité, chaque T_n, triangle plein est un compact de $\mathbb{C}$.
On a une suite emboitée de compact de $\mathbb{C}$, donc son intersection est un fermé non vide.
La longueur de ces compacts tend vers 0 donc (T_n) converge vers un unique point a.
f est holomorphe en a. Donc, pour tout $\epsilon > 0$,

il existe V voisinage de a, tel que : $\forall\, z\in V, |f(z)-f(a)-f'(a)\times(z-a)|\leqslant\epsilon|z-a|$.
Or, il existe n tel que $T_n\subset V$, et donc

$$\left|\oint_{T_n} f(z)\mathrm{d}z - f(a)\oint_{T_n}\mathrm{d}z + f'(a)\oint_{T_n}(z-a)\mathrm{d}z\right|\leqslant\epsilon\oint_{T_n}|z-a|\mathrm{d}z\leqslant\epsilon\sup_{T_n}|z-a|\times\ell(T_n)$$

Et comme $f(a)\oint_{T_n}\mathrm{d}z = f'(a)\oint_{T_n}(z-a)\mathrm{d}z = 0$, on a :

$$\left|\oint_{T_n} f(z)\mathrm{d}z\right|\leqslant\epsilon\ell(T_n)^2=\frac{\epsilon\ell^2(\Delta)}{2^{2n}}$$

Ainsi, pour tout $\epsilon>0$

$$0\leqslant C<4^n\times\epsilon\frac{\ell^2(D_n)}{4^n}=\epsilon\ell^2(\Delta)$$

Donc $C=0$. □

Remarque - Allégement des hypothèses

En fait, on peut considérer que f est holomorphe sur $U\setminus\{p\}$ où p est un point quelconque de Δ.
Mais la démonstration est plus compliquée.

Proposition - Dérivabilité

Soit U un ouvert, étoilé (i.e. : $\exists\, A\in U$ tel que $\forall\, M\in U$, $[AM]\subset U$.
On suppose que f est holomorphe sur U, alors f admet une primitive sur U.

Démonstration

Considérons le point $A(a)$ à l'origine de l'étoile incluse dans U.
Notons, pour tout $z\in U$ (z affixe du point M),

$$F : z\mapsto\int_{[AM(z)]} f(u)\mathrm{d}u=\int_0^1(z-a)\times f\big(a+t(z-a)\big)\mathrm{d}t$$

car $\gamma:[0,1]\to U$, $t\mapsto(1-t)a+tz=z_0+(z-a)t$ est une paramétrisation de $[AM]$.
Fixons $z_0\in U$ et z, au voisinage de z_0, inclus dans U (ouvert).

$$\begin{aligned}F(z)-F(z_0)=&\int_{[AM(z)]}f(u)\mathrm{d}u-\int_{[AM_0(z_0)]}f(u)\mathrm{d}u=\int_{[AM(z)]}f(u)\mathrm{d}u+\int_{[M_0(z_0)A]}f(u)\mathrm{d}u\\ =&-\int_{[M(z)M_0(z_0)]}f(u)\mathrm{d}u=\int_{[M_0M]}f(u)\mathrm{d}u=\int_0^1(z-z_0)\times f\big(z_0+t(z-z_0)\big)\mathrm{d}t\end{aligned}$$

puisque, comme f est holomorphe : $\oint_{[AMM_0A]}f(\tau)\mathrm{d}\tau=0$.
Donc :

$$\frac{F(z)-F(z_0)}{z-z_0}-f(z_0)=\int_0^1\big(f(z_0+t(z-z_0))-f(z_0)\big)\mathrm{d}t$$

Puis f continue au voisinage de z_0.
Soit $\epsilon>0$. Il existe V, voisinage de z_0, tel que $\forall\, u\in V$, $|f(u)-f(z_0)|\leqslant\epsilon$.
Puis, pour tout $z\in V$, $\forall\, t\in[0,1]$, $|z_0+t(z-z_0)-z_0|\leqslant|z-z_0|$, donc $u:=z_0+t(z-z_0)-z_0\in V$.
Ainsi :

$$\left|\frac{F(z)-F(z_0)}{z-z_0}-f(z_0)\right|\leqslant\int_0^1\epsilon\mathrm{d}t=\epsilon$$

Ainsi F est une primitive de f. □

On a le corollaire suivant, puisque $f=F'$:

Théorème - Première formule de Cauchy

Si U est un ouvert étoile, ou donc un ouvert convexe voire un ouvert simplement connexe. Si f est holomorphe sur U et Γ est un chemin fermé ou lacet de U :

$$\oint_\Gamma f(z)\mathrm{d}z=0$$

Remarque - Hypothèses du théorème

Sur les points de non-holomorphie de f (dont on parlera plus loin), le théorème indique qu'il n'y a aucun point singulier de f à l'intérieur de Γ.

Pour aller plus loin - Fonction harmonique

Les applications qui vérifie la propriété de la moyenne sur la boule sont des fonctions harmoniques (vérifiant également $\Delta f=0$ (lire Laplacien de f)). Elles sont très importantes en physique où elles sont associées à tout type de phénomènes ondulatoires.

Théorème - Formule intégrale de Cauchy

Soit f une fonction holomorphe sur un ouvert U simplement connexe.
Soit $z_0\in U$ et Γ un chemin fermé ne contenant pas z_0. Alors

$$f(z_0)\times\mathrm{Ind}_\Gamma(z_0)=\frac{1}{2i\pi}\oint_\Gamma\frac{f(z)}{z-z_0}\mathrm{d}z$$

Démonstration

On considère $g:z\mapsto\begin{cases}\frac{f(z)-f(z_0)}{z-z_0} & \text{si } z\neq z_0\\ f'(z_0) & \text{si } z=z_0\end{cases}$ définie sur U.
Alors g est continue et holomorphe sur $U\setminus\{z_0\}$ (au moins).
On a donc

$$0=\oint_\Gamma g(z)\mathrm{d}z=\int_\Gamma\frac{f(z)}{z-z_0}\mathrm{d}z-f(z_0)\oint_\Gamma\frac{\mathrm{d}z}{z-z_0}$$

En multipliant par $2i\pi$, on reconnait l'indice de z_0 par rapport à Γ. □

Application - Interprétation nouvelle de $\int_0^{2\pi}f(z_0+re^{i\theta})\mathrm{d}\theta$

Notons $\Gamma=\{z=z_0+re^{i\theta},\theta\in[0,2\pi]\}$, $\gamma:\theta\mapsto z_0+re^{i\theta}$.
Γ est un chemin fermé, γ en est un paramétrage.
Donc, pour tout f holomorphe sur U, ouvert contenant Γ,

$$f(z_0)\mathrm{Ind}_\Gamma(z_0)=\frac{1}{2i\pi}\oint_\Gamma\frac{f(z)}{z-z_0}\mathrm{d}z=\frac{1}{2i\pi}\int_0^{2\pi}\frac{f(\gamma(\theta))\times ire^{i\theta}\mathrm{d}\theta}{re^{i\theta}}=\frac{i}{2i\pi}\int_0^{2\pi}f(z_0+re^{i\theta})\mathrm{d}\theta$$

Donc $\int_0^{2\pi}f(z_0+re^{i\theta})\mathrm{d}\theta=2\pi\mathrm{Ind}_\Gamma(z_0)\times f(z_0)$ Mais, compte-tenu de la définition de Γ (cercle de centre z_0) : l'indice $\mathrm{Ind}_\Gamma(z_0)=\frac{1}{2i\pi}\int_0^{2\pi}\frac{rie^{i\theta}\mathrm{d}\theta}{re^{i\theta}}=\frac{1}{2\pi}$.
Donc $\int_0^{2\pi}f(z_0+re^{i\theta})\mathrm{d}\theta=f(z_0)$

Analyse - Accès à $f^{(n)}(z_0)$

Si on veut avoir accès à la valeur de $f^{(n)}(z_0)$, on peut avoir intérêt à calculer

$$\oint_\Gamma\frac{f^{(n)}(z)}{z-z_0}\mathrm{d}z$$

On aurait envie de faire une intégration par parties : en intégrant $f^{(n)}$ et dérivant $\frac{1}{(z-z_0)}$ et en effet :

$$\oint_\Gamma\frac{f^{(n)}(z)}{z-z_0}\mathrm{d}z=\oint_\Gamma\frac{f^{(n-1)}(z)}{(z-z_0)^2}\mathrm{d}z=\cdots=\oint_\Gamma\frac{n!\times f(z)}{(z-z_0)^{n+1}}\mathrm{d}z$$

Pour les crochet, comme l'intégrale est sur un contour fermé, ils sont tous nuls. On retrouve une partie d'un résultat énoncé plus haut. Il faudrait ajouter que cela permet de voir comme une fonction analytique.

Théorème - Formule intégrale de Cauchy d'ordre n

Soient f est holomorphe sur U, et $z_0\in U$.
Soit $r>0$, tel que $\Gamma=\{z_0+re^{i\theta},\theta\in[0,2\pi[\}\subset U$, alors f est infiniment dérivable en z_0 et

$$\forall\, n\in\mathbb{N},\qquad f^{(n)}(z_0)=\frac{n!}{2\pi}\oint_\Gamma\frac{f(z)}{(z-z_0)^{n+1}}\mathrm{d}z=\frac{n!}{2r^n\pi}\int_0^{2\pi}f(z_0+re^{i\theta})e^{-in\theta}\mathrm{d}\theta$$

Démonstration
Pour faire cette démonstration, considérons $a_n = \frac{n!}{2\pi}\oint_\Gamma \frac{f(u)}{(u-z_0)^{n+1}}\mathrm{d}u$.

Puis notons $g : z \mapsto \sum_{n=0}^{+\infty} a_n (z-z_0)^n$.

Soit z, à l'intérieur de Γ, i.e. $|z-z_0| < r$. On a alors pour tout $u \in \Gamma$ et $\rho := \frac{z-z_0}{u-z_0}$, $|\rho| < \frac{|z-z_0|}{r} < 1$.

Ainsi la série géométrique $\sum_{n\geq 0} \frac{1}{u-z_0}\rho^n$ converge vers $\frac{1}{u-z_0}\times\frac{1}{1-\rho} = \frac{1}{u-z}$.

Cette convergence est uniforme en u, donc on peut (théorème de seconde année) intervertir série et intégrale :

$$f(z_0) = \frac{1}{2i\pi}\oint_\Gamma \frac{f(u)}{u-z_0}\mathrm{d}u = \frac{1}{2i\pi}\oint_\Gamma \sum_{n=0}^{+\infty}\frac{(z-z_0)^n f(u)}{(u-z_0)^{n+1}}\mathrm{d}u = \frac{1}{2i\pi}\sum_{n=0}^{+\infty}(z-z_0)^n\oint_\Gamma\frac{f(u)}{(u-z_0)^{n+1}}\mathrm{d}u = \sum_{n=0}^{+\infty}\frac{a_n}{n!}(z-z_0)^n = g(z_0)$$

La fonction g est une série entière donc de classe $\mathscr{C}^\infty$ sur son disque de convergence.
g, donc f est de classe $\mathscr{C}^\infty$, puis on sait que le DSE de g est unique et donne $a_n = g^{(n)}(z_0) = f^{(n)}(z_0)$.
□

4.3. Petit détour : Formule de Green-Riemann

Voici un théorème qui sort du cadre des fonctions holomorphes, mais il permet d'avoir une nouvelle vision sur le théorème de Cauchy. Il fait aussi le lien avec le calcul vectoriel dont on abuse en physique en seconde année…
La force du théorème suivant : il permet de passer à des intégrales sur une surfaces (flux) à une intégrale sur le bord (circulation)…

Théorème - Théorème de Green-Riemann
Soient $P, Q : \mathbb{R}^2 \to \mathbb{C}$ des fonction $\mathbb{R}^2$-différentiables et K un compact suffisamment régulier, de frontière Γ. Alors

$$\oint_\Gamma (P\mathrm{d}x + Q\mathrm{d}y) = \iint_K \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right)\mathrm{d}x\mathrm{d}y$$

.

