Les beaux théorèmes de Sup (et même plus)

20 mars 2024

Table des matières

1 Calcul algébrique

1.1 Sommes

1.1.1 Sommes d'entiers et de puissances d'entiers.

Première sommes de Newton : pour tout entier naturel n :

$$\sum_{k=0}^{n} k^0 = n+1$$

$$\sum_{k=0}^{n} k = \frac{n.(n+1)}{2}$$

$$\sum_{k=0}^{n} k^2 = \frac{n.(n+1).(2.n+1)}{6}$$

$$\sum_{k=0}^{n} k^3 = \left(\frac{n.(n+1)}{2}\right)^2$$

La première formule est une évidence, il suffit de compter les termes.

On rappelle que k^0 vaut 1, même pour k égal à 0. L'entier 0^0 dénombre les applications d'un ensemble à 0 élément(s) dans lui même, et il y en a une, c'est l'identité. Ce qui est une forme indéterminée, c'est $(o(1))^{o(1)}$ au sens des limites de suites ou de fonctions.

On peut démontrer les autres par récurrence sur n, mais on va proposer ici d'autres preuves.

Pour tout n, on pose $A_n = \sum_{k=0}^{n} k$, **et** $B_n = \sum_{k=0}^{n} k^2$, $C_n = \sum_{k=0}^{n} k^3$.

Dans A_n, on fait un renversement d'indice : $p = n - k$. Quand k va de 0 à n, l'entier p va de n à 0.

On a donc $A_n = \sum_{p=0}^{n} (n-p)$ que l'on sépare en $A_n = \sum_{p=0}^{n} n - \sum_{p=0}^{n} p$. La somme $\sum_{p=0}^{n} n$ vaut $n.(n+1)$ *(nombre de termes)*. La somme $\sum_{p=0}^{n} p$ est encore A_n *(variable de sommation muette)*. On a donc $A_n = n.(n+1) - A_n$,

qui donne bien $A_n = \dfrac{n.(n+1)}{2}$.

Pour calculer B_n, on calcule de deux façons $C_{n+1} - C_n$.
Par définition de $\sum_{k=0}^{n+1}$, on trouve déjà $(n+1)^3$.
Mais c'est aussi $\sum_{k=1}^{n+1} k^3 - \sum_{k=0}^{n} k^3$ (dans la première somme, on peut sommer à partir de $k=1$, puisque le terme d'indice $k=0$ est nul). On ré-indexe la première en posant $p = k-1$:

$$C_{n+1} - C_n = \sum_{p=0}^{n} (p+1)^3 - \sum_{k=0}^{n} k^3$$

La seconde somme vaut aussi $\sum_{p=0}^{n} p^3$ puisque les variables sont muettes.

On a donc en fusionnant : $C_{n+1} - C_n = \sum_{p=0}^{n} \left((p+1)^3 - p^3\right)$.
On développe par la formule du binôme :

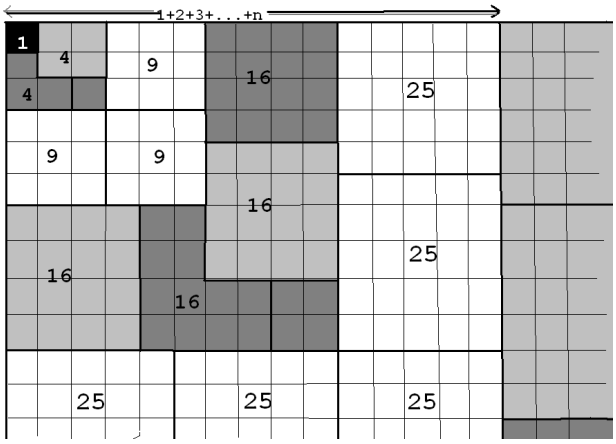
$$C_{n+1} - C_n = \sum_{p=0}^{n} \left(3.p^2 + 3.p + 1\right)$$

On sépare en trois sommes déjà nommées dans l'énoncé : $C_{n+1} - C_n = 3.B_n + 3.A_n + n + 1$
On égale les deux calculs : $(n+1)^3 = 3.B_n + 3.A_n + n + 1$, et on extrait $B_n = \dfrac{n.(n+1).(2.n+1)}{6}$ *(et c'est bien toujours un entier naturel)*.

Pour C_n, on définit la matrice de terme général $i.k$: $\begin{matrix} 1.1 & 1.2 & 1.3 & \dots & 1.n \\ 2.1 & 2.2 & 2.3 & \dots & 2.n \\ 3.1 & 3.2 & 3.3 & \dots & 3.n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n.1 & n.2 & n.3 & \dots & n.n \end{matrix}$ et on en somme tous les termes.
Il s'agit de $\sum_{\substack{i\leqslant n \\ k\leqslant n}} i.k$ qui se sépare *(indépendance des variables de sommation)* en $\left(\sum_{i\leqslant n} i\right).\left(\sum_{k\leqslant n} k\right)$. Les deux sommes sont égales, c'est $\left(A_n\right)^2$, soit encore justement $\left(\dfrac{n.(n+1)}{2}\right)^2$.
Mais on peut aussi sommer par zones visuellement délimitées comme suit

$1.1 \ . \ . \ \dots \ .$ $. \ . \ . \ \dots \ .$ $. \ . \ . \ \dots \ .$ $\vdots \ \vdots \ \vdots \ \ddots \ \vdots$ $. \ . \ . \ \dots \ .$	$. \ 1.2 \ . \ \dots \ .$ $2.1 \ 2.2 \ . \ \dots \ .$ $. \ . \ . \ \dots \ .$ $\vdots \ \vdots \ \vdots \ \ddots \ \vdots$ $. \ . \ . \ \dots \ .$	$. \ . \ 1.3 \ \dots \ .$ $. \ . \ 2.3 \ \dots \ .$ $3.1 \ 3.2 \ 3.3 \ \dots \ .$ $\vdots \ \vdots \ \vdots \ \ddots \ \vdots$ $. \ . \ . \ \dots \ .$	jusqu'à	$. \ . \ . \ \dots \ 1.n$ $. \ . \ . \ \dots \ 2.n$ $. \ . \ . \ \dots \ 3.n$ $\vdots \ \vdots \ \vdots \ \ddots \ \vdots$ $n.1 \ n.2 \ n.3 \ \dots \ n.n$

Proprement, on écrit $\sum_{j=1}^{n} \Big(\sum_{Max(i,k)=j} i.k \Big)$.



A j fixé, une somme $\sum_{Max(i,k)=j} i.k$ est faite de deux sommes $\sum_{\substack{i=j\\k\leqslant j}} i.k + \sum_{\substack{k=j\\i<j}} i.k$ *(dans une des deux sommes, on accepte $i=k=j$, mais pas dans l'autre pour ne pas compter deux fois le même terme "en coin").*
On sort ce qui est indépendant de la variable de sommation :

$$\sum_{Max(i,k)=j} i.k = j.\sum_{k\leqslant j} k + j.\sum_{i<j} i$$

On utilise le résultat du calcul de A_j :

$$\sum_{Max(i,k)=j} i.k = j.\frac{j.(j+1)}{2} + j.\frac{(j-1).j}{2} = j^3$$

On a donc $\sum_{j=1}^{n}\Big(\sum_{Max(i,k)=j} i.k\Big) = \sum_{j=1}^{n} j^3 = C_n$.
On a donc bien finalement $(A_n)^2 = \sum_{\substack{i\leqslant n\\k\leqslant n}} i.k = C_n$.

1.1.2 Somme des premiers entiers impairs.

La somme des n premiers entiers impairs est égale au carré de n :

$$1+3+5+\ldots+(2.n-1) = \sum_{k=1}^{n}(2.k-1) = n^2$$

Méthode 1 : $\sum_{k=1}^{n}(2.k-1) = \sum_{\substack{0\leqslant j\leqslant 2.n\\ j=1[2]}} j = \sum_{j=0}^{2.n} j - \sum_{0\leqslant i\leqslant n} 2.i = \frac{2.n.(2.n+1)}{2} - 2.\frac{n.(n+1)}{2} = n^2$

Méthode 2 : $\sum_{k=1}^{n}(2.k-1) = 2.\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 = 2.\frac{n.(n+1)}{2} - n = n^2$

Méthode 3 : il y a n termes et la moyenne des extrêmes vaut $\frac{1+(2.n-1)}{2}$.

1	2	3	4	5	6
2	2	3	4	5	6
3	3	3	4	5	6
4	4	4	4	5	6
5	5	5	5	5	6
6	6	6	6	6	6

Une preuve dénombre aussi le contenu d'un carré de taille n sur n, en voyant des bandes de longueur 1, 3, 5 et ainsi de suite.

1.1.3 Série géométrique.

Dans un corps commutatif, pour tout élément a différent du neutre, pour tout entier naturel n, on a

$$1 + a + a^2 + \ldots + a^n = \sum_{k=0}^{n} a^k = \frac{1 - a^{n+1}}{1 - a}$$

Il existe une démonstration par récurrence sur n.
Mais la meilleure solution est le produit en croix.
Le produit $(1-a).\sum_{k=0}^{n} a^k$ vaut $\sum_{k=0}^{n} a^k - a^{k+1}$ par distributivité, puis se simplifie en $\sum_{k=0}^{n} a^k - \sum_{k=0}^{n} a^{k+1}$.
Un télescopage ou une ré-indexation donne $1 - a^{n+1}$.
Il ne reste qu'à diviser par $1 - a$ inversible.

Si la multiplication n'est pas commutative (et donc la division non plu), on ne sait quel sens donner à $\frac{1-a^{n+1}}{1-a}$; est ce $(1-a^{n+1}).(1-a)^{-1}$ ou $(1-a)^{-1}.(1-a^{n+1})$.
La formule se généralise à $\sum_{k=p}^{q} a^k$ ou $\sum_{k=p}^{q} \alpha_k$ où $\alpha_i)$ est une suite géométrique de raison a.
On conseillera de retenir $\frac{(premier\ terme\ ecrit) - (premier\ terme\ a\ venir)}{1 - raison}$ plutôt que de compter le nombre de termes.
Pour rappel, de p à q (inclus) il y a $q + 1 - p$ termes, ce que l'informaticien sait par le fait qu'il s'agit de $range(p,\ q+1)$.

Sous forme de produit en croix, la formule se généralise avec deux éléments a et b permutables [1] dans un anneau $(A, +, .)$:

$$(a-b).\Big(\sum_{k=0}^{n} a^{n-k}.b^k\Big) = a^{n+1} - b^{n+1}$$

Il suffit là encore de développer et télescoper.
C'est la formule générale de

$$(a-b).(a+b) = a^2 - b^2,\ (a-b).(a^2 + a.b + b^2) = a^3 - b^3$$

$$(a-b).(a^3 + a^2.b + a.b^2 + b^3) = a^4 - b^4$$

dont il existe aussi les versions

$$(a+b).(a^2 - a.b + b^2) = a^3 + b^3 \text{ et } (a+b).(a^4 - a^3.b + a^2.b^2 - a.b^3 + b^4) = a^5 + b^5$$

et ainsi de suite.

On évitera de confondre ces formules avec la formule du binôme $\sum_{k=0}^{n} \binom{n}{k}.a^{n-k}.b^k$.