Pour aller plus loin - Théorème de Stokes
La formule de Stokes est le nom générique donné à toutes les formules du type $\int_\Omega \mathrm{d}\omega = \int_{\partial\Omega}\omega$ *qui dit que l'intégrale sur une surface est égale à la différence de la variation d'une certaine primitive.*
C'est le cas de la formule de Newton, ou des plus fameuses formule de Stokes ou formule d'Ostrogradski vu en cours de physique de spé.

Remarque - Explication des termes
L'intégrable double, de droite, est une intégrale d'une variable du plan. On peut l'interpréter simplement en deux intégrations selon les deux variables x et y qui la composent (c'est ce qui est fait pour la pseudo-démonstration). Mais cela est trop restrictif (cf le calcul de flux en physique).
L'intégrable de droite et une double intégrale curviligne, on regarde en fonction de x et de y, séparément.
Il s'agit plus d'un éclairage que d'une démonstration. Par exemple le compact considéré sera considéré sans trou et avec une frontière biunivoque (à chaque y, correspond deux et seulement deux x sur Γ ; de même pour chaque x - excepté les quatre points de rebroussement).

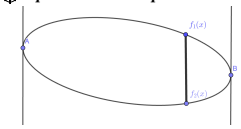
Démonstration
On se place donc sur la figure de la marge.
On peut couper les deux intégrales en deux : $\oint_\Gamma P\mathrm{d}x = \iint_K -\frac{\partial P}{\partial y}\mathrm{d}x\mathrm{d}y$ et $\oint_\Gamma Q\mathrm{d}y = \iint_K \frac{\partial Q}{\partial x}\mathrm{d}x\mathrm{d}y$.
Pour la première, on prend les notations de la figure.

$$\begin{aligned}\iint_K -\frac{\partial P}{\partial y}\mathrm{d}x\mathrm{d}y &= -\int_a^b\left(\int_{f_2(x)}^{f_1(x)}\frac{\partial P}{\partial y}\mathrm{d}y\right)\mathrm{d}x = -\int_a^b P(x,f_1(x)) - P(x,f_2(x))\mathrm{d}x\\ &= \int_a^b P(x,f_2(x))\mathrm{d}x - \int_a^b P(x,f_2(x))\mathrm{d}x = \int_{[AB]_2} P\mathrm{d}x + \int_{[BA]_1} P\mathrm{d}x = \oint_\Gamma P\mathrm{d}x\end{aligned}$$

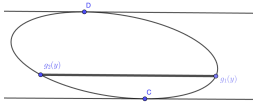
$$\begin{aligned}\iint_K \frac{\partial Q}{\partial x}\mathrm{d}x\mathrm{d}y &= -\int_c^d\left(\int_{g_2(y)}^{g_1(y)}\frac{\partial Q}{\partial x}\mathrm{d}x\right)\mathrm{d}y = \int_c^d Q(g_1(y),y) - Q(g_2(y),y)\mathrm{d}y\\ &= \int_c^d Q(y,g_1(y))\mathrm{d}y - \int_c^d Q(g_2(y),y)\mathrm{d}y = \int_{[CD]_1} Q\mathrm{d}y + \int_{[DC]_2} Q\mathrm{d}y = \oint_\Gamma Q\mathrm{d}y\end{aligned}$$

□

Représentation - Représentation de K



Intégration $\mathrm{d}x$



Intégration $\mathrm{d}y$

Application - (Première) formule de Cauchy
Soit f une fonction holomorphe sur U.

Soient P et Q tel que $P(x,y) = \mathrm{Re}(f(x+iy))$ et $Q(x,y) = \mathrm{Im}(f(x+iy))$.
Les formules de Cauchy-Riemann donne $\frac{\partial P}{\partial x} = \frac{\partial Q}{\partial y}$ et $\frac{\partial Q}{\partial x} = -\frac{\partial P}{\partial y}$.
Soit Γ, la frontière d'un compact K de U (donc Γ est un chemin fermé) et γ un paramétrage de Γ définit sur $[a,b]$. Supposons que $\gamma(t) = x(t) + iy(t)$, donc $\gamma'(t) = x(t) + iy(t)$

$$\begin{aligned}\oint_\Gamma f(z)\mathrm{d}z &= \int_a^b f(\gamma(t))\gamma'(t)\mathrm{d}t = \int_a^b (P(x(t),y(t)) + iQ(x(t),y(t)))(x'(t)+iy'(t))\mathrm{d}t\\ &= \int_a^b P(x(t),y(t))x'(t)\mathrm{d}t - Q(x(t),y(t))y'(t)\mathrm{d}t\\ &\qquad + i\int_a^b P(x(t),y(t))y'(t)\mathrm{d}t + Q(x(t),y(t))y'(t)\mathrm{d}t\\ &= \oint_\Gamma P\mathrm{d}x - Q\mathrm{d}y + i\oint_\Gamma Q\mathrm{d}x + P\mathrm{d}y\\ &= \iint_K -\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\mathrm{d}x\mathrm{d}y + i\iint_K \frac{\partial P}{\partial x} - \frac{\partial Q}{\partial y}\mathrm{d}x\mathrm{d}y = \iint_K 0\mathrm{d}x\mathrm{d}y\end{aligned}$$

d'après les relations de Cauchy-Riemann, puisque f est holomorphe sur K.

Remarque - Interprétation et formule d'Ampère
Peut-être avez-vous rencontré le théorème d'Ampère : $\oint_{\mathscr{C}} \vec{H}\mathrm{d}\vec{\ell} = \iint_S \vec{j}\mathrm{d}\vec{S}$ ou sa version différentielle $\vec{\mathrm{rot}}\vec{H} = \vec{\nabla}\wedge\vec{H}$.
Le premier terme s'appelle la circulation du champ vectoriel $\vec{H}$ sur le contour $\mathscr{C}$. Il s'agit d'une l'intégrale d'un produit scalaire, donc du type $(P,Q)\cdot(\mathrm{d}x,\mathrm{d}y)$, ce qui donne le premier terme de la formule de Green-Riemman.
On a alors pour le second terme un produit vectoriel (dimension 3) ou un déterminant (dimension 2) : $\begin{vmatrix}\frac{\partial}{\partial x} & P\\ \frac{\partial}{\partial y} & Q\end{vmatrix} = \frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}$ pour l'intégration sur une surface (appelé un flux, par les physiciens.

5. Théorème des résidus

5.1. Principe du théorème des résidus

Heuristique - Une idée pour calculer $\int_\Gamma f(z)\mathrm{d}z$, directement
Si on reprend la formule précédente, on voit que pour $n \in \mathbb{N}$, la valeur de $\frac{n!}{2\pi}\oint_\Gamma \frac{f(z)}{(z-z_0)^{n+1}}\mathrm{d}z$, donne accès à $f^{(n)}(z_0)$.
Et par ailleurs, ce nombre $f^{(n)}(z_0)$, ce trouve dans le développement de Taylor (série entière) $f(z) = \sum_{k=0}^{+\infty}\frac{f^{(k)}(z_0)}{k!}(z-z_0)^k$.
Mais, ce que l'on rencontre souvent c'est plutôt : $\int_\Gamma f(z)\mathrm{d}z$, comme si $n=-1$, dans le calcul précédent.
N'aurait-on pas : $\int_\Gamma f(z)\mathrm{d}z = \mathrm{Ind}_\Gamma(z_0) f^{(-1)}(z_0)$?

Pour aller plus loin - Développement de Laurent
Le développement considéré ici s'appelle le développement de Laurent, il s'étend normalement sur un ouvert u de U contenant z_0, f étant holomorphe sur $u\setminus\{z\}$.

Définition - Résidu de f en z_0
On appelle résidu de f au point z_0 de $\mathbb{C}$, noté $\mathrm{Res}(f,z_0)$, le coefficient devant $(z-z_0)^{-1}$ dans le développement asymptotique de f au voisinage de z_0.

Exemple - Fraction $F(z) = \frac{z^2+z-1}{z^4-z^3-z+1}$
Comme $z^4-z^3-z+1 = (z^2+z+1)(z^2-2z+1)$, cette fraction admet trois pôles, deux sont simples : j et j^2 et un est double : 1.
On a la décomposition en éléments simples

$$F(z) = \frac{j^2+j-1}{j^3-3j^2-j} = \frac{c}{z-j} + \frac{\overline{c}}{z-j^2} + \frac{a}{z-1} + \frac{b}{(z-1)^2} = \frac{j-1}{3(z-j)} + \frac{j^2-1}{3(z-j^2)} - \frac{1}{z-1} + \frac{1}{3(z-1)^2}$$

car $c = \frac{j^2+j-1}{j^3-3j^2-j} = \frac{-2}{2-2j^2} = \frac{1}{j^2-1} = \frac{j-1}{3}$, $b = \frac{1+1-1}{1+1+1} = \frac{1}{3}$ et $a+c+\overline{c} = \lim_{z\to+\infty} zf(z) = 0$, donc $a = -\frac{1}{3}$.

On a donc pour tout $z \notin \{1, j, j^2\}$, $\mathrm{Res}(f,z) = 0$, $\mathrm{Res}(f,j) = \frac{j-1}{3}$, $\mathrm{Res}(f,j^2) = \frac{j^2-1}{3}$, et $\mathrm{Res}(f,1) = \frac{-1}{3}$. En effet :

$$\begin{aligned} F(z) &= \frac{1}{3(z-1)^2} - \frac{1}{3(z-1)} + \frac{j-1}{3j}\sum_{k=0}^{+\infty}\left(\frac{z}{j}\right)^k + \frac{j^2-1}{3j^2}\sum_{k=0}^{+\infty}\left(\frac{z}{j^2}\right)^k \\ &= \frac{1}{3(z-1)^2} - \frac{1}{3(z-1)} + \sum_{h=0}^{+\infty} b_h (z-1)^h \end{aligned}$$

Heuristique - Extension : des polynômes aux fractions rationnelles. Des séries entières, au séries de Laurent.

En première partie, nous avons vu que les fonctions holomorphes sont la bonne façon de voir les séries entières, extension degré infini des polynômes.
Or les polynômes connaissent une autre extension intéressante (anneau→corps) : les fractions rationnelles, avec la notion de pôles et de degré négatif. Les séries de Laurent sont localement (autour des pôles ou des points normaux) les extensions naturelles de fractions rationnelles. Il est important que les pôles soient isolés.
Quant aux fonctions holomorphes avec des pôles, elles sont appelées : fonctions méromorphes. Les pôles sont isolés.

Théorème - Résidus

Soit f une fonction holomorphe sur U, un ouvert étoilé, présentant des singularités en des points isolés de $S = \{s_1, \dots s_m\} \subset U$.
Soit Γ un chemin fermé tracé dans U, ne rencontrant pas S. Alors

$$\int_\Gamma f(z)\mathrm{d}z = 2i\pi \sum_{i=1}^{m} \mathrm{Ind}_\Gamma(s_i) \times \mathrm{Res}(f, s_i)$$

Ce théorème a de multiples applications que nous verrons plus loin.
Plutôt qu'une démonstration complète, nous nous contenterons d'un dessin animé commenté…

Démonstration

En notant, pour tout $n \in \mathbb{N}^*$ et $i \in \mathbb{N}_m$, $\Gamma_i^n = \mathscr{C}(s_i, \frac{1}{n})$, le cercle centré en s_i de rayon $\frac{1}{n}$, tournant dans le sens inverse de Γ, ainsi que $[A_i B_i^n]$, le segment joignant Γ à Γ_i^n.
Enfin, on considère le chemin

$$\Gamma^n = [A_1 \to B_1^n \to \Gamma_i^n \to B_1^n \to A_1] \underset{\text{sur }\Gamma}{\to} [A_2 \to B_2^n \to \Gamma_i^n \to B_2^n \to A_2]$$

$$\underset{\text{sur }\Gamma}{\to} \cdots \underset{\text{sur }\Gamma}{\to} [A_m \to B_m^n \to \Gamma_i^n \to B_m^n \to A_m] \underset{\text{sur }\Gamma}{\to} [A_1]$$

A l'intérieur de ce chemin, f n'a pas de singularité, donc son intégrale est nulle : $\oint_{\Gamma^n} f(z)\mathrm{d}z = 0$.