Le cours de Prépas fait aussi usage de la dérivée de la série géométrique, mais la formule n'est pas à retenir, juste à retrouver.

1. c'est à dire $a.b = b.a$, par exemple si la multiplication est commutative ou si l'un des deux est le neutre

1.1.4 Noyau de Dirichlet (hors-programme mais classique).

Noyau dit de Dirichlet : pour tout réel θ qui n'est pas multiple pair de π

$$\frac{1}{2}+\sum_{k=1}^{n}\cos(k.\theta)=\frac{\sin\left(\frac{2.n+1}{2}.\theta\right)}{2.\sin\left(\frac{\theta}{2}\right)}$$

On prend θ qui n'appartient pas à $\{2.k.\pi \mid k\in\mathbb{Z}\}$ *(son cosinus ne vaut pas* 1 *et* $\sin(\theta/2)$ *est non nul)*.
On part de la somme $\frac{1}{2}+\sum_{k=1}^{n}\cos(k.\theta)$ qu'on écrit $\frac{1}{2}+\sum_{k=1}^{n}\frac{e^{-i.k.\theta}+e^{i.k.\theta}}{2}$.
On met $\frac{1}{2}$ en facteur et on obtient

$$\frac{1}{2}\Big(\sum_{k=1}^{n}e^{-i.k.\theta}+1+\sum_{k=1}^{n}e^{i.k.\theta}\Big)$$

qui donne même $\frac{1}{2}\Big(\sum_{k=-n}^{n}e^{i.k.\theta}\Big)$.
On reconnaît une série géométrique de premier terme $e^{-i.n.\theta}$, de terme à venir $e^{i.(n+1).\theta}$ et de raison $e^{i.\theta}$ *(différente de* 1*)*.
On l'écrit donc $\frac{e^{-i.n.\theta}-e^{i.(n+1).\theta}}{2.(1-e^{i.\theta})}$.
On multiplie haut et bas par $e^{-i.\theta/2}$ et on a $\frac{e^{-i.(n+1/2).\theta}-e^{i.(n+1/2).\theta}}{2.(e^{-i.\theta/2}-e^{i.\theta/2})}$.
En utilisant $e^{-i.\alpha}-e^{i.\alpha}=-2.i.\sin(\alpha)$ on arrive à $\frac{2.\sin((n+1/2).\theta)}{4.\sin(\theta/2)}$.

Une autre preuve est possible par produit en croix, en utilisant $2.\sin(a).\cos(b)=\sin(a+b)-\sin(a-b)$ et une somme télescopique.

1.2 Coefficients binomiaux, formule du binôme.

1.2.1 Relation de Pascal.

En prenant la définition $\binom{n}{k}=\frac{n!}{k!.(n-k)!}$ ou la définition « nombre de façons de choisir k individus parmi n », on a

$$\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$$

Cette formule permet de remplir de proche en proche les lignes du triangle de Pascal.
Avec la convention sur les binomiaux aberrants $\binom{n}{k}=0$ si $k>n$, cette formule est encore valable.

On peut évidemment réduire au dénominateur commun la somme

$$\frac{n!}{(n-k)!.k!}+\frac{n!}{(n-k-1)!.(k+1)!}=\frac{n!}{(n-k)!.(k+1)!}.\Big((k+1)-(n-k)\Big)$$

Mais on peut aussi dénombrer le nombre de groupes de $k+1$ individus au sein d'un ensemble $\{a_0, \dots a_n\}$ de $n+1$ individus.
Il y a celles ne contenant pas a_0 : k individus parmi n.
Il y a celles contenant a_0 : il reste à choisir $k-1$ individus parmi n.

1.2.2 Formule de Zhu-Shi-Jie (hors programme).

Pour tout couple d'entiers naturels $(n,\ k)$, on a

$$\sum_{i=0}^{n} \binom{i}{k} = \binom{n+1}{k+1}$$

1							
1	1						
1	2	1					
1	3	3	**1**				
1	4	6	**4**	1			
1	5	10	**10**	5	**1**		
1	6	15	**20**	15	**6**	1	
1	7	21	**35**	35	**21**	7	1
1	8	28	**56**	70	**56**	28	8
1	9	36	**94**	126	126	**94**	36
1	10	45	**120**	210	252	210	120
1	11	55	165	**330**	462	462	330

Il s'agit d'une somme en colonne, qui ne commence vraiment qu'à $\binom{k}{k}$, les termes comme $\binom{0}{k}$ étant nuls.

La preuve la plus simple utilise la formule de Pascal « à l'envers » :

$$\sum_i \binom{i}{k} = \sum_i \binom{i+1}{k+1} - \binom{i}{k+1}$$

et un télescopage.

Il existe aussi une preuve par dénombrement.

1.2.3 Formule comité président.

Pour tout couple d'entiers naturels (n, p) avec $p \leqslant n$, on a

$$\binom{n}{p}.p = n.\binom{n-1}{p-1}$$

On peut évidemment démontrer cette formule en revenant à la définition « quotient de factorielles ».
Mais la démonstration probabiliste dénombre le nombre de façons (au sein d'un groupe de n individus) de former des groupes de p individus avec un président.
Première approche : on choisit les n individus (ici $\binom{n}{p}$), puis les p individus choisissent parmi eux un président (ici p choix).

Deuxième approche : on choisit un président au sein du grand groupe (ici n choix), puis on le complète avec $p-1$ quidams pour le comité (ici $\binom{n-1}{p-1}$ puisqu'il ne reste que $n-1$ individus).

On peut généraliser aux comités de p individus avec k délégués : $\binom{n}{p}.\binom{p}{k} = \binom{n}{k}.\binom{n-k}{p-k}$.

Il existe d'autres formules pour avancer en ligne, en colonne, en diagonale :
En colonne : $\binom{n+1}{k} = \frac{n+1}{n-k+1}.\binom{n}{k}$ et en diagonale $\binom{n+1}{k+1} = \frac{n+1}{k+1}.\binom{n}{k}$:

$\binom{n}{k}$	$\rightarrow \times \frac{n-k}{k+1}$	$\binom{n}{k+1}$
$\downarrow \times \frac{n+1}{n-k+1}$	$\searrow \times \frac{n+1}{k+1}$	
$\binom{n+1}{k}$		$\binom{n+1}{k+1}$

1.2.4 Formule du binôme dans un anneau commutatif.

Dans un anneau commutatif (typiquement $(\mathbb{R}, +, .)$ ou $(\mathbb{C}, +, .)$), on a pour tout couple $(a,\ b)$ et tout entier naturel n :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}.a^{n-k}.b^k = \sum_{p=0}^{n} \binom{n}{p}.a^p.b^{n-p} = \sum_{i+j=n} \frac{n!}{i!.j!}.a^i.b^j$$

La formule est initialisée pour n égal à 0, 1 et 2.
Supposons la vraie pour un n donné et développons alors

$$a.(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}.a^{n+1-k}.b^k$$

mais aussi

$$b.(a+b)^n = \sum_{i=0}^{n} \binom{n}{i}.a^{n-i}.b^{i+1} = \sum_{k=1}^{n} \binom{n}{k-1}.a^{n+1-k}.b^k$$

On peut fusionner les deux sommes au moins sur leur partie commune

$$a.(a+b)^n + b.(a+b)^n = 1.a^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right).a^{n+1-k}.b^k + 1.b^{n+1}$$

On regroupe par la formule de ascal au milieu et on reformule les deux termes du bout pour pouvoir les incorporer :

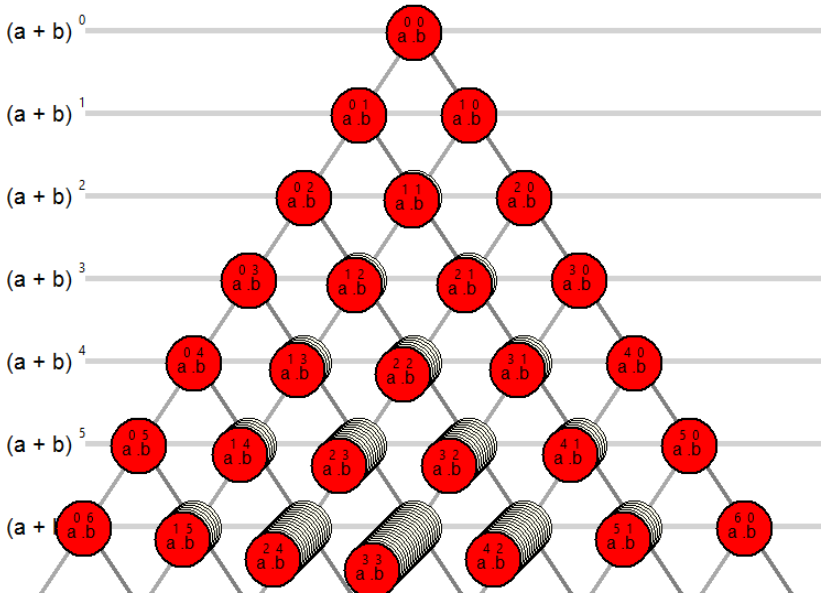
$$a.(a+b)^n + b.(a+b)^n = \binom{n+1}{0}.a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k}.a^{n+1-k}.b^k + \binom{n+1}{n+1}.b^{n+1}$$

Il n'y a plus qu'à remettre les deux termes dans la somme et à réécire le premier membre comme $(a+b).(a+b)^n$.

Une preuve par dénombrement est possible.

Pour passer d'une ligne à la suivante, on multiplie par a (déplacement à gauche) et par b (déplacement à droite).

On voit alors les jetons se superposer suivant la règle de Pascal.



1.2.5 Formule du multinôme dans un anneau commutatif.

La formule du binôme se généralise à un plus grand nombre de termes :

$$(a+b+c)^n = \sum_{i+j+k=n} \frac{n!}{i!.j!.k!}.a^i.b^j.c^k$$

$$(a+b+c+d)^n = \sum_{i+j+k+l=n} \frac{n!}{i!.j!.k!.l!}.a^i.b^j.c^k.d^l$$

jusqu'à $\left(\sum_{k=1}^{p} a_k\right)^n = \sum_{i_1+\ldots+i_p=n} \frac{n!}{i_1!\ldots i_p!}.(a_1)^{i_1}\ldots(a_p)^{i_p}$ **qu'on peut écrire de manière encore plus rigoureuse.**

On effectue une récurrence sur le nombre p de termes dans la somme.
C'est ainsi qu'on a

$$(a+b+c)^3 = a^3+b^3+c^3+3.(a^2.b+a^2.c+b^2.a+b^2.c+c^2.a+c^2.b)+6.(a.b.c)$$

correspondant à $(i,j,k)=(3,0,0)$, puis $(i,j,k)=(2,1,0)$ et $(i,j,k)=(1,1,1)$ et leurs variantes.

$$(a+b+c)^4 = \begin{array}{c} a^4+b^4+c^4 \\ +6.(a^2.b^2+a^2.c^2+b^2.c^2) \end{array} \quad \begin{array}{c} +4.(a^3.b+a^3.c+b^3.a+b^3.c+c^3.a+c^3.b) \\ +12.(a^2.b.c+b^2.a.c+c^2.a.b) \end{array}$$

correspondant à $(i,j,k)=(4,0,0)$, puis $(i,j,k)=(3,1,0)$ et $(i,j,k)=(2,2,0)$ et leurs variantes.

1.2.6 Formule de Leibniz pour des applications n fois dérivables.

Si a et b sont deux applications au moins n fois dérivables, alors $a \times b$ l'est aussi, et de plus

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

La notation $a^{(k)}$ signifie a déivée k fois, avec la convention naturelle $a^{(0)} = a$ et $a^{(n+1)} = (a^{(n)})' = (a')^{(n)}$ qu'il faudrait démontrer par récurrence sur n.

La formule de Leibniz à l'ordre 0 dit juste « si a et b existent, alors $a \times b$ existe et on a

$$a \times b = (a \times b)^{(0)} = 1.a^{(0)} \times b^{(0)}$$

Supposons pour un entier n donné quelconque la formule vraie à l'ordre n, et ajoutons l'hypothèse : a et b sont $n+1$ fois dérivables.
Chaque terme de la somme $\sum_{k=0}^{n} \binom{n}{k} \times a^{(n-k)} \times b^{(k)}$ est dérivable au oins une fois de plus.
En effet, $(a^{(n-k)} \times b^{(k)})' = (a^{(n-k)})' \times b^{(k)} + a^{(n-k)} \times (b^{(k)})'$ et $a^{(n-k)}$ et $b^{(k)}$ sont bien dérivables au moins une fois de plus.
En utilisant la linéarité de la dérivation, on a donc

$$((a \times b)^{(n)})' = \sum_{k=0}^{n} \binom{n}{k} \times \left(a^{(n-k+1)} \times b^{(k)} + a^{(n-k)} \times b^{(k+1)}\right)$$

si l'on se fie au calcul précédent.

On sépare en deux sommes

$$(a \times b)^{(n+1)} = \sum_{k=0}^{n} \binom{n}{k} \times a^{(n-k+1)} \times b^{(k)} + \sum_{k=0}^{n} \binom{n}{k} \times a^{(n-k)} \times b^{(k+1)}$$

On décalle dans la deuxième somme en posant $k' = k+1$

$$(a \times b)^{(n+1)} = \sum_{k=0}^{n} \binom{n}{k} \times a^{(n-k+1)} \times b^{(k)} + \sum_{k'=1}^{n+1} \binom{n}{k'-1} \times a^{(n+1-k')} \times b^{(k')}$$

Les variables étant muettes, on peut fusionner les deux sommes en une au moins sur la partie commune

$$(a \times b)^{(n+1)} = \binom{n}{0} \times a^{(n+1)} \times b^{(0)} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1}\right) \times a^{(n-k+1)} \times b^{(k)} + \binom{n}{n} \times a^{(0')} \times b^{(n+1)}$$

La partie centrale donne $\binom{n+1}{k} \times a^{(n+1-k)} \times b^{(k)}$ et les deux termes du bout peuvent s'écrire $\binom{n+1}{0} \times a^{(n+1)} \times b^{(0)}$ et $\binom{n+1}{n+1} \times a^{(0)} \times b^{(n+1)}$ et compléter la somme.

On notera qu'avec les applications $a = t \longrightarrow e^{\alpha.t}$ et $b = t \longrightarrow e^{\beta.t}$ dont ls dérivées sont faciles à calculer, la formule de Leibniz redonne la formule du binôme dans $\mathbb{R}$ ou même $\mathbb{C}$.

1.3 Calcul dans $\mathbb{R}$ et $\mathbb{C}$.

1.3.1 Inégalité triangulaire dans $\mathbb{R}$.

Pour tout couple de réels $(a,\ b)$, on a $|a+b| \leqslant |a| + |b|$,
en rappelant, si nécessaire : $|a| = Max(a,\ -a)$ et $|a|^2 = a^2$.

On se donne a et b et on compare escarrés des deux réels positifs :

$$\begin{array}{rcccc} (a+b)^2 & = & a^2 & +b^2 & +2.a.b \\ (|a|+|b|)^2 & = & |a|^2 & +|b|^2 & +2.|a|.|b| \end{array}$$

Il suffit d'écrire $2.a.b \leqslant 2.|a.b| = 2.|a|.|b|$ pour avoir alors $(a+b)^2 \leqslant (|a|+|b|^2)$ et passer enfin à la racine.

1.3.2 Inégalité triangulaire dans $\mathbb{C}$.

Pour tout couple $(a,\ b)$ de complexes, on a $|a+b| \leqslant |a| + |b|$ (en rappelant $|z| = \sqrt{z.\overline{z}} = \sqrt{(\Re e(z))^2 + (\Im m(z))^2}$).

Soient a et b dans $\mathbb{C}$, alors :

$$\begin{aligned} |a+b|^2 &= (a+b.)\overline{(a+b)} \\ &= a.\overline{a} + a.b + b.\overline{a} + b.\overline{b} \\ &= |a|^2 + |b|^2 + (a.\overline{b} + \overline{a}.b) \\ &= |a|^2 + |b|^2 + (a.\overline{b} + \overline{a.\overline{b}}) \end{aligned}$$

Or on sait : $\Re e(z) = \dfrac{z+\overline{z}}{2}$, donc :

$$|a+b|^2 = |a|^2 + |b|^2 + 2.\Re e(a.b)$$

On a également $(|a|+|b|)^2 = |a|^2 + |b|^2 + 2|a.b|$.
De plus $\Re e(z) \leqslant |z|$. En effet, en posant $z = a + i.b$:

$$\begin{aligned} \Re(z) &= a \\ &\leqslant |a| = \sqrt{a^2} \\ &\leqslant \sqrt{a^2+b^2} = |z| \end{aligned}$$

Donc $2.\Re e(z) \leqslant 2.|a.\overline{b}| = 2.|a.b|$.
Finalement : $|a+b|^2 \leqslant (|a|+|b|)^2 \Rightarrow \boxed{|a+b| \leqslant |a| + |b|}$

1.3.3 Seconde inégalité triangulaire.

Deuxième inégalité triangulaire : pour tout couple de complexes $(a,\ b)$, on a

$$\big||a| - |b|\big| \leqslant |a-b|$$

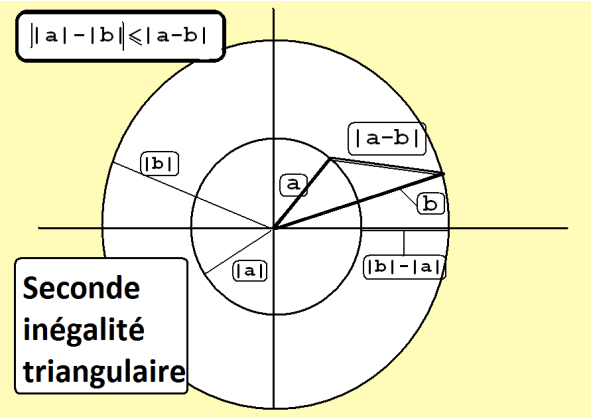
On écrit pour a et b donnés la première inégalité triangulaire :

$$|a| = |a - b + b| \leqslant |a - b| + |b|$$
$$|b| = |b - a + a| \leqslant |b - a| + |a|$$

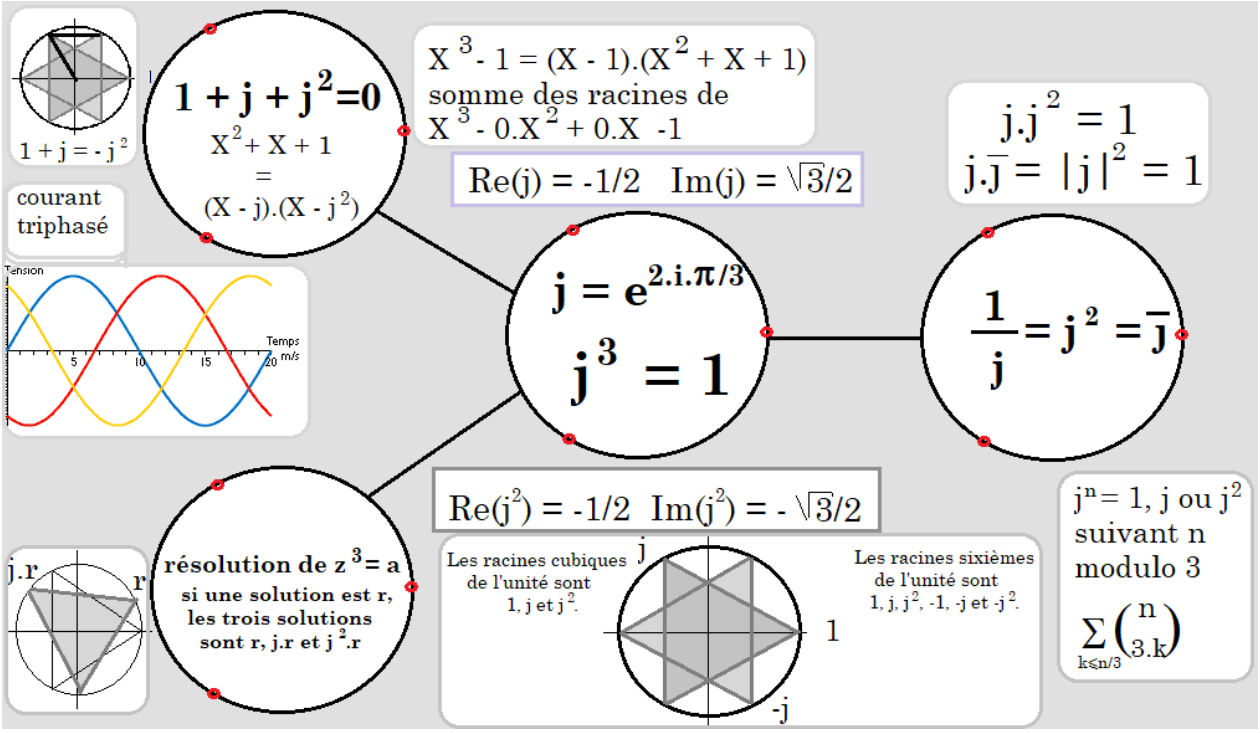
On fait passer de l'autre côté dans les deux :

$$|a| - |b| \leqslant |a - b|$$
$$|b| - |a| \leqslant |a - b|$$

Or, le réel positif $\big||a| - |b|\big|$ est l'un des deux nombres $|a| - |b|$ ou son opposé $|b| - |a|$.
Qu'il soit l'un ou l'autre, il est plus petit que $|a - b|$.



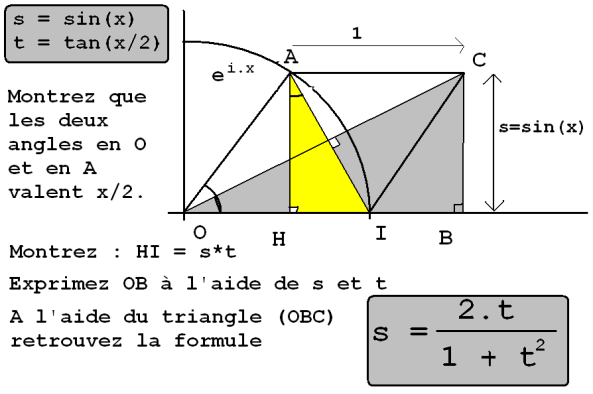
1.3.4 Le nombre j , racine cubique de l'unité.