Or on peut recoller l'intégrale et comme sur les chemins $\int_{A_i B_i^n} f(z)\mathrm{d}z + \int_{B_i^n A_i} f(z)\mathrm{d}z = 0$, on trouve

$$0 = \int_{\Gamma^n} f(z)\mathrm{d}z = \int_\Gamma f(z)\mathrm{d}z + \sum_{i=1}^{m} \oint_{\Gamma_i^n} f(z)\mathrm{d}z$$

$$\oint_\Gamma f(z)\mathrm{d}z = \sum_{i=1}^{m} \oint_{-\Gamma_i^n} f(z)\mathrm{d}z$$

Pour tout $\epsilon > 0$, pour n suffisamment grand (i.e. Γ_i^n proche de s_i), en remplaçant f par son développement analytique local :

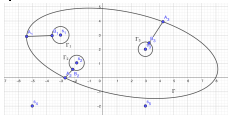
$$\left| \oint_\Gamma f(z)\mathrm{d}z - \sum_{i=1}^{m} \oint_{-\Gamma_i^n} \sum_{h=-\infty}^{+\infty} a_h(s_i)(z-s_i)^h \mathrm{d}z \right| = \left| \oint_\Gamma f(z)\mathrm{d}z - \sum_{i=1}^{m} (2i\pi)\mathrm{Ind}_{-\Gamma_i^n}(s_i) \times a_{-1}(s_i) \right| \leqslant \epsilon$$

Ainsi, en passant à la limite sur n : $\oint_\Gamma f(z)\mathrm{d}z = \sum_{i=1}^{m} 2i\pi \mathrm{Ind}_{-\Gamma_i^n}(s_i) \times a_{-1}(s_i)$ Il faut donc tourner dans le même sens entre Γ et Γ_i.
Notons ici que la démonstration sous-entend un seul tour Γ, mais elle s'adapte à plusieurs tours… □

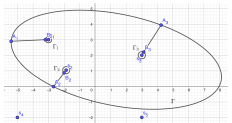
Pour aller plus loin - Zéros isolés

Nous verrons plus loin (classification des zéros) que si f n'est pas nulle, alors ses zéros sont isolés et au plus dénombrables.
On reviendra sur ce résultat profond d'analycité avec le théorème de prolongement analytique.

Représentation - Théorème des résidus



Décomposition de Γ, sans singularité.



Avec $n \to +\infty$.

Pour aller plus loin - Calculer des sommes par les résidus

On peut aussi exploiter le théorème des résidus pour évaluer quelques sommes du type $\sum_{n\in\mathbb{Z}\setminus S} f(n)$ ou $\sum_{n\in\mathbb{Z}\setminus S} (-1)^n f(n)$. Voir la page Théorème des résidus de Wikipedia.

5.2. Calculer les résidus

On admet :

Proposition - Linéarité du résidu

Si f et g sont méromorphes et $\lambda, \mu \in \mathbb{C}$,
$\mathrm{Res}(\lambda f + \mu g, a) = \lambda \mathrm{Res}(f,a) + \mu \mathrm{Res}(g,a)$.

La méthode du calcul connue pour les pôles de fractions s'adaptent aux fonctions holomorphes plus compliquées :

Savoir faire - Calculer les résidus de f en a

Plusieurs méthode :

1. On exploite un développement asymptotique de f au voisinage de a.
2. Si f a en a un pôle d'ordre 1 : $\mathrm{Res}(f,a) = \lim_{z\to a}(z-a)f(z)$.
3. Si f a en a un pôle d'ordre n : $\mathrm{Res}(f,a) = \frac{1}{(n-1)!}\lim_{z\to a}\frac{\partial^{n-1}}{\partial z^{n-1}}\left((z-a)^n f(z)\right)$.
4. Si h possède en a une racine d'ordre 1 : $\mathrm{Res}\left(\frac{g}{h}, a\right) = \frac{g(a)}{h'(a)}$.

Remarque - Explication du second résultat

Supposons que $f(z) = \sum_{k=1}^{n} \frac{\alpha_k}{(z-a)^k} + g(z)$ où a n'est pas pôle de g. On cherche α_1.
En multipliant par $(z-a)^n$, on trouve :

$$(z-a)^n f(z) = \sum_{k=1}^{n} \alpha_k (z-a)^{n-k} + (z-a)^n g(z) \text{ puis}$$

$$\frac{\partial^{n-1}}{\partial z^{n-1}}\left((z-a)^n f(z)\right) = (n-1)!\alpha_1 + 0 + \cdots + 0 + \sum_{k=0}^{n-1}\binom{n-1}{k}\frac{n!}{(n-k)!}(z-a)^{n-k} g^{(n-k)}(z).$$

Exercice

Que vaut $\mathrm{Res}\left(\frac{\cos t}{t}, 0\right)$?

Correction

$\frac{\cos t}{t} = \frac{1}{t} - \frac{t}{2} + \frac{t^3}{24} + \dots$ Donc $\mathrm{Res}\left(\frac{\cos t}{t}, 0\right) = 1$.

5.3. Applications (aux calculs d'intégrales immondes et sommes effrayantes)

Le principe est (presque) toujours le même : on prolonge l'intégrande en une fonction holomorphe sur une partie $\mathbb{C}$. Puis on calcul ses résidus.

Savoir faire - Intégrale de premier type

Il s'agit de calculer $I = \int_0^{2\pi} R(\cos t, \sin t)\mathrm{d}t$ où R est une fraction rationnelle ayant un nombre fini de pôle : s_j et donc aucun n'appartient à $\mathbb{U} = \mathscr{C}(0,1)$, le cercle unité.
Alors $I = 2i\pi \sum_{|s_j|<1} \mathrm{Res}(f, s_z)$ où $f(z) = \frac{1}{iz} R\left(\frac{z+z^{-1}}{2}, \frac{z-z^{-1}}{2i}\right)$.

Exemple - $\int_0^{2\pi} \frac{\mathrm{d}x}{a+\sin x}$ avec $a > 1$.

La fonction $R : (x,y) \mapsto \frac{1}{a+y}$, on a bien l'intégrande qui est $t \mapsto R(\cos t, \sin t)$.

Posons z de tel sorte que t vérifie $z = e^{it} = \gamma(t)$, donc $\cos t = \frac{z+z^{-1}}{2}$ et $\sin t = \frac{z-z^{-1}}{2i}$ et $\gamma'(t) = i\gamma(t) = iz$. $f(z) = \frac{1}{iz} R\left(\frac{z+z^{-1}}{2}, \frac{z-z^{-1}}{2i}\right) = \frac{1}{iz}\frac{1}{a+\frac{z-z^{-1}}{2i}} = \frac{2}{z^2+2iaz-1}$ et

$$\int_0^{2\pi} \frac{\mathrm{d}x}{a+\sin x} = \oint_\Gamma f(z)\mathrm{d}z = 2i\pi \sum_{s\in S} \mathrm{Ind}_\Gamma(s)\mathrm{Res}(f,s)$$

Or $z^2+2iaz-1=(z+ia)^2+(a^2-1)=(z+ia-i\sqrt{a^2-1})(z+ia+i\sqrt{a^2-1})$.
Les pôles sont donc $i(-a-\sqrt{a^2-1})$ de module $a+\sqrt{a^2-1}>1$,
$i(-a+\sqrt{a^2-1})$ de module $a-\sqrt{a^2-1}\in]0,1]$ car $a>1$. La fonction f ne présente qu'une singularité dans $\mathbb{U}$ en $i(-a+\sqrt{a^2-1})$ (l'autre point à un indice nul).
Le cercle $\Gamma=\mathbb{U}$ fait un tour autour de ce point donc $\mathrm{Ind}_\Gamma(i(-a+\sqrt{a^2-1}))=1$.
Puis $\mathrm{Res}(f,i(-a+\sqrt{a^2-1}))=\left[(z+ia-i\sqrt{a^2-1})f(z)\right]_{\cdot}^{i(-a+\sqrt{a^2-1})}=\dfrac{1}{i\sqrt{a^2-1}}$.
Donc

$$\int_0^{2\pi}\frac{\mathrm{d}x}{a+\sin x}=\oint_\Gamma f(z)\mathrm{d}z=2i\pi\times 1\times\frac{1}{i\sqrt{a^2-1}}=-\frac{2\pi}{\sqrt{a^2-1}}$$

Savoir faire - Intégrale de deuxième type

Il s'agit de calculer $I=\displaystyle\int_{-\infty}^{+\infty}f(x)\mathrm{d}x$.
On suppose que cette intégrale est convergente, ce qui impose nécessairement que $zf(z)\underset{|z|\to\infty}{\longrightarrow}0$.
En considérant le « demi-cercle » de diamètre l'axe des réels et la partie positive (resp. négative), on trouve :

$$I=2i\pi\sum_{\mathrm{Im}(s_j)>0}\mathrm{Res}(f,s_z)=-2i\pi\sum_{\mathrm{Im}(s_j)<0}\mathrm{Res}(f,s_z).$$

Exemple - $\displaystyle\int_{-\infty}^{+\infty}\frac{\mathrm{d}x}{x^2+a^2}$ **avec** $a>0$**.**

L'idée est de ne pas exploiter arctan.
On considère Γ_r, le demi-cercle de centre 0, de rayon r de partie imaginaire positive.
Un paramètrage de Γ_r est par exemple $\gamma_r:[0,\pi+2]\to\mathbb{C}$ tel que $\gamma_r(t)=re^{it}$ si $t\in[0,\pi]$, puis $\gamma_r(t)=-r+(t-\pi)r$ sur $[\pi,\pi+2]$.
$f:z\mapsto\dfrac{1}{z^2+a^2}=\dfrac{1}{2ia(z-ia)}-\dfrac{1}{2ia(z+ia)}$. Si $r>a$, f admet un seul pôle dans Γ_r : le point ia.
On a alors $\mathrm{Ind}_{\Gamma_r}(ia)=1$ et $\mathrm{Res}(f,ia)=\dfrac{1}{2ia}$. Alors

$$\oint_{\Gamma_r}f(z)\mathrm{d}z=2i\pi\times 1\times\frac{1}{2ia}=\frac{\pi}{a}$$

Par ailleurs, pour tout $\epsilon>0$, il existe r tel que $|f(z)|z||<\epsilon$ pour $|z|>r$, donc :

$$\oint_{\Gamma_r}f(z)\mathrm{d}z=\int_0^{\pi}f(re^{it})rie^{it}\mathrm{d}t+\int_{\pi}^{\pi+2}f(-r+(t-\pi)r)r\mathrm{d}t$$

$$\left|\oint_{\Gamma_r}f(z)\mathrm{d}z-\underbrace{\int_{-r}^{r}f(u)\mathrm{d}u}_{u=-r+(t-\pi)r}\right|<\epsilon\times\pi$$

Ainsi pour r suffisamment grand : $\displaystyle\int_{-r}^{r}f(u)\mathrm{d}u\underset{r\to+\infty}{\longrightarrow}\frac{\pi}{a}$ et $\displaystyle\int_{-\infty}^{+\infty}\frac{\mathrm{d}x}{x^2+a^2}=\frac{\pi}{a}$
Pour le dernier savoir-faire, on fera attention au moment du calcul du résidu que la fonction $z\mapsto f(z)e^{iaz}$ n'est pas, en règle générale, une fraction rationnelle.

Savoir faire - Intégrale de troisième type

Il s'agit de calculer $I=\displaystyle\int_{-\infty}^{+\infty}f(x)e^{iax}\mathrm{d}x$.
On suppose que cette intégrale est convergente, ce qui impose nécessairement que $zf(z)\underset{|z|\to\infty}{\longrightarrow}0$. On suppose également que $S\subset\mathbb{C}\setminus\mathbb{R}$ (pas de points singuliers (pôles) réels).
En considérant le « demi-cercle » de diamètre l'axe des réels et la partie positive (resp. négative), on trouve :

$$I=2i\pi\sum_{\mathrm{Im}(s_j)>0}\mathrm{Res}(fe^{ia\cdot},s_z)\text{ si }a>0.$$

$$I=-2i\pi\sum_{\mathrm{Im}(s_j)<0}\mathrm{Res}(fe^{ia\cdot},s_z)\text{ si }a<0\text{ (resp.).}$$

Souvent on exploite ce savoir-faire à une recherche de cos ou sin au numérateur (en prenant la partie réelle ou imaginaire).

Exemple - $\displaystyle\int_{-\infty}^{+\infty}\frac{\cos(bx)\mathrm{d}x}{x^2+a^2}$ **avec** $a,b>0$**.**

L'idée est considérer $x\mapsto\dfrac{e^{bx}}{x^2+b^2}$, puis de prendre la partie réelle.
On considère de nouveau Γ_r, le demi-cercle de centre 0, de rayon r de partie imaginaire positive. Un paramètrage de Γ_r est par exemple $\gamma_r:[0,\pi+2]\to\mathbb{C}$ tel que $\gamma_r(t)=re^{it}$ si $t\in[0,\pi]$, puis $\gamma_r(t)=-r+(t-\pi)r$ sur $[\pi,\pi+2]$.
$f:z\mapsto\dfrac{1}{z^2+a^2}$ admet deux pôles ia et donc si $r>a$, f admet un seul pôle dans Γ_r : le point ia.
On a alors $\mathrm{Ind}_{\Gamma_r}(ia)=1$ et $\mathrm{Res}(g,ia)=\lim\limits_{z\to ia}(z-ia)\dfrac{e^{ibz}}{z^2+a^2}=\dfrac{e^{-ab}}{2ia}$

$$\oint_{\Gamma_r}f(z)\mathrm{d}z=2i\pi\times 1\times\frac{e^{-ab}}{2ia}=\frac{\pi e^{-ab}}{a}$$

Par ailleurs, pour tout $\epsilon>0$, il existe r tel que $f(z)|z|<\epsilon$ pour $|z|>r$, donc :

$$\oint_{\Gamma_r}f(z)\mathrm{d}z=\int_0^{\pi}f(re^{it})e^{ibre^{it}}r\mathrm{d}t+\int_{-r}^{r}f(u)e^{ibu}\mathrm{d}u$$

Ainsi pour r suffisamment grand : $\displaystyle\int_{-r}^{r}f(u)\mathrm{d}u\underset{r\to+\infty}{\longrightarrow}\frac{\pi e^{-ab}}{a}$ et $\displaystyle\int_{-\infty}^{+\infty}\frac{\mathrm{d}x}{x^2+a^2}=\frac{\pi e^{-ab}}{a}$. Rest à prendre la partie réelle : $\displaystyle\int_{-\infty}^{+\infty}\frac{\cos(bx)\mathrm{d}x}{x^2+a^2}=\frac{\pi e^{-ab}}{a}$

6. Prolongement analytique

6.1. Zéros d'une fonction holomorphe

Avant d'étudier le théorème de résidus, nous avons rencontré les fonctions méromorphes. Il s'agit de fonctions holomorphes sauf en un nombre finis de point de $\mathbb{C}$. L'étude des pôles et l'étude des racines d'une fonction holomorphe sont certainement intéressants.

Remarque - Rappels topologique 1 : points d'accumulation et points isolés

On rappelle qu'un points adhérent est la limite d'une suite de points d'un ensemble.
Les points d'accumulation a sont des points adhérents par une suite de points de A, tous différent du point limite.
$\exists\,(a_n)\in(A\setminus\{a\})^{\mathbb{N}}$ telle que $(a_n)\to a$.
Ou encore : $\forall\,\epsilon>0$, $\exists\,a_\epsilon\in A$ tel que $0<|a-a_\epsilon|<\epsilon$.
Les points isolés sont des points qui ne sont pas des points d'accumulation
$\exists\,\epsilon>0$ tel que $B(x,\epsilon)\cap A=\{x\}$.

Remarque - Rappels topologique 2 : parties connexes

On a vu que E est connexe (dans $\mathbb{R}$), si on ne peut pas l'écrire comme réunion de deux sous-ensembles séparés non vide.
On n'a pas $E=A\cap B$ avec $\overline{A}\cap B=\emptyset$ et $A\cap\overline{B}=\emptyset$.
Une méthode pour démontrer que E est connexe (par arcs) consiste à montrer que pour tout $a,b\in E$, il existe $\varphi:[0,1]\to[a,b]$ continue avec $\varphi(0)=a$ et $\varphi(1)=b$.
Une autre méthode consiste souvent à faire un raisonnement par l'absurde et à travailler à partir du nombre x_0 qui est obtenu comme borne supérieure d'un ensemble A (à inventer) et élément de B ou bien élément de A et borne inférieure de B. A partir de ce x_0, trouver une contradiction.

Analyse - Factorisation par $(z-a)^m$

On sait que f est holomorphe donc analytique sur U.
Soit $a\in Z_f$, f admet un développement autour de a,

$\exists\, r>0$ tel que $\forall\, z\in B(a,r)$ (U est un ouvert) : $f(z)=\sum_{n=0}^{+\infty} a_n(z-a)^n$.

$a\in Z_f$, donc $f(a)=0=a_0$. Soit $K=\{n\in\mathbb{N}^*\mid a_n\neq 0\}\subset\mathbb{N}$.

• Ou bien K est majoré, et donc K admet un plus grand élément >0 : $m(a)-1$.

On a au voisinage de a : $f(z)=\sum_{n=m(a)}^{+\infty} a_n(z-a)^n=(z-a)^{m(a)}\sum_{n=0}^{+\infty} a_{n+m}(z-a)^n$.

La fonction $g: z\mapsto \dfrac{f(z)}{(z-a)^{m(a)}}$ est bien définie au voisinage de a et sur $U\setminus\{a\}$.

Et f ne s'annule qu'en a sur le voisinage de a.

Le nombre de zéros de f est au plus dénombrable.

• Ou bien K n'est pas majoré et donc $f=0$ est identiquement nulle au voisinage de a.

Ce point a est un point d'accumulation.

Le théorème suivant reprend cette idée, mais il annonce plus : s'il existe un point d'accumulation, alors f est nécessairement nulle sur tout le connexe.

Notons $Z_f=\{a\in U\mid f(a)=0\}$, l'ensemble des zéros de f.
Puisque f est holomorphe en a, elle est développable en série entière autour de a

Définition - Ordre des zéros de f
Soit U un ouvert connexe de $\mathbb{C}$ et f une fonction holomorphe définie sur U.
Soit $a\in Z_f$.
- Ou bien : $\forall\, n\in\mathbb{N}$, $f^{(n)}(a)=0$ Dans ce cas il existe V voisinage de a tel que $\forall\, x\in V\setminus\{a\}$, $f(x)=0$.
- Ou bien : il existe $m(a)\in\mathbb{N}^*$ et $g\in\mathscr{H}$ tel que $g(a)\neq 0$ et $\forall\, z\in U$, $f(z)=g(z)(z-a)^{m(a)}$.
  Le nombre $m(a)$ s'appelle l'ordre du zéro de f au point a.
  Dans ce cas il existe V voisinage de a tel que $\forall\, x\in V\setminus\{a\}$, $f(x)\neq 0$.

Proposition - Zéros isolés
Soit U un ouvert connexe de $\mathbb{C}$. Soit f holomorphe sur U.
S'il existe $a\in Z_f$, d'ordre infini, alors f est identiquement nulle sur U.

Démonstration
Supposons que a est d'ordre infini. Donc pour tout $n\in\mathbb{N}$, $f^{(n)}(a)=0$.
Posons $A=\{x\in U\mid \forall\, n\in\mathbb{N}, f^{(n)}(x)=0\}$ A est non vide, puisque $a\in A$. Soit $b\in U$, quelconque et $\gamma:[0,1]\to[a,b]$ un chemin (non nécessairement droit de a à b dans le connexe U).
$\gamma(0)\in A$. Notons $T=\sup\{t\in[0,1]\mid \gamma(t)\in A\}$.
Il existe une suite (t_n) d'éléments de $[0,1]$ tel que $(t_n)\to T$ et $\gamma(t_n)\in A$.
Comme f est continue, ainsi que toutes ses dérivées : $\forall\, k\in\mathbb{N}$, $f^{(k)}(t_n)=0\to f^{(k)}(T)$. Donc $\gamma(T)\in A$.
Ainsi $\gamma(T)$ est un zéro d'ordre infini de f. Il existe une voisinage de $\gamma(T)$ sur lequel f est nul.
Comme T est une borne supérieure, cela signifie que $T=1$, nécessairement et donc $f(b)=0$. □

6.2. Prolongement analytique

Analyse - L'application $z\mapsto\dfrac{1}{1+z}$

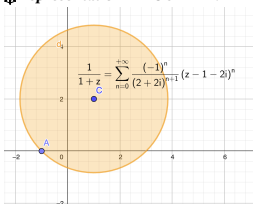
C'est bien connu, $f(z)=\sum_{k=0}^{+\infty}(-1)^k z^k$, pour $z\in\mathscr{D}(0,1)$ (ouvert).

Peut-on étendre plus? Ici, on est centré en 0 et le rayon est $R=1$, à cause du pôle en -1.
Et centré en a quelconque (dans $\mathbb{C}$? On pose $z=a+h$, on a

$$\frac{1}{1+z}=\frac{1}{1+a+h}=\frac{1}{1+a}\times\frac{1}{1+\frac{h}{1+a}}=\frac{1}{1+a}\sum_{n=0}^{+\infty}\left(\frac{-1}{1+a}\right)^n h^n=\sum_{n=0}^{+\infty}\frac{(-1)^n}{(1+a)^{n+1}}(z-a)^n$$

On a trouvé le développement en série analytique de $\frac{1}{1+z}$ au point a.
La série obtenue est géométrique, elle converge pour tout z tel que $\left|\frac{z-a}{1+a}\right|<1\iff z\in$

Représentation - DES en $1+2i$



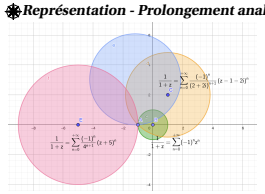
$\mathscr{B}(a,1+a)$ En fait, le rayon $R=a+1$ peut s'interpréter comme la valeur maximale de manière à ne pas avoir $z=-1$. Il est certain que $\frac{1}{1+z}$ n'est pas défini en -1.

Proposition - Prolongement analytique
Soient f et g deux fonctions holomorphes ou analytiques.
Soit U un ouvert connexe contenant $\mathscr{D}_f$ et $\mathscr{D}_g$.
Si $\{z\in U\mid f(z)=g(z)\}$ admet une point d'accumulation, alors $f=g$ sur U entier.

Remarque - Domaine d'égalité
On exploite ce théorème souvent sur $U=\mathscr{D}_f\cap\mathscr{D}_g$ directement (à condition que cet ensemble soit (ouvert et) connexe.