1.3.5 Arc moitié.

Pour θ entre 0 et $2.\pi$, le complexe $1 + e^{i.\theta}$ a pour module $2.\cos(\theta/2)$ et pour argument $\theta/2$.

Graphiquement, $1+e^{i.\theta}$ a pour argument $\theta/2$ et on mesure son demi module dans un triangle rectangle.



Proprement, on factorise :

$$e^{i.\theta}+1=e^{i.\theta/2}.(e^{i.\theta/2}+e^{-i.\theta/2})=2.\cos(\theta/2).e^{i.\theta/2}$$

Le module est donc bien $2.\cos(\theta/2)$ (positif si on a bien pris θ entre $-\pi$ et π).
L'argument est $\theta/2$.
On factorise de même :

$$e^{i.\alpha}+e^{i.\beta}=e^{i.\frac{\alpha+\beta}{2}}.(e^{i.\frac{\alpha-\beta}{2}}+e^{i.\frac{-\alpha+\beta}{2}})=2.\cos\left(\frac{\alpha-\beta}{2}\right).e^{i.\frac{\alpha+\beta}{2}}$$

En passant aux parties réelles et imaginaires, on retrouve les formules classiques :

$\cos(\alpha)+\cos(\beta)=2.\cos\left(\frac{\alpha-\beta}{2}\right).\cos\left(\frac{\alpha-\beta}{2}\right)$ et	$\sin(\alpha)+\sin(\beta)=2.\cos\left(\frac{\alpha-\beta}{2}\right).\sin\left(\frac{\alpha-\beta}{2}\right)$

1.3.6 Formules en tangente de l'arc moitié (premier sens).

Si θ n'est pas un multiple impair de π ($\theta\in\mathbb{R}-\{(2.k+1).\pi \mid k\in\mathbb{Z}\}$), on peut poser $t=\tan\left(\frac{\theta}{2}\right)$ et écrire

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

Pour la troisième, on interdit aussi à θ d'être un multiple impair de $\frac{\pi}{2}$ (existence de $\tan(\theta)$, ce qui revient d'ailleurs à interdire $t=\pm1$.

On notera que les deux quanités $\frac{1-t^2}{1+t^2}$ et $\frac{2.t}{1+t^2}$ restent « assez naturellement » entre -1 et 1, ce qui valide leur rôle en tant que sinus et cosinus.

Il suffit en effet d'étudier le signe de $1-\frac{1-t^2}{1+t^2}$ et autres $\frac{2.t}{1+t^2}-(-1)$ et d'y retrouver les identités remarquables cachées.
On peut aussi calculer la somme des carrés $\left(\frac{2.t}{1+t^2}\right)^2+\left(\frac{1-t^2}{1+t^2}\right)^2$ assez instructive.

Il suffit pour démontrer les formules de commencer par écrire $\cos^2(\theta/2)=\frac{1}{1+\tan^2(\theta/2)}$ qui n'est rien de plus qu'une formule de Pythagore.
Ensuite, on a

$$\sin(\theta)=\sin\left(2.\frac{\theta}{2}\right)=2.\sin\left(\frac{\theta}{2}\right).\cos\left(\frac{\theta}{2}\right)=2.\frac{\sin\left(\frac{\theta}{2}\right)}{\cos\left(\frac{\theta}{2}\right)}.\cos^2\left(\frac{\theta}{2}\right)$$

$$\cos(\theta)=\cos\left(2.\frac{\theta}{2}\right)=2.\cos^2\left(\frac{\theta}{2}\right)-1=2.\frac{1}{1+\tan^2\left(\frac{\theta}{2}\right)}-1$$

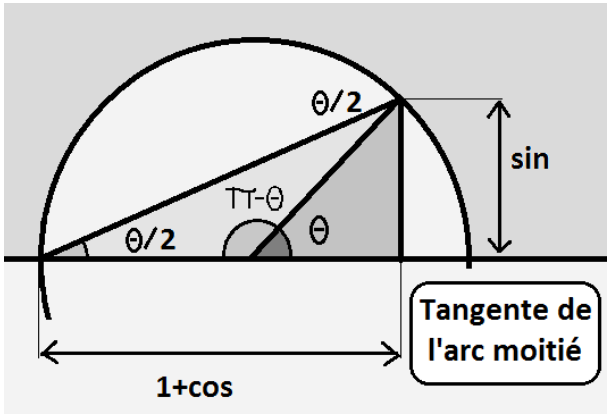
1.3.7 Formules en tangente de l'arc moitié (second sens).

Si θ n'est pas un multiple de π ($\theta \in \mathbb{R} - \{k.\pi \mid k \in \mathbb{Z}\}$), on a

$$\tan\left(\frac{\theta}{2}\right) = \frac{\sin(\theta)}{1+\cos(\theta)} = \frac{1-\cos(\theta)}{\sin(\theta)}$$

On peut partir du membre de droite et appliquer les formules précédentes.

On peut aussi exploiter le théorème de l'angle au centre (ou juste mesurer des angles), puis appliquer les formules dans le triangle rectangle.



1.3.8 Inégalité de Cauchy-Schwarz.

Soient deux vecteurs de $\mathbb{R}^n$: $(a_1, \dots a_n)$ et $(b_1, \dots b_n)$. Alors on a

$$\left|\sum_{k=1}^{n} a_k.b_k\right| \leqslant \sqrt{\sum_{k=1}^{n}(a_k)^2}.\sqrt{\sum_{k=1}^{n}(b_k)^2}$$

Si l'un des deux vecteurs est nul, on a une égalité directe. Inutile d'envisager ce cas.

On définit l'application

$$t \longrightarrow \sum_{k=1}^{n}(t.a_k + b_k)^2$$

de $\mathbb{R}$ dans $\mathbb{R}^+$. Son ensemble d'arrivée est effectivement inclus dans $\mathbb{R}^+$ car on a une somme de carrés de réels.
Si on développe chaque carré et sépare par linéarité, cette application est un trinôme du second degré en t de la forme $A.t^+ + 2.B.t + C$ avec $A = \sum_{k=1}^{n}(a_k)^2$, $B = \sum_{k=1}^{n} a_k.b_k$ et $C = \sum_{k=1}^{n}(b_k)^2$.
Comme ce trinôme est de signe constant (positif), son discriminant est négatif ou nul (c'est la contraposée de « discriminant positif implique change de signe entre les racines réelles »).
On a donc $B^2 - A.C \leqslant 0$ soit effectivement

$$\left(\sum_{k=1}^{n} a_k.b_k\right)^2 \leqslant \left(\sum_{k=1}^{n}(a_k)^2\right).\left(\sum_{k=1}^{n}(b_k)^2\right)$$

Il suffit de passer à la racine pour avoir l'inégalité demandée.

Il existe d'autres démonstrations avec quand même une somme de carrés de réels.

Variante. Pour f et g continues de $[\alpha,\ \beta]$ dans $\mathbb{R}$ on a

$$\Big(\int_\alpha^\beta f(t).g(t).dt\Big)^2 \leqslant \Big(\int_\alpha^\beta (f(t))^2.dt\Big).\Big(\int_\alpha^\beta (g(t))^2.dt\Big)$$

cette fois en étudiant $t \longrightarrow \displaystyle\int_\alpha^\beta (t.f(t)+g(t))^2.dt$.

Corolaire probabiliste. Si A est une variable aléatoire à valeurs dans $\mathbb{R}$ alors on a

$$E(A)^2 \leqslant E(A^2)$$

En notant a_k les valeurs prises par la variable aléatoire et p_k les probabilités positives $p_k = P(A = a_k)$, il suffit d'appliquer l'inégalité de Cauchy-Schwarz aux deux vecteurs $(\sqrt{p_1},\ldots,\sqrt{p_n})$ et $(a_1.\sqrt{p_1},\ldots,a_n\sqrt{p_n})$.
Le premier membre $\Big(\displaystyle\sum_{k=1}^n \sqrt{p_k}.a_k.\sqrt{p_k}\Big)^2$ est alors $(E(A))^2$.
Les deux facteurs du second membre sont $\displaystyle\sum_{k=1}^n(\sqrt{p_k})^2$ de valeur 1 et $\displaystyle\sum_{k=1}^n(a_k.\sqrt{p_k})^2$ dans lequel on reconnaît $E(A^2)$.

Corolaire géométrique. Pour nos deux vecteurs donnés $(a_1,\ldots,a_n)$ et $(b_1,\ldots,b_n)$ (supposés non nuls), le quotient

$$\frac{\displaystyle\sum_{k=1}^n (a_k.b_k)}{\sqrt{\displaystyle\sum_{k=1}^n (a_k)^2}.\sqrt{\displaystyle\sum_{k=1}^n (b_k)^2}}$$

est entre -1 et 1. On peut donc définir un angle θ dont il est le cosinus.
L'inégalité s'écrit alors

$$\frac{\overrightarrow{a}.\overrightarrow{b}}{||\overrightarrow{a}||\times||\overrightarrow{b}||} = \frac{\displaystyle\sum_{k=1}^n (a_k.b_k)}{\sqrt{\displaystyle\sum_{k=1}^n (a_k)^2}.\sqrt{\displaystyle\sum_{k=1}^n (b_k)^2}} = \cos(\theta)$$

puis $(\overrightarrow{a}.\overrightarrow{b}) = ||\overrightarrow{a}||\times||\overrightarrow{b}||\times\cos(\theta)$ qui généralise dans $\mathbb{R}^n$ la formule qui lie le produit scalaire au produit des normes.

1.3.9 Cas d'égalité dans l'inégalité de Cauchy-Schwarz.

En reprenant la démonstration de l'inégalité de Cauchy-Schwarz pour deux vecteurs non nuls $\overrightarrow{a} = (a_1,\ldots,a_n)$ et $\overrightarrow{b} = (b_1,\ldots,b_n)$, l'inégalité devient une égalité si et seulement si le discriminant du trinôme est nul.
Ceci signifie que le trinôme admet une racine (double) qu'on va noter t_0.
Pour cette racine, la somme $\displaystyle\sum_{k=1}^n (t_0.a_k - b_k)^2$ est nulle, ce qui ne laisse qu'une possibilité : $\forall k,\ t_0.a_k = b_k$.
Comme le réel t_0 ne dépend pas de k, on déduit $t_0.\overrightarrow{a} = -\overrightarrow{b}$.
Géométriquement, ceci traduit que les deux vecteurs sont colinéaires, et on a raisonné par équivalences.

1.3.10 Le produit matriciel est associatif.

Pour trois matrices A, B et C de formats compatibles, on a

$$(A.B).C = A.(B.C)$$

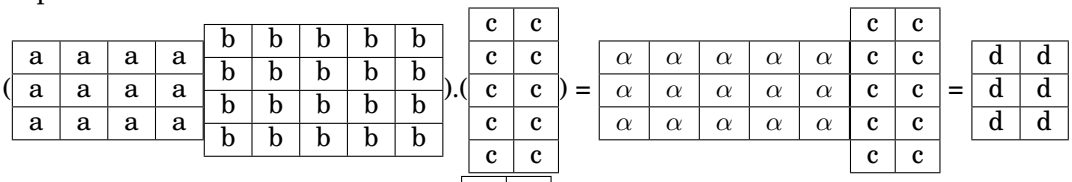
Pour que les formats soient compatibles :

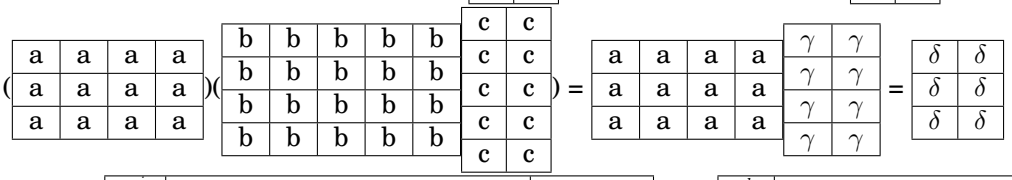
matrice	A	B	C
nombre de lignes	m	n	p
nombre de colonnes	n	p	q

Vérification des formats

matrice	A	B	$A.B$	C	$(A.B).C$		A	$B.C$	$A.(B.C)$
nombre de lignes	m	n	m	p	m		m	n	m
nombre de colonnes	n	p	p	q	q		n	q	q

Explication visuelle des notations.





On note

a_i^j	le terme général de la matrice	A
b_j^k	le terme général de la matrice	B
α_i^k	le terme général de la matrice	$A.B$
c_k^l	le terme général de la matrice	C
d_i^l	le terme général de la matrice	$(A.B).C$

puis

b_j^k	le terme général de la matrice	B
c_k^l	le terme général de la matrice	C
γ_j^l	le terme général de la matrice	$B.C$
a_i^j	le terme général de la matrice	A
δ_i^l	le terme général de la matrice	$A.(B.C)$

Les formules du cours donnent

$$\alpha_i^k = \sum_{j=1}^{n} a_i^j.b_j^k$$

puis

$$d_i^l = \sum_{k=1}^{p} \alpha_i^k.c_k^l = \sum_{k=1}^{p} \Big(\sum_{j=1}^{n} a_i^j.b_j^k \Big).c_k^l = \sum_{\substack{1\leqslant j\leqslant n\\ 1\leqslant k\leqslant p}} a_i^j.b_j^k.c_k^l$$

De même $\gamma_j^l = \sum_{k=1}^{p} b_j^k.c_k^l$ et

$$\delta_i^l = \sum_{j=1}^{n} a_i^j.\gamma_j^l = \sum_{j=1}^{n} \Big(a_i^j.\sum_{k=1}^{p} a_i^j.b_j^k \Big) = \sum_{\substack{1\leqslant k\leqslant p\\ 1\leqslant j\leqslant n}} a_i^j.b_j^k.c_k^l$$

Ce sont bien les deux mêmes formules.

Une preuve passe aussi par les applications linéaires.

A	est le matrice de	f	de $(E,+,.)$ muni d'une base $\mathbb{B}_1$	vers $(F,+,.)$ muni d'une base $\mathbb{B}_2$
B	est le matrice de	g	de $(F,+,.)$ muni d'une base $\mathbb{B}_2$	vers $(G,+,.)$ muni d'une base $\mathbb{B}_3$
C	est le matrice de	f	de $(G,+,.)$ muni d'une base $\mathbb{B}_3$	vers $(H,+,.)$ muni d'une base $\mathbb{B}_4$
$(A.B).C$	est le matrice de	$(f\circ g)\circ h$	de $(E,+,.)$ muni de la base $\mathbb{B}_1$	vers $(H,+,.)$ muni de la base $\mathbb{B}_4$
$A.(B.C)$	est le matrice de	$f\circ(g\circ h)$	de $(E,+,.)$ muni de la base $\mathbb{B}_1$	vers $(H,+,.)$ muni de la base $\mathbb{B}_4$

De l'associativité de la loi de composition se déduit alors l'associativité du produit matriciel.

1.4 Polynômes et fractions rationnelles.

1.4.1 Théorème de rigidité.

Deux polynômes de degré inférieur ou égal à d qui coïncident en $d+1$ points sont forcément égaux.

On prend deux polynômes P et Q de degré inférieur ou égal à d, égaux en $d+1$ points.
Le polynôme $P-Q$ a alors $d+1$ racines, alors qu'il est de degré inférieur ou égal à d.

Le polynôme $P-Q$ se factorise alors sous la forme $R(X).\prod_{i=0}^{d}(X-i)$.

Pour que son degré soit inférieur ou égal à d, la seule solution est $R(X)=0$ (polynôme nul).

1.4.2 Décomposition en éléments simples.

Décomposition en éléments simples : si les a_k sont n complexes distincts, alors toute fraction de la forme $\dfrac{P(X)}{(X-a_1)\dots(X-a_n)}$ avec $P(X)$ de degré inférieur ou égale à $n-1$ se décompose d'une façon unique sous la forme

$$\frac{P(X)}{(X-a_1)\dots(X-a_n)}=\frac{\alpha_1}{X-a_1}+\dots+\frac{\alpha_n}{X-a_n}$$

(avec les α_k dépendant linéairement des coefficients du polynôme P).

On prend le problème à rebours et on utilise un théorème d'algèbre linéaire.

Pour tout n-uplet de complexes $(\alpha_1,\dots\alpha_n)$, on définit $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$.

L'objet obtenu est un polynôme de degré inférieur ou égal à $n-1$ puisque c'est en fait

$$\alpha_1.(X-a_2)\dots(X-a_n)+\alpha_2.(X-a_1).(X-a_3)\dots(X-a_n)+\dots+\alpha_n.(X-a_1)\dots(X-a_{n-1})$$

L'application ainsi définie est linéaire de $(\mathbb{C}^n,+,.)$ dans $(\mathbb{C}_{n-1}[X],+,.)$

(vérification purement technique $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\lambda.\alpha_i+\mu.\beta_i}{X-a_i}=\lambda.\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}+\mu.\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\beta_i}{X-a_i}$*)*

On montre que cette application est injective par la "*méthode des pôles*".

Supposons en effet que $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$ soit le polynôme nul.

En le calculant en a_1 sous la forme développée

$$\alpha_1.(X-a_2)\dots(X-a_n)+\alpha_2.(X-a_1).(X-a_3)\dots(X-a_n)+\dots+\alpha_n.(X-a_1)\dots(X-a_{n-1})$$

on obtient que α_1 est nul. De même, en a_i, chaque α_i est nul. Le seul n-uplet d'image nulle est le n-uplet $(0,\dots 0)$.

Comme les deux espaces ont la même dimension *(n pour les deux)*, l'application linéaire injective est automatiquement bijective *(corolaire de la formule du rang)*.

Sa réciproque est aussi une application linéaire bijective. On traduit : pour tout polynôme $P(X)$ de degré inférieur ou égal à $n-1$ il existe un n-uplet tel que $P(X)$ s'écrive $\prod_{k=1}^{n}(X-a_k).\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$.

On divise : $\dfrac{P(X)}{\prod_{k=1}^{n}(X-a_k)}=\sum_{i=1}^{n}\frac{\alpha_i}{X-a_i}$.

Le théorème reste valable si on remplace $\mathbb{C}$ par $\mathbb{R}$; si le degré du polynôme dépasse n, on effectue une division euclidienne pour arriver à $\dfrac{P(X)}{\prod_{k=1}^{n}(X-a_k)} = R(X) + \sum_{i=1}^{n} \dfrac{\alpha_i}{X-a_i}$; si les a_i ne sont pas tous distincts, on croise des termes en $\dfrac{\alpha_i}{X-a_i} + \dfrac{\beta_i}{(X-a_i)^2}$ voire $\dfrac{\alpha_i}{X-a_i} + \dfrac{\beta_i}{(X-a_i)^2} + \dfrac{\gamma_i}{(X-a_i)^3}$ et même plus, mais avec le même type de démonstration.

1.4.3 Relations coefficients racines.

Si le polynôme $\sum_{k=0}^{d} a_k.X^k$ admet pour racines les α_i avec i de 1 à d (chaque racine devant être citée autant de fois que son éventuelle multiplicité), alors on a

$$\sum_{i=1}^{d} \alpha_i = -\frac{a_{d-1}}{a_d}, \qquad \sum_{1\leqslant i<j\leqslant n} \alpha_i.\alpha_j = +\frac{a_{d-2}}{a_d}$$

$$\sum_{1\leqslant i<j<k\leqslant n} \alpha_i.\alpha_j.\alpha_k = -\frac{a_{d-3}}{a_d} \quad \textbf{jusqu'à} \quad \prod_{i=1}^{n} \alpha_i = (-1)^d.\frac{a_0}{a_d}$$

Comme on connaît les racines du polynôme et son coefficient dominant, on peut l'écrire sous forme factorisée $a_d.\prod_{i=1}^{n}(X-\alpha_i)$, développer formellement et identifier le coefficient de X^{d-k} de chaque côté : a_{d-k} est égal à la somme des produits de racines par paquets de k des racines.

C'est la généralisation de $X^2 - S.X + P$ pour un polynôme de degré 2 avec S pour la somme des racines et P pour le produit.

Le polynôme unitaire de degré inférieur ou égal à 3 de racines α, β et γ s'écrit $X^3 - S.X^2 + D.X - P$ et dans l'autre sens, si le polynôme de racines α, β et γ s'écrit $a_3.X^3 + a_2.X^2 + a_1.X + a_0$ alors on a

$$P(X) = a_3.(X-\alpha).(X-\beta).(X-\gamma)$$

$$a_3.\Big(X^3 - (\alpha+\beta+\gamma).X^2 + (\alpha.\beta+\beta.\gamma+\gamma.\alpha).X - \alpha.\beta.\gamma\Big)$$

$$a_3.X^3 + a_2.X^2 + a_1.X + a_0$$

$$S = \alpha+\beta+\gamma = -\frac{a_2}{a_3} \quad D = \alpha.\beta+\beta.\gamma+\gamma.\alpha = -\frac{a_1}{a_3} \quad P = \alpha.\beta.\gamma = -\frac{a_0}{a_3}$$

1.4.4 Interpolation de Lagrange. (Seconde année)

On se donne $n+1$ réels (ou complexes) distincts a_0 à a_n.
Pour tout choix $[y_0, \dots y_n]$ il existe un unique polynôme P de degré inférieur ou égal à n vérifiant $P(a_k) = y_k$ pour tout k.
Par $n+1$ points il passe un unique polynôme.
Les formules explicites pour n petit seront

$$f(a).\frac{X-b}{a-b} + f(b).\frac{X-a}{b-a}$$

$$f(a).\frac{(X-b).(X-c)}{(a-b).(a-c)} + f(b).\frac{(X-a).(X-c)}{(b-a).(b-c)} + f(c).\frac{(X-a).(X-b)}{(c-a).(c-b)}$$

$$f(a).\frac{(X-b).(X-c).(X-d)}{(a-b).(a-c).(a-d)} + f(b).\frac{(X-a).(X-c).(X-d)}{(b-a).(b-c).(b-d)} + f(c).\frac{(X-a).(X-b).(X-d)}{(c-a).(c-b).(c-d)} + f(d).\frac{(X-a).(X-b).(X-c)}{(d-a).(d-b).(d-c)}$$

Unicité en cas d'existence.
Si les deux polynômes P et Q de degré inférieur ou égal à n vérifient $P(a_k) = y_k$ et $Q(a_k) = y_k$ pour tout k de 0 à n, alors le polynôme $P - Q$ est nul en $n+1$ points.
Ayant plus de racines que son degré, c'est le polynôme nul. On a donc $P = Q$.