Démonstration
Considérons $h=f-g$, alors Z_h admet un point d'accumulation, on a donc un zéro non isolé.
Par conséquent $h=0$ sur tout U, i.e : $f_{|U}=g_{|U}$. □

Représentation - Prolongement analytique



Application - $z\mapsto\dfrac{1}{1+z}$
On peut passer d'une zone à une autre par connexité.
Cela permet aussi d'élargir la définition d'une fonction. En effet, il n'existe en fait qu'une seule fonction holomorphe ayant un développement particulier en un point.
Dans le cadre des fonctions holomorphes, le rêve de Cauchy se réalise!

Exemple - $z\mapsto e^{-1/z^2}$
Cette fonction f vérifie pour tout $z\in\mathbb{C}^*$, $f^{(n)}(z)\mapsto_0 0$ et pourtant $f=\neq 0$.
0 est la fonction holomorphe qui s'annule ainsi que toutes ses dérivées en 0.
f n'est nécessairement pas holomorphe.

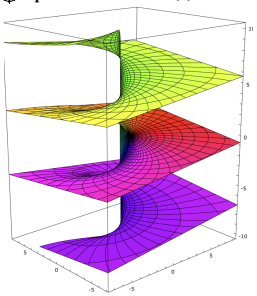
6.3. Fonctions à singularités. Vers les surfaces de Riemann

On termine par un preview de la saison 2.

Heuristique - Tourner autour d'un pôle

Lorsqu'on fait le tour autour de 0 de la fonction $z\mapsto\dfrac{1}{1+z}$, on retrouve la même série entière.
La fonction $z\mapsto\dfrac{1}{1+z}$ est univariée.
Il n'en est pas de même de son intégrale : $\displaystyle\int_\Gamma\frac{\mathrm{d}z}{1+z}$

Représentation - $z\mapsto\ln(z)$



Analyse - $z\mapsto\ln z$
La fonction $z\mapsto\ln z$ qui est « la » primitive de $\frac{1}{z}$ ne peut être définie En tournant autour du pôle, un décallage de $2i\pi$ se mesure.
La fonction ln est en fait multivariée : $\forall\, k\in\mathbb{Z}$, $\exp(\ln a)=\exp(\ln(a)+2ik\pi)$ Riemann propose un concept pour dépasser cette limite, a priori.

Définition - Surface de Riemann
Une surface de Riemann est un espace topologique séparé X, admettant un atlas modelé sur le plan complexe $\mathbb{C}$ dont les applications de changement de cartes sont des applications biholomorphes.
Autrement dit X admet un recouvrement par des ouverts U_i homéomorphes à des ouverts de $\mathbb{C}$; ces cartes dites holomorphes $f_i: U_i\to V_i$ sont telles que les fonctions de changement de cartes $f_i\circ f_j^{-1}$ soient des fonctions holomorphes entre ouverts de $\mathbb{C}$.

En fait, en géométrie différentielle et géométrie analytique complexe, une surface de Riemann est une variété complexe de dimension 1. Vivement la prochaine saison!

7. Bilan

Synthèse

- ⇝ Une fonction holomorphe sur un ouvert U est une fonction dérivable en tout $z_0 \in U$, de la variable complexe. Cette forme de dérivation est plus exigeante que la dérivation à deux variables : localement la transformation n'est pas simplement affine, elle est conforme (similitude). Il existe de nombreuses fonctions holomorphes (toutes nos fonctions usuelles, entre autres).
- ⇝ Cette rigidité donne aux fonctions de a-la variable complexe une propriété impensable pour les fonctions réelles : si elles sont une fois dérivable (holomorphe) alors elles sont infiniment dérivable, et même analytique. Cela signifie qu'en tout point de u, la fonction holomorphe est comparable à une série entière (centrée en ce point) de rayon > 0.
- ⇝ Pour montrer ce résultat important, il a d'abord fallut faire un détour par les intégrales curvilignes, i.e. les intégrales sur des chemins (lignes) de $\mathbb{C}$. Là, une foule de théorème, tous plus ou moins dûs à Cauchy s'observent : ils lient les intégrales de chemin d'une fonction aux valeurs aux extrémités de la primitive (comme toute intgrale) mais également aux nombres de points singuliers (pôles) de la fonction intégrée à l'intérieur du chemin d'intégration (indice d'un point par rapport à une courbe fermée). En découle des tas de théorèmes comme le principe du maximum que nous verrons en TD.
- ⇝ Une première application a été le théorème de résidus qui permet, lorsqu'on le maitrise bien de calculer les valeurs exactes d'intégrales difficiles voire de sommes infinies immondes.
- ⇝ Une seconde application est celui du recollement par prolongement analytique sur un convexe. En fait, les éeros d'une fonction holomorphe sont soient isolés soit dense. Ou encore : il n'existe qu'une fonction holomorphe sur $\mathbb{C} \setminus E$ (où E est au plus dénombrable) connaissant la valeur de toutes les dérivées en un point.

Savoir-faire et Truc & Astuce du chapitre

- — Savoir-faire - Montrer l'holomorphie (ou non) avec $H : \mathbb{R}^2 \to \mathbb{C}, (x, y) \mapsto f(x + iy)$
- — Savoir-faire - Démontrer qu'une fonction n'est pas la dérivée d'une fonction holomorphe
- — Savoir-faire - Calculer les résidus de f en a
- — Savoir-faire - Intégrale de premier type (Résidus)
- — Savoir-faire - Intégrale de deuxième type (Résidus)
- — Savoir-faire - Intégrale de troisième type (Résidus)

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\mathscr{H}(U)$	Ensemble des fonctions holomorphe définies sur un ouvert $U \subset \mathbb{C}$	$\forall\, z_0 \in U\ f(z) = f(z_0) + A(z - z_0) + (z - z_0)\epsilon(z)$ où $A \in \mathbb{C}$ (similitude) et $\epsilon(z) \underset{z \to z_0}{\longrightarrow} 0$	$(\mathscr{H}(U), \cdot, +, \times)$ est une algèbre
$\int_\Gamma g(z)\mathrm{d}z$	Intégrale curvilgne de g le long de Γ	Si $\Gamma = \mathrm{Im}(\gamma)$ avec $\gamma : [a, b] \to \mathbb{C}$, de classe $\mathscr{C}^1$ sans point stationnaire : $\int_\Gamma g(z)\mathrm{d}z = \int_a^b g(\gamma(t))\gamma'(t)\mathrm{d}t$	Ce nombre est indépendant du choix de γ.
$\mathrm{Ind}_\Gamma(z_0)$	Indice de Γ par rapport à z_0	$\mathrm{Ind}_\Gamma(z_0) = \frac{1}{2i\pi}\oint_\Gamma \frac{\mathrm{d}z}{z - z_0} \in \mathbb{Z}$	Il indique le nombre de tour (sens direct) de Γ autour de z_0
$\mathrm{Res}(f, z_0)$	Résidu de f en z_0	Le coefficient devant $(z - z_0)^{-1}$ dans le DAS de f au voisinage de z_0	Si z_0 est pôle d'ordre n, $\mathrm{Res}(f, z_0) = \frac{1}{(n-1)!}\lim_{z \to z_0} \frac{\partial^{n-1}}{\partial z^{n-1}}((z - z_0)^n f(z))$

Retour sur les problèmes

A.4 C'est l'enjeu de ce cours

A.5 Intégration curviligne (sur une ligne ou un chemin), ou bien intégration sur une surface comme pour le théorème de Green-Riemann

A.6 Si P ne s'annule pas alors $\frac{1}{P}$ est holomorphe et verifie donc le principe de maximum, . Voir TD

A.7 Question avancée dans la partie sur le prolongement analytique.

A.8 Oui, la relation $\Gamma(z + 1) = z\Gamma(z)$ permet de définir pour $z \in \mathbb{R}^-$ et $z \notin \mathbb{Z}$, $\Gamma(z) = \frac{1}{(z+1)(z+2)\cdots(z+\lfloor z \rfloor)}\Gamma(z + \lceil z \rceil)$, il n'y a qu'une fonction holomorphe qui égale avec Γ sur le connexe $\mathbb{R}_+^*$.

Table de matières

I Techniques mathématiques, à travers l'histoire **3**

1 Calculs polynomiaux **5**
1. Quelques problèmes . . . 6
1.1. Problèmes . . . 6
1.2. Vocabulaires et contextes . . . 7
2. Equation polynomiale. Algèbre et géométrie . . . 7
2.1. Révolution 1 : Viète . . . 7
2.2. Révolution 2 : Descartes . . . 9
3. Opérer (=calculer) avec des polynômes . . . 12
3.1. Développer . . . 12
3.2. Factoriser . . . 14
3.3. Expliciter formellement les racines . . . 17
4. Equation polynomiale et analyse . . . 18
4.1. La meilleure méthode : l'essai/erreur . . . 18
4.2. Retro-contrôle . . . 19
4.3. Méthode de la sécantes . . . 19
4.4. Vers la dérivation. Méthode de la tangente . . . 20
5. Bilan . . . 21

2 Calculs trigonométriques **23**
1. Problèmes . . . 24
2. Fonctions trigonométriques . . . 24
2.1. Construction historique . . . 24
2.2. Fonctions sinus et cosinus . . . 25
2.3. Fonction tangente . . . 26
3. Formules trigonométriques . . . 27
3.1. Formules de Regiomontanus . . . 27
3.2. Produit en somme et réciproquement . . . 29
3.3. Angle moitié . . . 30
4. Trigonométrie réciproque . . . 31
4.1. Arcsinus . . . 31
4.2. Arccosinus . . . 32
4.3. Arctangente . . . 33
5. Bilan . . . 34

3 Fonctions *à la Euler* **37**
1. Problèmes . . . 38
2. Généralités sur les fonctions . . . 38
2.1. Définition et représentation d'une fonction . . . 38
2.2. Opérations sur les fonctions . . . 39
2.3. Vocabulaire d'analyse de fonctions . . . 40
2.4. Bijections et réciproques . . . 42

2.5. Etude des branches infinies en ∞ . . . 43
3. Fonctions trigonométriques . . . 45
3.1. Fonctions circulaires . . . 45
3.2. Fonctions circulaires réciproques . . . 46
4. Fonctions polynomiales et puissances rationnelles . . . 48
4.1. Fonction puissance entière relative . . . 48
4.2. Fonctions polynomiales . . . 50
4.3. Fonction puissance rationnelle . . . 51
5. Exponentielles et logarithmes . . . 52
5.1. ExponentielleS . . . 52
5.2. LA fonction exponentielle . . . 54
5.3. LogarithmeS . . . 56
5.4. Retour sur les fonctions puissances, avec un exposant non rationnel . . . 57
5.5. Croissances comparées . . . 58
5.6. Fonctions hyperboliques directes . . . 58
6. Sommes numériques infinies . . . 59
7. Bilan . . . 60

4 Ensemble des nombres complexes **63**
1. Problèmes . . . 64
2. EULER : manipulateur des nombres du diable . . . 64
2.1. Racine de polynômes . . . 64
2.2. Calcul algébrique . . . 65
2.3. Représentation graphique (addition et longueur) . . . 67
2.4. Inégalités . . . 67
3. Le visionnaire : GAUSS et la multiplication complexe . . . 68
3.1. Les complexes de module 1 . . . 68
3.2. Notation exponentielle . . . 69
3.3. Formules d'Euler et de de Moivre . . . 71
3.4. Argument, forme trigonométrique . . . 73
4. Racines d'un nombre complexe . . . 74
4.1. Recherche de racines carrées . . . 74
4.2. Racines n-ièmes de l'unité . . . 75
4.3. Racines n-ièmes d'un nombre complexe . . . 76
5. $\mathbb{R}^2 = \mathbb{C} = \mathscr{P}$ . . . 77
5.1. Regard géométrique sur le plan complexe . . . 77
5.2. Lignes de niveau . . . 78
5.3. Transformations du plan (point de vue complexe) . . . 80
6. Bilan . . . 84