A partir de cette unicité, par un argument d'algèbre linéaire sur les dimensions, on peut conclure à l'existence.
Il suffit d'utiliser le théorème du rang.

Existence.
La rédaction est ici proposée pour quatre éléments a, b, c et d plutôt que a_0 jusqu'à a_n., afin d'alléger par rapport aux formules en $L_k = \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq k}} \frac{X - a_i}{a_k - a_i}$.

$P(X)$	$P(a)$	$P(b)$	$P(c)$	$P(d)$
$\frac{(X-b).(X-c).(X-d)}{(a-b).(a-c).(a-d)}$	1	0	0	0
$\frac{(X-a).(X-c).(X-d)}{(b-a).(b-c).(b-d)}$	0	1	0	0
$\frac{(X-a).(X-b).(X-d)}{(c-a).(c-b).(c-d)}$	0	0	1	0
$\frac{(X-a).(X-b).(X-c)}{(d-a).(d-b).(d-c)}$	0	0	0	1
combinaison	α	β	γ	δ

La combinaison est ici le polynôme

$$\alpha.\frac{(X-b).(X-c).(X-d)}{(a-b).(a-c).(a-d)} + \beta.\frac{(X-a).(X-c).(X-d)}{(b-a).(b-c).(b-d)} + \gamma.\frac{(X-a).(X-b).(X-d)}{(c-a).(c-b).(c-d)} + \delta.\frac{(X-a).(X-b).(X-c)}{(d-a).(d-b).(d-c)}$$

proposé plus haut.

1.4.5 Théorème de Gauss-Lucas. (Hors programme)

Si P est un polynôme (complexe ou réel), les raciens de sa dérivée P' sont dans l'enveloppe convexe de l'ensemble des racines de P (c'est à dire dans le polygône délémité par les racines de P).

Soit P dans $\mathbb{C}[X]$ un polynôme unitaire. Alors on a $P(X) = \lambda \prod_{k=1}^{n}(X - z_k)$. On décompose en éléments simples $\frac{P'}{P} = \sum_{k=1}^{n} \frac{1}{X - z_k}$.

Soit z une racine de P' différente de z_k. Alors

$$\begin{aligned}
\frac{P'(z)}{P(z)} = 0 &\Leftrightarrow \sum_{k=1}^{n} \frac{1}{z - z_k} = 0 \\
&\Leftrightarrow \sum_{k=1}^{n} \frac{\overline{(z - z_k)}}{(z - z_k)\overline{(z - z_k)}} = 0 \text{ (quantité conjuguée)} \\
&\Leftrightarrow \sum_{k=1}^{n} \frac{\overline{(z - z_k)}}{|z - z_k|^2} = 0 \\
&\Leftrightarrow \sum_{k=1}^{n} \frac{z - z_k}{|z - z_k|^2} = 0 \quad \text{(on repasse au conjugé)} \\
&\Leftrightarrow z \sum_{k=1}^{n} \frac{1}{|z - z_k|^2} = \sum_{k=1}^{n} \frac{z_k}{|z - z_k|^2} \\
&\Leftrightarrow z = \sum_{k=1}^{n} z_k \lambda_k
\end{aligned}$$

Avec $\lambda_k = \dfrac{\dfrac{1}{\overline{|z - z_k|^2}}}{\displaystyle\sum_{k=1}^{n} \frac{1}{|z - z_k|^2}}$.

On remarque que $\displaystyle\sum_{k=1}^{n} \lambda_k$ vaut 1. Donc on a écrit z comme barycentre à poids positifs des z_k, donc

z est bien dans l'enveloppe convexe des z_k.

2 Structures algébriques.

2.1 Théorie des ensembles.

2.1.1 Ensemble des parties d'un ensemble, son cardinal.

Si E est un ensemble, on note $P(E)$ l'ensemble des parties de E (ensemble d'ensembles).
Si E est un ensemble fini de cardinal n, alors $P(E)$ est un ensemble de cardinal 2^n.

Il faut se méfier des étages, on a

$$(A \subset E) \Leftrightarrow (A \in P(E))$$

La formulation ambigüe « a est dans E » signifie « a est un élément de E » et s'écrit $a \in E$.
La formulation ambigüe « A est dans E » signifie « A est un sous-ensemble de E » et s'écrit $A \subset E$ ou $A \in P(E)$.

On note qu'on a

$$(a \in E) \Leftrightarrow (\{a\} \in P(E))$$

et aussi pour tout ensemble E

$$\emptyset \in P(E) \text{ mais aussi } \emptyset \subset P(E)$$

Le cardinal de $P(E)$ est 2^n quand E est de cardinal n.

Exemples :

cardinal de E	E	$P(E)$	cardinal de $P(E)$
0	$\emptyset$	$\{\emptyset\}$	1
1	$\{a\}$	$\{\emptyset,\ \{a\}\}$	2
2	$\{a,\ b\}$	$\{\emptyset,\ \{a\},\ \{b\},\ \{a,b\}\}$	4
3	$\{a,\ b,\ c\}$	$\{\emptyset,\ \{a\},\ \{b\},\ \{a,b\},\ \{b,c\},\ \{c,a\},\ \{a,b,c\}\}$	8
3	$\{a,\ b,\ c,\ d\}$	$\{\emptyset,\ \{a\},\ \{b\},\ \{a,b\},\ \{b,c\},\ \{c,a\},\ \{a,b,c\},$ $\{d\},\ \{a,d\},\ \{b,d\},\ \{a,b,d\},\ \{b,c,d\},\ \{c,a,d\},\ \{a,b,c,d\}\}$	16

Preuve par dénombrement.
Dans $P(E)$, il y a les parties à zéro élément, à un élément, à deux éléments, à k éléments, jusqu'à la partie à n éléments.
Or, pour k fixé, il y a $\binom{n}{k}$ parties à k éléments.

Argument : n choix pour le premier élément d'une liste d'éléments distincts, $n-1$ choix pour le second, $n-2$ pour le troisième, jusqu'à $n-k+1$ choix pour le k^{ieme}. Ceci justifie le numérateur.
Pour toute partie de cardinal k, il y a $k!$ listes possibles de k éléments distincts, d'où le dénominateur.

On somme alors

$$Card(P(E)) = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$$

Preuve d'informaticien.
On numérote les éléments de E de a_0 à a_{n-1}.
Chaque partie A est codée par un mot binaire formé de 0 et de 1.
Le k^{ieme} chiffre indique par 1 ou 0 si a_k est dans la partie A.
On a alors 2^n mots (deux choix indépendants pour chaque lettre), du mot $00\ldots0$ (ensemble vide) au mot $11\ldots1$ (ensemble E), donc 2^nparties.

Variante.
Pour toute partie A , on définit sa fonction caractéristique $\chi_A = x \to \begin{cases} 1 & si\ x \in A \\ 0 & si\ x \notin A \end{cases}$ de E dans $\{0,\ 1\}$.
De même, pour toute application de E dans $\{0,\ 1\}$, on construit une partie $A = \{x \in E \mid \chi(x) = 1\}$.
Il y a donc autant de parties que de fonctions de E dans $\{0,\ 1\}$.
Et il y a 2^n applications de E dans $\{0,\ 1\}$ (deux choix indépendants pour l'image de chaque élément).

Preuve par récurrence.
Le tableau est initialisé en haut.
On suppose que l'ensemble $\{a_0, \ldots a_{n-1}\}$ a 2^n parties.
On passe à l'ensemble $\{a_0, \ldots a_{n-1},\ a_n\}$ qui a $n+1$ éléments.
Pour chaque partie A de $\{a_0, \ldots a_{n-1}\}$, on crée deux parties de $\{a_0, \ldots a_{n-1},\ a_n\}$: A et $A \cup \{a_n\}$.
On a deux fois plus de parties, on passe donc de 2^n à $2.2^n = 2^{n+1}$.

2.1.2 Théorème de Cantor.

Théorème de Cantor : soit E un ensemble il ne peut pas y avoir d'application surjective de E dans $P(E)$ et donc pas de bijection entre E et $P(E)$.

Le théorème est une évidence en dimension finie, puisque $P(E)$ est de cardinal 2^nquand E est de cardinal n, et bien sûr, on a $2^n > n$.

Supposons qu'une telle application F de E dans $P(E)$ soit surjective.
On pose alors $A = \{a \in E \mid a \notin F(a)\}$ *(cette définition est cohérente, puisque a est un élément de E et $F(a)$ une partie de E; l'élément peut appartenir ou non à la partie)*.
L'ensemble A ainsi défini est une partie de E. Il a donc au moins un antécédent α par F puisque F est supposée surjective.
Mais alors, il n'y a que deux possibilités : α est dans A ou α n'est pas dans A.
• Si α est dans A, on a alors $\alpha \in F(\alpha)$ *(puisque $A = F(\alpha)$)*, et par définition, ceci donne $\alpha \notin A$. Contradiction.
• Si α n'est pas dans A, on a alors $\alpha \notin F(\alpha)$ *(puisque $A = F(\alpha)$)*, et par définition, ceci donne $\alpha \in A$. Contradiction.

Les deux seuls cas possibles conduisent à une contradiction. C'est donc que l'hypothèse "*A admet au moins un antécédent α par F*" est impossible. F ne peut pas être surjective.

2.1.3 $\mathbb{Z}$ est dénombrable.

Il existe une bijection entre $\mathbb{N}$ et $\mathbb{Z}$.

L'application $n \longrightarrow (-1)^{n-1}.\left[\frac{n+1}{2}\right]$ va de $\mathbb{N}$ dans $\mathbb{Z}$ et elle est bijective.
Sa réciproque est $p \longrightarrow \begin{cases} 2.p-1 & si\ p \geqslant 0 \\ -2.p & si\ p < 0 \end{cases}$.
Visuellement

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	10	11	...
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	5	-5	6	...

2.1.4 $\mathbb{Q}$ est dénombrable.

On peut construire une bijection entre $\mathbb{Q}$ et $\mathbb{N}$.

La suite de Stern-Brocott (hors programme) construit explicitement par récurrence une bijection entre $\mathbb{N}$ et $\mathbb{Q}^{+*}$.

$$u_0 = 1\ et\ u_{n+1} = \frac{1}{1 + 2[v_n] - v_n}$$

$$\frac{p_0}{q_0} = \frac{1}{1}\ et\ \frac{p_{n+1}}{q_{n+1}} = \frac{q_n}{p_n + q_n - 2.(p_n \% q_n)}$$

2.1.5 $\mathbb{R}$ n'est pas dénombrable.

Si on suppose qu'il existe une bijection entre $\mathbb{R}$ et $\mathbb{N}$ alors on peut établir une contradiction.

Le raisonnement qui suit n'a pas toute la rigueur voulue, mais donne une idée de la méthode dite de Cantor.
On suppose qu'il existe une bijection entre $\mathbb{N}$ et $]0,\ 1[$ (ce qui suffira, puisqu'il existe ensuite une bijection entre $]0,\ 1[$ et $]0,\ +\infty[$ puis une bijection entre $]0,\ +\infty[$ et $]-\infty,\ +\infty[$ [2]).
Pour chaque entier naturel n, on associe un réel a_n dont l'écriture décimale sera $a_n = 0, \alpha_{n,1}\alpha_{n,2}\alpha_{n,3}\ldots$ chaque $\alpha_{n,k}$ étant un chiffre de 0 à 9 inclus.
Proprement, $a_n = \sum_{k=1}^{+\infty} \frac{\alpha_{n,k}}{10^k}$ (somme infinie sauf si il n'y a qu'un nombre fini de chiffres non nuls).