5 Utilisation de la dérivation **87**
1. Problèmes . . . 88
2. Dérivation . . . 89
2.1. Approche historique . . . 89
2.2. Dérivabilité . . . 89
2.3. Approximation linéaire . . . 90
2.4. Règles de dérivation . . . 90
2.5. Dérivation de fonctions usuelles . . . 91
2.6. Dérivées seconde, troisième... . . . 94
3. Quelques utilisations de la dérivation . . . 94
3.1. Variations . . . 94
3.2. Bijections et réciproques . . . 95
3.3. Inégalités . . . 97
3.4. Calculs de limites (lever les indéterminations) . . . 97
3.5. Approximation polynomiale (développement limité) . . . 99
4. Dérivation de fonctions réelles à valeurs complexes . . . 100
4.1. Fonctions à valeurs complexes . . . 100

4.2. Dérivation d'une fonctions d'une variable réelle, à valeurs complexes . . . 103
4.3. Propriétés . . . 103
4.4. Composition avec l'exponentielle complexe . . . 104
5. Bilan . . . 104

6 Fonctions primitives et équations différentielles 107
1. Problèmes . . . 108
2. Primitives . . . 109
2.1. Définitions . . . 109
2.2. Primitives usuelles . . . 110
2.3. Quelques cas particuliers . . . 111
3. Intégrales . . . 113
3.1. Théorème fondamental et conséquences . . . 113
3.2. Quelques propriétés de l'intégrale . . . 115
3.3. Technique 1 : Intégration par parties . . . 116
3.4. Technique 2 : Changement de variables . . . 118
4. Equation différentielle (dérivation/primitivation tordue) . . . 123
4.1. Vocabulaire . . . 123
4.2. Equation différentielle linéaire d'ordre 1 . . . 124
4.3. Equation différentielle linéaire d'ordre 2 à coefficients constants . . . 129
5. Bilan . . . 135

7 Calculs et opérations avec des sommes ou des produits 137
1. Quelques problèmes . . . 138
2. Symboles $\sum$ et $\prod$ . . . 138
2.1. Définition . . . 138
2.2. Quatre règles opératoires . . . 140
2.3. Avec Python . . . 143
2.4. Des sommes connues . . . 144
2.5. Sommes doubles (multiples…) . . . 146
2.6. Exercice d'applications . . . 150
3. Coefficients binomiaux et formule du binôme . . . 151
3.1. Factorielles et coefficients binomiaux . . . 151
3.2. Triangle de Pascal . . . 152
3.3. Formule du binôme . . . 153
4. Bilan . . . 154

8 Résolution de systèmes linéaires. 157
1. Quelques problèmes . . . 158
2. Systèmes linéaires. Equivalence . . . 158
2.1. Vocabulaire . . . 159
2.2. Systèmes équivalents . . . 159
3. Résolution explicite. cas des petits systèmes $n = p = 2$ ou $n = p = 3$ . . . 160
3.1. Vers la formule de Cramer . . . 160
4. Algorithme su pivot de Gauss . . . 162
4.1. Systèmes équivalents : opérations élémentaires . . . 162
4.2. Algorithme du pivot de Gauss . . . 162
4.3. Applications. Différents formes de l'ensemble des solutions . . . 163
5. Bilan . . . 164

9 Calcul matriciel 165
1. Problèmes . . . 166
2. Esnsemble $\mathcal{M}_{n,p}(\mathbb{K})$ . . . 167
2.1. Ensemble des matrices . . . 167
2.2. Opérations (vectorielles) sur les matrices . . . 168
2.3. Transposition . . . 170
3. Multiplication matricielle . . . 171
3.1. Définition . . . 171
3.2. Interprétation en terme de systèmes linéaires . . . 172
3.3. Propriété du produit . . . 173
3.4. Produit par blocs . . . 175
4. Les matrices carrées . . . 176
4.1. L'anneau $(\mathcal{M}_n(\mathbb{K}), +, \times)$ . . . 176
4.2. Puissance de matrices . . . 176
4.3. Inversibilité d'une matrice . . . 177
4.4. Quelques sous-ensembles remarquables . . . 180
4.5. Trace d'une matrice carrée . . . 181
5. Opérations élémentaires sur les matrices . . . 182
5.1. Opérations élémentaires sur les lignes d'une matrices . . . 182
5.2. Opérations élémentaires sur les colonnes d'une matrice . . . 185
5.3. Méthode du pivot de Gauss pour obtenir l'inverse d'une matrice . . . 185
6. Bilan . . . 189

II Logique ensembliste 193

10 Structure logique 195
1. Cours mathématiques . . . 196
1.1. L'énigme mathématique . . . 196
1.2. Structure de cours . . . 196
2. Quantificateurs et notations ensemblistes . . . 197
2.1. Appartenance, éléments . . . 197
2.2. Différentes manières d'écrire un ensemble . . . 198
2.3. Utilisation de quantificateurs . . . 200
2.4. Parties d'un ensemble . . . 201
2.5. Produit cartésien . . . 202
2.6. Opérations sur les ensembles . . . 202
3. Vocabulaire sur les assertions . . . 203
3.1. Définitions . . . 203
3.2. Négation . . . 204
3.3. Implications et équivalence d'assertions . . . 205
4. Principales méthodes de démonstration . . . 206
4.1. Démonstration d'une implication . . . 206
4.2. Démonstration d'une équivalence . . . 209
4.3. Raisonnement par l'absurde . . . 210
4.4. Conditions nécessaire, suffisante . . . 211
4.5. Exploiter un contre-exemple dans une démonstration . . . 212
4.6. Démonstration par récurrence . . . 212
4.7. Démonstration par algorithme . . . 214
5. Bilan . . . 217

11 Applications (entre ensembles) 219
1. Problèmes . . . 220
2. Applications de E dans F . . . 220
2.1. Vocabulaire lié aux applications . . . 220
2.2. Bijections (injections et surjections) . . . 222
3. Image directe et image réciproque d'un ensemble . . . 226
3.1. Image directe . . . 226

3.2. Image réciproque d'un ensemble . . . 228
4. Fonction indicatrice . . . 229
4.1. Définition . . . 229
4.2. Propriétés ensemblistes et calcul avec fonctions indicatrices . . . 229
5. Cardinal d'ensemble fini . . . 230
5.1. Principe des tiroirs . . . 230
5.2. Classe des ensembles de même cardinal . . . 231
5.3. Cardinal, fonction indicatrice et somme (finie) . . . 232
6. Familles . . . 233
6.1. Familles quelconques . . . 233
6.2. Famille indexée sur $\mathbb{N}$. Suites . . . 234
7. Bilan . . . 237

12 Relations binaires sur un ensemble 239
1. Problèmes . . . 240
2. Graphe . . . 241
2.1. Formalisation . . . 241
2.2. Vocabulaire . . . 241
2.3. Applications . . . 241
3. Relations binaires . . . 242
3.1. Construction et représentation . . . 242
3.2. Caractérisations . . . 242
4. Relation d'ordre . . . 242
4.1. Définitions . . . 242
4.2. Ensemble avec ordre total . . . 243
4.3. Ensemble avec ordre partiel . . . 244
4.4. Eléments particuliers . . . 244
4.5. Ordre strict . . . 247
5. Relation d'équivalence . . . 247
5.1. Propriétés caractéristiques . . . 247
5.2. Classes d'équivalence . . . 248
5.3. Partition de E . . . 249
6. Bilan . . . 250

III Arithmétique & Structures élémentaires 253

13 Groupes 255
1. Problèmes . . . 256
2. Lois de composition internes . . . 257
2.1. Définitions . . . 257
2.2. Propriétés directes . . . 258
2.3. Induction . . . 258
3. Structure de groupe . . . 258
3.1. Définition et propriétés . . . 258
3.2. Groupes produits . . . 259
3.3. Exemples . . . 260
4. Sous-groupe . . . 263
4.1. Définition et caractérisations . . . 263
4.2. Intersection . . . 264
4.3. Sous-groupe engendré . . . 265
4.4. Démontage d'un groupe . . . 267
5. Morphismes de groupes . . . 270
5.1. Définition et propriété immédiate . . . 270
5.2. Image et noyau d'un morphisme . . . 270
5.3. Premier théorème d'isomorphisme . . . 271
6. Bilan . . . 272

14 Construction d'ensembles numériques : des entiers à la droite réelle 275
1. Problèmes . . . 276
2. Nombres algébriques . . . 277
2.1. Nombres entiers . . . 277
2.2. Nombres rationnels . . . 279
2.3. Nombres algébriques . . . 280
3. Propriétés de $\mathbb{R}$ . . . 280
3.1. Principe de construction de $\mathbb{R}$ . . . 280
3.2. Fonctions classiques associées à $\mathbb{R}$ . . . 281
4. Parties de $\mathbb{R}$ et topologie . . . 283
4.1. Bornes supérieure et inférieure . . . 283
4.2. Densité de $\mathbb{D}$ ou $\mathbb{Q}$ dans $\mathbb{R}$ . . . 286
5. Bilan . . . 287

15 Divisibilité et congruence sur $\mathbb{Z}$. PGCD & PPCM 289
1. Problèmes . . . 290
2. Divisibilité dans $\mathbb{Z}$ . . . 291
2.1. Intégrité de $\mathbb{Z}$ et régularité . . . 291
2.2. Diviseurs, multiples . . . 291
2.3. Division euclidienne de a par b . . . 292
2.4. Arithmétique modulaire . . . 294
3. Plus Grand Commun Diviseur de deux nombres . . . 295
3.1. $PGCD$ de deux nombres. Définition « naturelle » . . . 295
3.2. Algorithme d'Euclide . . . 296
3.3. Couple de Bézout . . . 298
3.4. Deux caractérisations essentielles du PGCD . . . 300
4. Entiers premiers entre eux. Factorisation . . . 302
4.1. Définition et critère de Bézout . . . 302
4.2. Lemme de Gauss et décomposition en facteurs relativement premiers . . . 302
5. Généralisation à plusieurs entiers . . . 303
5.1. $PGCD$ d'un nombre fini d'entiers relatifs . . . 303
5.2. Deux caractérisation du $PGCD(a_1, a_2, \dots a_k)$ . . . 305
5.3. Entiers premiers entre eux dans leur ensemble . . . 306
6. Plus Petit Commun Multiple . . . 307
6.1. Construction . . . 307
6.2. Relation PPCM et PGCD . . . 308
7. Bilan . . . 308

16 Nombres premiers 311
1. Problèmes . . . 312
2. Théorèmes d'Euclide . . . 312
2.1. Définition . . . 312
2.2. Lemmes d'Euclide . . . 312
2.3. Théorème fondamental . . . 313
3. L'ensemble des nombres premiers . . . 314
3.1. Ensemble infini . . . 314
3.2. Crible d'Eratosthène . . . 315
4. Valuation (p-adique) . . . 315
4.1. Fonction valuation (en base p) . . . 315
4.2. Morphisme (de monoïde) . . . 316
4.3. Factorisation en produit de premiers . . . 316
4.4. Formule de Legendre . . . 317
5. Garantir que des nombres sont premiers . . . 318
5.1. Motivations . . . 318
5.2. Enoncé et applications . . . 319
5.3. Démonstrations . . . 319
6. Bilan . . . 322

17 Anneaux et corps **323**
1. Problèmes . . . 324
2. Structures d'anneau . . . 324
2.1. Définitions et propriétés premières . . . 324
2.2. Construction d'anneaux . . . 326
2.3. Idéaux . . . 328
2.4. Anneau euclidien. Anneau principal . . . 331
3. Structures de corps . . . 332
3.1. Corps . . . 332
3.2. Idéaux maximaux . . . 332
3.3. Sous-corps. Morphisme (de corps) . . . 333
4. Bilan . . . 333