2. la première est $t \longrightarrow \frac{1-t}{t}$, et la seconde est le logarithme

On crée alors un nouveau réel A dont le n^{ieme} chiffre β_n est construit à partir du n^{ieme} chiffre de a_n.
Proprement : $\beta_n = 9 - \alpha_{n,n}$ et donc $A = \sum_{n=1}^{+\infty} \frac{9-\alpha_{n,n}}{10^n}$.

L'existence de ce réel n'est pas détaillée ici (série convergente par domination par $\sum_{n=1}^{+\infty} \frac{9}{10^n}$).

Par encadrement, A est un réel entre 0 et 1.
Il est donc égal à l'un des a_N (bijection) : $A = a_N = 0, \alpha_{N,1}\alpha_{N,2}\dots\alpha_{N,N}\dots$.
Mais en même temps $A = 0, \beta_1\beta_2\dots\beta_N\dots$
Le N^{ieme} chiffre de A est à la fois $\alpha_{N,N}$ mais aussi $\beta_N = 9 - \alpha_{N,N}$.
On tient notre contradiction.

2.2 Groupes, anneaux, corps.

2.2.1 Loi interne sur un ensemble.

.	Quantification G est l'ensemble et $*$ est la loi. *Une loi est une opération, qui prend deux éléments a et b et en calcule un nouveau, qu'on note $a*b$ si $*$ est le nom de la loi.*
Interne	$\forall(a,\ b) \in G^2,\ a*b \in G$
Associative	$\forall(a,\ b,\ c) \in G^3,\ (a*b)*c = a*(b*c)$
Neutre	$\exists e \in G,\ \forall a \in G,\ a*e = e*a = a$ on prouve son unicité ne pas écrire $\forall a,\ \exists e,\ a*e = e*a = a$
Symétriques au pluriel	$\forall a \in G,\ \exists \alpha \in G,\ a*\alpha = \alpha*a = e$ là aussi, il y a unicité par $\alpha' * a * \alpha$
En option : Commutative	$\forall(a,\ b) \in G^2,\ a*b = b*a$

Si possible, on évitera de confondre la loi (opération, action) et le résultat.

addition $+$	*soustraction* $-$	*multiplication* $\times$	*division* $\div$	*composition* $\circ$
somme $a+b$	*différence* $a-b$	*produit* $a\times b$	*quotient* a/b	*composée* $f\circ g$

2.2.2 Unicité du neutre dans un groupe.

Dans un groupe, le neutre est unique, et chaque élément n'a qu'un symétrique.

Soit $(E,*)$ un groupe *(pas forcément commutatif)*.
On suppose que deux éléments e et ε tiennent le rôle de neutre *(à droite comme à gauche) (objectif : $e=\varepsilon$)*.
On calcule alors $e*\varepsilon$. On a $e = e*\varepsilon = \varepsilon$ car ε est neutre et e est neutre.
Par transitivité de l'égalité, on a $e = \varepsilon$.

Il n'est pas judicieux dans cette démonstration de faire intervenir d'autre élément du groupe E. De plus, il faut avoir prouvé l'unicité du neutre avant de parler de symétriques.

.

2.2.3 Unicité du symétrique en cas d'existence.

Dans un groupe, chaque élément n'a qu'un symétrique.

On suppose que deux éléments α et β tiennent le rôle de symétrique d'un élément a de E *(objectif : $\alpha = \beta$)*.
On calcule alors $\alpha * a * \beta$ en exploitant l'associativité :

$$\begin{array}{llll} & & \alpha * a * \beta & = (\alpha * a) * \beta = \quad e * \beta = \quad \beta \\ \alpha = & \alpha * e = & \alpha * (a * \beta) = & \alpha * a * \beta \end{array}$$

Par transitivité de l'égalité, on a $\alpha = \beta$.

On notera qu'il s'agit de preuves directes et non pas de raisonnements par l'absurde ; on prend deux éléments répondant à la définition et on montre que c'est le même

2.2.4 Théorème de Lagrange : le cardinal d'un sous-groupe divise le cardinal du groupe. (Seconde année)

Soit $(G, *)$ un groupe et H un sous-groupe de G.
Alors le cardinal de G est un multiple du cardinal de H.

On considère un groupe $(G, *)$ de cardinal fini n, de neutre e , pas forcément commutatif.
On définit sur E la relation $\Re$ par

$$\forall (a,\ b) \in G^2,\ (a\ \Re\ b) \Leftrightarrow (a * b^{-1} \in H)$$

On vérifie que c'est une relation d'équivalence.

propriété	quantification	argument
réflexivité	$\forall a \in G,\ a * a^{-1} \in H$	$e \in H$
symétrie	$\forall (a,\ b) \in G^2,\ (a * b^{-1} \in H) \Rightarrow (b * a^{-1} \in H)$	$\forall h \in H,\ h^{-1} \in H$
transitivité	$\forall (a,\ b,\ c) \in G^3,\ (a * b^{-1} \in H \text{ et } b * c^{-1} \in H) \Rightarrow (a * c^{-1} \in H)$	$\forall (h,k) \in H^2,\ h * k \in H$

Chaque classe d'équivalence a alors le même cardinal que H.
En effet, si on se donne un élément a de G et si on cherche sa classe d'équivalence (ensemble des éléments en relation avec a), alors elle est formée des $h * a$ pour h dans H ; il y a a donc un élément dans la classe de a pour chaque h de H et vice versa.

En notant k le nombre de classes d'équivalence, toutes de cardinal $Card(H)$, on dénombre tous les éléments de G (chacun est dans une classe et une seule) :

$$Card(G) = Card(H) + \ldots + Card(H) = k.Card(H)$$

2.2.5 Intersection de sous-groupes.

L'intersection de sous-groupes d'un groupe $(G, *)$ est encore un sous-groupe de $(G, *)$.

On commence, même si c'est inutile par le cas de deux sous-groupes A et B.
On suppose donc que A et B sont deux sous groupes de $(G, *)$ *(inclusion, stabilité, présence du neutre, passage au symétrique)*.
On montre que $A \cap B$
• est inclus dans G car A et B le sont,
• contient le neutre n de $(G, *)$ car n est à la fois dans A et dans B,
• est stable par composition :
on prend x et y dans $A \cap B$; comme x est dans A et y aussi, le "produit" $x * y$ est dans A *(stabilité de A)* ;

comme x est dans B et y aussi, le produit $x * y$ est dans le sous-groupe B ; on reconnaît que $x * y$ est dans $A \cap B$,

• est stable par passage au symétrique :
on prend x dans $A \cap B$; comme il est dans le sous-groupe A, x^{-1} est dans A ; comme x est dans B, son symétrique x^{-1} est dans B ; on reconnaît que x^{-1} est dans $A \cap B$.

On passe au cas d'un nombre quelconque (même infini) *de sous-groupes A_i pour i décrivant un ensemble d'indexation I.*
On rappelle $\bigcap_{i\in I} A_i = \{x \in G \mid \forall i \in I,\ x \in A_i\}$.

• Par construction, $\bigcap_{i\in I} A_i$ est une partie de G.

• Chaque A_i est un sous-groupe de $(G, *)$, le neutre n de G en fait partie ; il est donc dans l'intersection.

• On prend x et y tous deux dans $\bigcap_{i\in I} A_i$. Pour chaque i de I, x est dans A_i et y est dans A_i. Comme chaque A_i est un sous-groupe de $(G, *)$, le "produit" $x * y$ est dans A_i. Comme $x * y$ est dans tous les A_i, il est dans $\bigcap_{i\in I} A_i$.

• On prend x dans $\bigcap_{i\in I} A_i$. Par définition, pour tout i, x est dans A_i. Comme chaque A_i est un sous-groupe de $(G, *)$, le symétrique x^{-1} est dans A_i. Comme ceci est vrai pour tout i, x^{-1} est dans $\bigcap_{i\in I} A_i$.

2.2.6 Réunion de sous-groupes.

La réunion de deux sous-groupes d'un groupe $(G, *)$ n'est jamais un sous-groupe de $(G, *)$, sauf si l'un est inclus dans l'autre.

On considère deux sous groupes A et B d'un groupe $(G, *)$. On a trois cas

$A \subset B$	$B \subset A$	$A \not\subset B$ et $B \not\subset A$
$A \cup B = B$, sous groupe	$A \cup B = A$, sous groupe	$A \cup B$ n'est pas stable par $*$

Seul le troisième cas va être étudié ici, évidemment.
Comme A n'est pas inclus dans B, il existe au moins un élément a qui est dans A, mais pas dans B *(négation de $\forall a \in A,\ a \in B$)*.
Comme B n'est pas inclus dans A, il existe au moins un élément b qui est dans B, mais pas dans A.
Comme A et B sont des sous-groupes, on a

$a \in A$	$a \notin B$	$a \in A \cup B$	$a^{-1} \in A$
$b \notin A$	$b \in B$	$b \in A \cup B$	$b^{-1} \in B$

On regarde où se trouve l'élément $a * b$.
• Il n'est pas dans A, sinon $(a^{-1}) * (a * b)$ serait dans A *(stabilité de A)*.
• Il n'est pas dans B, sinon $(a * b) * (b^{-1})$ serait dans B *(stabilité de B)*.
N'étant ni dans A, ni dans B, il n'est pas dans $A \cup B$.
On reconnaît que $A \cup B$ n'est pas stable par la loi $*$.

Corolaire : un groupe ne peut pas être la réunion de deux sous-groupes propres [3].

2.2.7 $(P(E), \Delta, \cap)$ est un anneau commutatif.

La loi de composition interne Δ (différence symétrique) est commutative, associaitive.

$$\forall (A, B, C) \in (P(E))^3,\ (A\Delta B = B\Delta A),\ (A\Delta B)\Delta C = A\Delta(B\Delta C)$$

3. on appelle sous-groupe propre un sous-groupe différent du groupe

Attention, pour l'associativité, $A\Delta B\Delta C$ contient notemment $A \cap B \cap C$.

On dispose d'un élément neutre : l'ensemble vide.
Toute partie est alors son propre symétrique : $A\Delta A = \emptyset$.

La loi de composition interne $\cap$ est commutative et associaitive

$$\forall (A,B,C) \in (P(E))^3,\ (A \cap B = B \cap A),\ (A \cap B) \cap C = A \cap (B \cap C)$$

Elle estdistributive sur la différence symétrique

$$\forall (A,B,C) \in (P(E))^3,\ (A\Delta B)\ \cap\ C = (A \cap C)\ \Delta\ (B \cap C)$$

On dispose aussi du neutre de la seconde loi, c'est E lui même.

Les démonstrations se font par des tablesde vérité.
Ou bien plus simplement par les fonctions indicatrices : $1_{A\cap B} = 1_A \times 1_B$ et $1_{A\Delta B} = |1_A - 1_B|$
ou même $1_{A\Delta B} = (1_A + 1_B)\ \%2$.