IV Analyse réelle **335**

18 Suites numériques **337**
1. Problèmes . . . 338
2. Exemples fondamentaux . . . 339
2.1. Suites arithmético-géométriques . . . 339
2.2. Suites récurrentes linéaires homogène d'ordre 2 . . . 339
3. Suites extraites . . . 340
3.1. Rappels . . . 340
3.2. Valeur d'adhérence d'une suite . . . 341
3.3. Application 1 : Contraire de « à partir d'un certain rang » . . . 342
3.4. Application 2. Lemme des pics . . . 343
4. Limite d'une suite réelle . . . 343
4.1. Suite convergente . . . 343
4.2. Suites divergentes . . . 345
4.3. Opérations sur les suites/les limites et relation d'ordre . . . 346
4.4. Extension aux suites à valeurs complexes . . . 351
4.5. Bilan sur les théorèmes d'existence de limites . . . 353
5. Analyse asymptotique . . . 355
5.1. Hiérarchie de suites . . . 355
5.2. Suites équivalentes . . . 357
5.3. Suites dominées . . . 363
6. Bilan . . . 366

19 Questions topologiques interprétées sur $\mathbb{R}$ **369**
1. Problèmes . . . 369
2. Halo autour de $a \in \mathbb{R}$ . . . 370
2.1. Voisinages . . . 370
2.2. Intérieur, adhérence . . . 371
3. Intervalles et connexité . . . 374
3.1. Connexité . . . 374
3.2. Intervalle réel . . . 375
3.3. Sur-ensemble : droite numérique achevée . . . 376
4. Segments et compacités . . . 376
4.1. Segments emboîtés . . . 376
4.2. Fonctions d'intervalles et principe de dichotomie . . . 377
4.3. Théorème de Bolzano-Weierstrass . . . 379
4.4. Lemme de Cousin . . . 380
5. Curiosité topologique : complétude . . . 382
5.1. Suites de Cauchy . . . 382
5.2. $\mathbb{R}$ est complet . . . 382
6. Bilan . . . 383

20 Continuité **385**
1. Problèmes . . . 386
2. Limites (de fonctions) . . . 386
2.1. Définitions . . . 386
2.2. Ordre et limites . . . 390
2.3. Opérations sur les limites . . . 391
2.4. Cas des fonctions monotones . . . 392
2.5. Continuité en un point . . . 394
3. Fonction continue sur un ensemble (intervalle, segment...) . . . 395
3.1. Fonctions continues sur I . . . 395
3.2. Prolongement par continuité . . . 396
3.3. Théorème des valeurs intermédiaires . . . 397
3.4. Cas de l'image d'un segment par f continue . . . 398
3.5. Théorème de la bijection (bis) . . . 401
3.6. Continuité uniforme . . . 402
4. Généralisation aux fonctions à valeurs dans $\mathbb{C}$ . . . 405
4.1. Opérations classiques sur $\mathscr{F}(X,\mathbb{C})$ . . . 405
4.2. Fonctions bornées . . . 405
4.3. Limites . . . 406
4.4. Opérations sur les limites . . . 406
4.5. Continuité . . . 407
5. Bilan . . . 407

21 Dérivation (approfondissements) **409**
1. Problèmes . . . 410
2. Dérivée . . . 410
2.1. Définitions . . . 410
2.2. Règles de calcul . . . 412
2.3. Fonctions de classe $\mathscr{C}^k$ . . . 414
3. Etude globale des fonctions dérivables . . . 417
3.1. Théorème de Rolle . . . 417
3.2. Egalité des accroissements finis . . . 419
3.3. Inégalité des accroissements finis . . . 421
3.4. Prolongement dérivable ou limite de la dérivée . . . 422
3.5. Prolongement de la règle de l'Hospital . . . 425
4. Généralisation aux fonctions à valeurs complexes . . . 426
4.1. Définitions . . . 426
4.2. Opérations . . . 427
5. Bilan . . . 428

22 Convexité **431**
1. Problèmes . . . 432
2. Fonctions convexes . . . 432
2.1. Ecriture paramétrique d'un segment . . . 432
2.2. Définition d'une fonction convexe (et concave) . . . 432
2.3. Stabilité de l'ensemble des fonctions convexes . . . 433
3. Inégalités . . . 433
3.1. Généralisation . . . 433
3.2. Comparaison des pentes . . . 434
3.3. Tangente . . . 435
4. Régularité . . . 436
4.1. Continuité . . . 436
4.2. Critères de convexité (avec la dérivation) . . . 436
5. Bilan . . . 438

23 Développements limités **439**
1. Problème . . . 440
2. Vocabulaire et opérations pour des développements asymptotiques de fonctions . . . 440
2.1. Rappel : le cas des suites . . . 440
2.2. Définitions . . . 441
2.3. Relations d'équivalence. Relation de préordre . . . 443
2.4. Echelle de comparaison . . . 444
2.5. Algèbre des relations de comparaison . . . 445
3. Développements limités . . . 447
3.1. Définitions . . . 447
3.2. Propriétés . . . 448
3.3. Existence de développements limités . . . 449
3.4. Opérations . . . 453
3.5. Généralisation . . . 456
4. Applications des DL . . . 457
4.1. Recherche de limites et d'équivalents (suite ou fonction) 457
4.2. Etude locale d'une fonction . . . 457
5. Bilan . . . 459

V Algèbre linéaire & bilinéaire **461**

24 Espaces vectoriels **463**
1. Problèmes . . . 464
2. Structure d'espace vectoriel . . . 465
2.1. Loi de composition externe . . . 465
2.2. Exemples fondamentaux d'espaces vectoriels . . . 466
2.3. Combinaisons linéaires . . . 467
3. Sous-espaces vectoriels . . . 468
3.1. Définition et caractérisation . . . 468
3.2. Exemples . . . 469
3.3. Sous-espace vectoriel engendré par une partie . . . 470
3.4. Somme de sous-espaces vectoriels . . . 472
4. Applications linéaires . . . 475
4.1. Définitions et exemples . . . 475
4.2. Cas général : structure de $\mathscr{L}(E,F)$ . . . 477
4.3. Cas particulier de $\mathscr{L}(E)$ . . . 478
4.4. Projecteurs et symétries . . . 480
5. Familles de vecteurs . . . 482
5.1. Sur-famille, sous-famille . . . 482
5.2. Familles génératrices de E . . . 482
5.3. Familles libres, liées . . . 484
5.4. Image d'une famille de vecteurs par une application linéaire . . . 486
6. Bilan . . . 487

25 Espace vectoriel de dimension finie **489**
1. Problèmes . . . 490
2. Bases et dimension . . . 491
2.1. Existence et unicité de l'écriture de tout vecteur dans une base . . . 491
2.2. Critère pour être une base . . . 492
2.3. Dimension d'un espace vectoriel . . . 494
2.4. Sous-espaces vectoriels en dimension finie . . . 498
3. Ecriture d'une application linéaire en dimension finie . . . 502
3.1. Détermination . . . 502
3.2. Matrice d'une application linéaire . . . 504
3.3. Changements de bases . . . 509

4. Théorème (formule) du rang et conséquences . . . 513
4.1. Théorème du rang . . . 513
4.2. Application du théorème du rang (Critère de bijection) . 514
4.3. Itération . . . 515
4.4. Formes linéaires et hyperplans . . . 516
5. Rang (et noyau) d'une matrice . . . 519
5.1. Rappel sur la résolution d'un système linéaire . . . 519
5.2. « Action » des matrices sur $\mathbb{K}^n \equiv \mathscr{M}_{n,1}(\mathbb{K})$ . . . 520
5.3. Image d'une matrice et famille génératrice . . . 521
5.4. Noyau d'une matrice et famille libre . . . 521
5.5. Théorème du rang . . . 522
5.6. Bilan : nouveau critère d'inversibilité (pour une matrice carrée) . . . 522
5.7. Action : $(P,Q)\cdot M \mapsto P\times M\times Q^{-1}$ . . . 523
5.8. Matrices extraites . . . 525
6. Bilan . . . 526

26 Structures affines **529**
1. Problèmes . . . 530
2. Introduction . . . 531
3. Translatés d'un sous-espace vectoriel . . . 531
3.1. Translation (linéaire) . . . 531
3.2. (Sous-)Espaces affines . . . 531
3.3. Exemples variées . . . 533
4. Systèmes d'équations linéaires . . . 534
4.1. Contextes . . . 534
4.2. Interprétations . . . 535
4.3. Structure de l'ensemble des solutions . . . 536
5. Equations, intersections et parallélisme . . . 536
5.1. Cas général . . . 536
5.2. Dans un plan (espace de dimension 2) . . . 538
5.3. Dans un espace de dimension 3 . . . 538
6. Bilan . . . 540

27 Espaces vectoriels euclidiens **541**
1. Problèmes . . . 542
2. Définitions et règles de calcul . . . 543
2.1. Produit scalaire . . . 543
2.2. Norme euclidienne . . . 544
2.3. Différentes identités . . . 547
3. Orthogonalité . . . 548
3.1. Vecteurs orthogonaux . . . 548
3.2. Sous-espaces orthogonaux . . . 549
3.3. Familles orthogonales, orthonormales . . . 550
4. Cas de la dimension finie : espaces euclidiens . . . 553
4.1. Définition . . . 553
4.2. Bases orthonormales . . . 554
5. Projections orthogonales . . . 556
5.1. Supplémentaire orthogonal . . . 556
5.2. Projections orthogonales . . . 557
5.3. Distance à un sous-ensemble d'une espace préhilbertien 558
5.4. Symétries orthogonales . . . 559
6. Hyperplans vectoriels et affines d'un espace euclidien . . . 560
6.1. Lemme de RIESZ . . . 560
6.2. Espace affine euclidien (élargissement vers l'affine) . . . 561
6.3. Transposition . . . 562
6.4. Crochet de dualité . . . 563
7. Bilan . . . 564

VI Combinatoire et groupe fini 567

28 Dénombrement (combinatoire) 569
1. Problèmes : expérience, modélisation et ensembles 570
   1.1. Questionnement 570
   1.2. Expériences réelles et modélisation 571
2. Ensembles finis 572
   2.1. Cardinal d'un ensemble 572
   2.2. Dénombrement par applications 574
   2.3. Dénombrement par calcul du cardinal d'une réunion. Addition. 575
   2.4. Dénombrement par calcul du cardinal d'un produit cartésien. Multiplication. 576
3. Listes et combinaisons 577
   3.1. Définitions des différents types d'ensemble 577
   3.2. Dénombrement d'un ensemble de listes avec répétition . 578
   3.3. Dénombrement de permutation d'un ensemble E 579
   3.4. Dénombrement d'un ensemble de p-listes sans répétition 580
   3.5. Dénombrement d'un ensemble de sous-ensemble à p éléments (combinaison) 581
   3.6. Propriétés du coefficient binomial (rappels) 582
4. Exercices d'applications 583
   4.1. Tableau des dénombrements classiques 583
   4.2. Coefficient multinomial 584
   4.3. Séries génératrices 585
5. Bilan 589

29 Un groupe fini : le groupe symétrique 591
1. Problèmes 592
2. Définitions 593
   2.1. Rappels sur le groupe symétrique 593
   2.2. Codages des permutations 593
   2.3. Des permutations particulières 595
3. Décomposition d'une permutation 597
   3.1. Partie génératrice d'un groupe 597
   3.2. Décomposition en produit de cycles 598
   3.3. Décompositions en produit de transpositions 600
4. Signature d'une permutation 601
   4.1. Motivation : nombre d'inversions 601
   4.2. Propriété caractéristique 602
   4.3. Autres façons d'obtenir la signature de σ 603
5. Bilan 604

30 Déterminants 607
1. Problèmes 608
2. Applications multilinéaires 609
   2.1. Définitions 609
   2.2. Expression d'une forme n-linéaire alternée relativement à une base donnée 610
3. Déterminant 611
   3.1. Déterminant de n vecteurs 611
   3.2. Déterminant d'un endomorphisme 613
   3.3. Déterminant d'une matrice 614
   3.4. Conséquences pratiques pour le calcul des déterminants 616
4. Calculs et applications des déterminants 617
   4.1. Formule de Cramer pour inverser un système 617
   4.2. Déterminant de matrices par blocs 617
   4.3. Développement suivant une ligne ou une colonne 617
   4.4. Calcul de l'inverse 620

   4.5. Déterminant comme fonction polynomiale 621
5. Bilan 622

VII Polynômes et fractions rationnelles 625

31 Structure algébrique de l'ensemble des polynômes 627
1. Problèmes 628
2. L'algèbre $\mathbb{K}[X]$ 629
   2.1. Construction 629
   2.2. $\mathbb{K}[X]$ comme $\mathbb{K}$ espace-vectoriel 629
   2.3. $\mathbb{K}[X]$ comme anneau 630
   2.4. Composée 631
   2.5. Remarques sur le corps $\mathbb{K}$ 632
3. Degré 633
   3.1. Définition 633
   3.2. Arithmétique des degrés 633
   3.3. Intégrité de $\mathbb{K}[X]$ et éléments inversibles 634
   3.4. Valuation 635
4. Dérivation d'un polynôme 635
   4.1. Définition 635
   4.2. Dérivation d'opérations polynomiales 636
   4.3. Dérivation d'ordre supérieur 637
   4.4. Applications 637
5. Bilan 639

32 Fonctions polynomiales et racines 641
1. Problèmes 642
2. Fonctions polynomiales et racines 643
   2.1. Fonctions polynomiales 643
   2.2. Racines d'un polynôme 643
   2.3. Nombres maximales de racines et degré de P 644
3. Interpolation de Lagrange 645
   3.1. Présentation du problème et polynômes de Lagrange . . 645
   3.2. Interpolation (de Lagrange) 646
4. Racines multiples et formule de Taylor 647
   4.1. Formules de Taylor (polynômiale) 647
   4.2. Multiplicité d'une racine 648
5. Relations coefficients-racines 649
   5.1. Polynôme scindé 649
   5.2. Fonctions symétriques élémentaires 649
   5.3. Applications 650
6. Théorème fondamental de l'algèbre 652
7. Bilan 652

33 L'anneau euclidien des polynômes 655
1. Problèmes 656
2. Division euclidienne dans $\mathbb{K}[X]$ 657
   2.1. Multiples d'un polynômes 657
   2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$ 658
   2.3. Nature de $\mathbb{K}[X]$ 659
3. Plus Grand Commun Diviseur 660
   3.1. Heuristique 660
   3.2. Algorithme d'Euclide et coefficients de Bézout 660
   3.3. PGCD 661
   3.4. Lemme de Gauss et facteurs relativement premiers 663
   3.5. Interprétation avec racines 664
   3.6. PGCD de plusieurs polynômes 665
4. Plus Petit Commun Multiple 666

4.1. Caractérisation essentielle . . . 666
4.2. Relation PGCD/PPCM . . . 667
5. Polynômes irréductibles . . . 668
5.1. Décomposition unique en produit d'irréductibles . . . 668
5.2. Décomposition dans $\mathbb{C}[X]$ . . . 670
5.3. Décomposition dans $\mathbb{R}[X]$ . . . 671
6. Bilan . . . 673

34 Le corps des fractions de l'anneau intègre des polynômes 675
1. Problèmes . . . 676
2. $\mathbb{K}(X)$, corps des fractions de $\mathbb{K}[X]$ anneau intègre . . . 676
2.1. Construction de $\mathbb{K}(X)$ . . . 676
2.2. Représentant irréductible. Degré et pôle . . . 677
2.3. Fonction rationnelle . . . 678
2.4. Dérivation . . . 678
3. Décomposition en éléments simples des fractions rationnelles . 679
3.1. Partie entière . . . 679
3.2. Principe de décomposition sur un corps $\mathbb{K}$ . . . 679
3.3. Application de la décomposition sur le corps $\mathbb{C}$ . . . 682
3.4. Application de la décomposition sur le corps $\mathbb{R}$ . . . 682
4. Bilan . . . 683

VIII Probabilités 685

35 Probabilités sur un univers fini 687
1. Problème . . . 688
2. Vocabulaire des expériences aléatoires . . . 689
2.1. Modélisation en probabilité . . . 689
2.2. Expérience aléatoire . . . 689
2.3. Evénements . . . 690
3. Espaces probabilisés finis . . . 691
3.1. Définitions . . . 691
3.2. Propriétés . . . 692
3.3. Suite (dé)croissante d'événements . . . 693
3.4. Exemples de probabilité . . . 694
3.5. Loi uniforme et simulation avec Python . . . 696
4. Conditionnement et indépendance . . . 697
4.1. Conditionnement . . . 697
4.2. Indépendance en probabilité . . . 704
5. Bilan . . . 707

36 Variables aléatoires (cas Ω fini) 709
1. Problèmes . . . 710
2. Variable aléatoire . . . 711
2.1. Quelques définitions . . . 711
2.2. Loi de probabilité . . . 712
2.3. Lois usuelles . . . 715
3. Couples de variables aléatoires . . . 716
4. Indépendance . . . 719
4.1. Indépendance de deux variables aléatoires . . . 719
4.2. Indépendance de plusieurs variables aléatoires . . . 719
4.3. Opération de variables aléatoires (indépendantes) . . . 722
4.4. Suite de variables aléatoires . . . 724
5. Moments d'une variable aléatoire réelle finie . . . 724
5.1. Espérance . . . 724
5.2. Variance (d'une variable aléatoire) . . . 728
5.3. Covariance (de deux variables aléatoires) . . . 731
6. Bilan . . . 734

IX Analyse (2) 737

37 Intégrale(s) (sur un segment) 739
1. Problème . . . 740
2. « Construire » l'intégrale. Préalable . . . 741
2.1. Rappels calculatoires . . . 741
2.2. « Vu de loin » . . . 742
2.3. Quelques rappels de topologie sur $\mathbb{R}$ . . . 744
2.4. Subdivision d'un segment de $\mathbb{R}$ . . . 744
3. Construction de l'intégrale . . . 748
3.1. Classes de fonctions à intégrer . . . 748
3.2. Somme de Cauchy/Riemann associée à f sur D . . . 752
3.3. Intégrales d'une fonction . . . 754
4. Espaces et sous-espaces des fonctions intégrables, ou : Qui est intégrable? . . . 761
4.1. Notations . . . 761
4.2. Passage à la limite des propriétés de somme de Riemann 761
4.3. Fermeture par convergence uniforme . . . 762
4.4. Théorèmes fondamentaux de l'analyse . . . 764
4.5. Bilan en termes d'espaces vectoriels croissants . . . 767
5. L'intégrale comme un « outil puissant » de l'analyse . . . 768
5.1. Relation de Chasles . . . 768
5.2. « Contrôle » par intégration . . . 773
5.3. Extension aux fonctions à valeurs complexes . . . 775
5.4. Formules de Taylor . . . 776
6. Bilan . . . 778

38 Séries numériques 781
1. Problèmes . . . 782
2. Généralités . . . 783
2.1. Définitions . . . 783
2.2. Propriétés . . . 784
2.3. Telescopage . . . 785
2.4. Opérations pour des séries convergentes . . . 787
2.5. Un cas classique : les séries de signe alterné . . . 787
3. Séries à termes positifs . . . 789
3.1. Majoration des sommes partielles . . . 789
3.2. Comparaison des séries à termes positifs . . . 790
3.3. Exploitation des séries de Riemann . . . 791
3.4. Séries absolument convergentes . . . 792
4. Quelques méthodes d'étude . . . 793
4.1. Plan d'étude . . . 793
4.2. Comparaison série-intégrale . . . 793
4.3. Séries de référence . . . 794
5. Bilan . . . 797

39 Familles sommables 801
1. Problème . . . 802
2. Somme de famille de réels positifs . . . 802
2.1. Définition . . . 803
2.2. Cas $I = \mathbb{N}$ . . . 803
2.3. Cas $I = \mathbb{N}^2$ . . . 804
2.4. Comparaisons . . . 805
2.5. Sommation par suite croissante d'ensembles . . . 806
2.6. Sommation par paquets et théorème de Fubini . . . 808
2.7. Enoncé dans $\overline{\mathbb{R}}_+ = [0, +\infty]$ . . . 811
3. Familles complexes sommables . . . 812
3.1. Définition . . . 812
3.2. Critère de sommabilité et calcul de somme . . . 812

3.3. Espace vectoriel $\ell^1(D,\mathbb{K})$ . . . 813
3.4. Transfert de propriétés sur $\ell^1(D,\mathbb{K})$ . . . 814
3.5. Sommation par paquets et Fubini . . . 816
3.6. Application : Produit de Cauchy . . . 819
4. Bilan . . . 820

40 Fonctions de deux variables 823
1. Problèmes . . . 824
2. Topologie . . . 825
2.1. Le cadre : espace vectoriel normé . . . 825
2.2. Initiation à la topologie sur un espace normé . . . 829
2.3. Topologie relative . . . 831
2.4. Compact . . . 832
2.5. Adhérences et intérieurs . . . 834
3. Continuité . . . 835
3.1. Limite . . . 835
3.2. Critère de continuité (ou non) à l'aide de suites . . . 838
3.3. Exemple d'applications continues . . . 839
3.4. Continuité sur un compact . . . 841
3.5. Représentation graphique . . . 841
4. Calcul différentiel . . . 843
4.1. Développement limité. Différentiabilité . . . 843
4.2. Dérivées partielles . . . 844
4.3. Application de classe $\mathscr{C}^1$ . . . 845
4.4. Règle de la chaine . . . 848
5. Visualisation et optimisation . . . 851
5.1. Tangente à une courbe, à une surface . . . 851
5.2. Interprétation physique du gradient . . . 854
5.3. Optimum libre . . . 855
5.4. Optima liés . . . 857
6. Bilan . . . 858

A Suite de variable aléatoire. Convergence (HP) 863
1. Problèmes . . . 864
2. Suite de variable aléatoire . . . 865
2.1. Suite de variables aléatoires . . . 865
2.2. Exemples de convergence de variable aléatoire . . . 865
3. Différents modes de convergence . . . 866
3.1. convergence presque sûre . . . 866
3.2. Convergence en probabilité . . . 869
3.3. Lien entre ces deux convergences de variables aléatoires 869
3.4. Convergence en loi . . . 870
4. Loi (faible) des grands nombres et estimateurs . . . 872
4.1. Lois des grands nombres . . . 872
4.2. Estimateurs . . . 872
5. Théorème limite central . . . 874
5.1. Rappels sur la loi normale . . . 874
5.2. Enoncé . . . 875
5.3. Intervalle de confiance . . . 876
6. Bilan . . . 877

B Fonctions holomorphes 879
1. Problèmes . . . 880
2. Holomorphie = Dérivation complexe . . . 881
2.1. Fonctions holomorphes . . . 881
2.2. Stabilité et premiers exemples . . . 882
2.3. Condition de Cauchy-Riemann . . . 883
2.4. Fonction analytique e(s)t fonction holomorphe . . . 884
3. Chemins dans le plan complexe et intégrale curviligne . . . 885

3.1. Arc du plan . . . 885
3.2. Intégration le long d'un chemin . . . 886
3.3. Longueur d'une courbe et majoration . . . 888
4. Théorème(s) de Cauchy . . . 889
4.1. Indice de Cauchy . . . 889
4.2. Lemme de Goursat et holomorphie . . . 890
4.3. Petit détour : Formule de Green-Riemann . . . 893
5. Théorème des résidus . . . 894
5.1. Principe du théorème des résidus . . . 894
5.2. Calculer les résidus . . . 896
5.3. Applications (aux calculs d'intégrales immondes et sommes effrayantes) . . . 896
6. Prolongement analytique . . . 898
6.1. Zéros d'une fonction holomorphe . . . 898
6.2. Prolongement analytique . . . 899
6.3. Fonctions à singularités. Vers les surfaces de Riemann . . 900
7. Bilan . . . 901