La seconde loi n'est pas intègre (sauf cas d'un ensemble E trop petit). On peut avoir $A \cap B = \emptyset$ sans avoir forcément $A = \emptyset$ ou $B = \emptyset$.

2.2.8 Relations sur un ensemble.

.	Une relation sur un ensemble est "formellement" une application de $E \times E$ dans $\{Vrai,\ Faux\}$. Pratiquement, on prend deux éléments a et b, et on dit si a est ou non en relation avec b ($a\Re b$).
Réflexive	Tout élément est en relation avec lui même $\forall a \in E,\ a\Re a$
Transitive	Les flèches se mettent bout à bout. $\forall (a,\ b,\ c) \in E^3,\ (a\Re b\ et\ b\Re c) \Rightarrow (a\Re c)$
Antisymétrique	Il ne peut pas y avoir de flèches dans les deux sens $\forall (a,\ b) \in E^2,\ (a\Re b\ et\ b\Re a) \Rightarrow (a = b)$ Ce n'est pas la négation de "symétrique".
Symétrique	Il y a une flèche à l'aller il y a une flèche au retour $\forall (a,\ b) \in E^2,\ (a\Re b) \Rightarrow (b\Re a)$
Ordre $\leqslant, \subset, \Rightarrow$	Relation réflexive, antisymétrique et transitive un ordre peut être total ($\forall (a,b),\ a \ll b\ ou\ b \ll a$) ou partiel ($\exists (a,b),\ a \not\ll b\ et\ b \not\ll a$)
Équivalence $=, \equiv, \Leftrightarrow$	Relation réflexive, symétrique et transitive la classe d'équivalence d'un élément a est l'ensemble des éléments en relation avec a : $Cl(a) = \{\alpha \in E \mid \alpha\Re a\}$

2.3 Anneau $(\mathbb{Z}, +, .)$, arithmétique.

2.3.1 Sous groupes de $(\mathbb{Z},\ +)$.

Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles de la forme $n.\mathbb{Z}$ (ensemble des multiples de n) pour n entier naturel.

Déjà, les ensembles de la forme $n.\mathbb{Z}$ sont bien des sous-groupes de $(\mathbb{Z}, +)$:

on se fixe n et on pose $n.\mathbb{Z} = \{n.p \mid p \in \mathbb{Z}\}$
• c'est une partie de $\mathbb{Z}$
• le neutre additif 0 y est, sous la forme $n.0$
• la somme de deux éléments de cet ensemble *($n.a$ et $n.b$)* est encore dans cet ensemble *(de la forme $n.(a+b)$ avec $a+b$ dans $\mathbb{Z}$)*
• l'opposé d'un élément de cet ensemble *(de la forme $n.a$)* est encore dans cet ensemble *(de la forme $n.(a-)$ avec $-a$ entier relatif)*.

On note que pour $n = 1$, l'ensemble $n.\mathbb{Z}$ est $\mathbb{Z}$ *(le plus grand)*, tandis que pour $n = 0$ c'est $\{0\}$ *(le plus petit)*.

On prend maintenant un sous-groupe G de $(\mathbb{Z}, +)$, il faut montrer que G est de la forme $n.\mathbb{Z}$ pour un n bien choisi.
Si G se réduit au seul neutre 0, c'est $0.\mathbb{Z}$ comme indiqué plus haut.
Sinon, il y a dans G au moins un élément non nul. Par stabilité par passage au symétrique si nécessaire, il y a dans G au moins un élément strictement positif.
On pose alors $P = G \cap \mathbb{N}^*$ *(les éléments strictement positifs de G)*.
C'est une partie de $\mathbb{N}$ non vide, comme on l'a dit plus haut.
Elle admet donc un plus petit élément.
On note celui ci n.
D'ores et déjà, en tant que plus petit élément de l'ensemble, n est dans P, donc dans G.
Par stabilité de G par addition, chaque nombre de la forme $n.a$ avec a dans $\mathbb{N}$ est dans G *(récurrence sur a)*.
Par passage à l'opposé, chaque élément de la forme $n.(-b)$ avec b dans $\mathbb{N}$ est dans G.
A ce stade, on a prouvé que G contient tous les $n.k$ avec k dans $\mathbb{Z}$: $n.\mathbb{Z} \subset G$.

Il nous manque l'autre inclusion. On prend N dans G.
On effectue la division euclidienne de N par n. Il existe deux entiers p et q vérifiant $N = n.q + r$ avec $0 \leqslant r < n$.
Mais alors on a $q = N - n.q$. Les deux entiers N et $n.p$ sont dans G *(hypothèse et résultat de la première inclusion)*. Par stabilité du sous-groupe G, la différence $N - n.q$ est aussi dans G.
Si cette différence est non nulle, c'est un élément de $G \cap \mathbb{N}^*$ strictement plus petit que n, ce qui contredit la définition de n.
Par élimination, l'entier r est nul.
On reporte : $N = n.p$, c'est un multiple de n.
On a cette fois $G \subset n.\mathbb{Z}$.La double inclusion donne l'égalité.

2.3.2 Théorème de Fermat, application au corps $(\mathbb{Z}_{/p.\mathbb{Z}}, +, .)$ avec p premier.

Petit théorème de Fermat : pour tout entier naturel premier p et tout entier n non multiple de p :

$$n^{p-1} = 1 \ mod \ p$$

Corolaire : $(\{0,\ 1, \ldots p-1\}, +, \times)$ est un corps pour l'addition et la multiplication modulo p.

Dans tout ce qui suit, p est donc un nombre premier.

On commence par un lemme : les coefficients binomiaux $\binom{p}{k}$ pour k de 1 à $p-1$ sont des multiples de p.
Le résultat est vrai pour $k = 1$: $\binom{p}{k} = p$.
Supposons le résultat vrai pour un k entre 1 et $p-2$. On a alors $(k+1).\binom{p}{k+1} = (p-k).\binom{p}{k}$ *(formule*

classique sur les coefficients binomiaux en ligne). Le second membre est un multiple de p par hypothèse. Comme $k+1$ est strictement plus petit que p et ne contient aucun facteur p, c'est que $\binom{p}{k+1}$ est multiple de p.

On poursuit avec un second résultat : pour tout entier naturel n, l'entier $n^p - n$ est un multiple de p *(par récurrence sur n)*.
Pour n égal à 0 *(et même 1)*, cet entier est nul, donc multiple de p.
Supposons le résultat vrai pour un n de $\mathbb{N}$. On calcule alors $(n+1)^p - (n+1)$ par la formule du binôme :

$$(n+1)^p - (n+1) = \sum_{k=0}^{p} \binom{p}{k}.n^k - (n+1) = \sum_{k=1}^{p-1} \binom{p}{k}.n^k + (n^p+1) - (n+1)$$

(on a isolé deux termes).
La somme $\sum_{k=1}^{p-1} \binom{p}{k}.n^k$ est un multiple de p par le lemme précédent comme somme de multiple de p.
La différence $(n^p+1) - (n+1)$ est un multiple de p par hypothèse de rang n.
La somme est bien multiple de p.

On termine en factorisant dans le cas où n n'est pas multiple de p : $n.(n^{p-1}-1)$ est multiple de p.
Or, il n'y a pas de facteur p dans n, c'est donc que $n^{p-1}-1$ est multiple de p.

Il existe des entiers p non premiers (dits "*nombres de Carmichael*") qui vérifient cette propriété pour tous les entiers n.

2.3.3 Théorème de Wilson (hors-programme).

Théorème de Wilson : pour p premier, $(p-1)!$ est congru à -1 modulo p.

On se place dans l'anneau des entiers de 0 à $p-1$ pour l'addition et la multiplication modulo p.
Il reste à prouver que tout entier non nul admet un inverse pour la multiplication modulo p.
On prend donc n entre 1 et $p-1$. On sait donc d'après le petit théorème de Fermat que $n^{p-1}-1$ est un multiple de p. On traduit : $n^{p-1} = 1 \ mod \ p$. On factorise : $n.n^{p-2} = 1 \ mod \ p$.
L'entier n^{p-2} *(réduit modulo p)* est l'inverse multiplicatif de n.

Dans le corps $(\{0,1,\dots p-1\},+,\times)$, on a donc $n^{p-1}=1$ pour tout entier de 1 à $p-1$.
Le polynôme $X^{p-1}-1$ admet donc $p-1$ racines : les entiers de 1 à $p-1$.
On peut donc le factoriser sous la forme $\alpha.\big(X-1\big)\times\dots\big(X-(p-1)\big)$, avec α égal à 1 *(terme de plus haut degré)*.
Partant de $X^{p-1}-1 = \big(X-1\big)\dots\big(X-(p-1)\big)$, on obtient en 0 : $-1 = (-1)\times(-2)\dots(1-p)$.
Il y a dans le membre de droite $p-1$ signes "moins", ce qui fait un signe "plus" *(on traite à part le cas trivial $p=2$)*. Il reste $-1 = (p-1)!$ *(pour la multiplication modulo p)*. C'est le théorème de Wilson.

Il existe une autre preuve du théorème de Wilson en regroupant les termes.
Dans le produit $(p-1)! = 1\times 2\times 3\dots(p-1)$, on regroupe dans la mesure du possible, les termes deux par deux :
• 1 et $p-1$ à part
• chaque élément de 2 à $p-2$ avec son inverse.
En effet, seul 1 et $p-1$ sont leur propre inverse puisque ce critère correspond à $x^2=1$, qui se factorise en $(x-1).(x+1)=0$, d'uniques solutions 1 et -1 *(qui s'appelle aussi $p-1$)*.
Les éléments groupés deux à deux ont à chaque fois pour produit 1 par définition même de l'inverse. Il reste (modulo p) :

$$(p-1)! = 1\times 1^{(p-3)/2}.(p-1) = p-1 = -1$$

2.3.4 Bézout implique Gauss.

Soient a,b et c trois entiers naturels. On suppose que a divise $b \times c$ et que a et b sont premiers entre eux.
Alors a divise c.

On traduit la première hypothèse : il existe un entier naturel k vérifiant $b \times c = a \times k$.
On traduit la seconde hypothèse sous la forme identité de Bézout : il existe deux entiers relatifs u et v vérifiant $a \times u + b \times v = 1$.

On multiplie la seconde par c : $a \times u \times c + b \times v \times c = c$.
On remplace avec la première hypothèse : $a \times u \times c + a \times k \times v = c$.
On factorise : $a \times (u \times c + k \times v) = c$.
On reconnaît que c est un multiple de a.

Il existe aussi une preuve reposant sur les décompositions en produit de facteurs premiers.
On écrit $a = 2^{\alpha_1} \times 3^{\alpha_2} \times 5^{\alpha_3} \times \dots$
$b = 2^{\beta_1} \times 3^{\beta_2} \times 5^{\beta_3} \times \dots$
$c = 2^{\gamma_1} \times 3^{\gamma_2} \times 5^{\gamma_3} \times \dots$
Proprement, en notant (p_n) la liste infinie des nombres premiers : $a = \prod_{n=1}^{+\infty} (p_n)^{\alpha_n}$ avec les α_i nuls à partir d'un certain rang.

On traduit les hypothèses : chaque α_n est plus petit que $\beta_n + \gamma_n$ car $a = \prod_{n=1}^{+\infty} (p_n)^{\alpha_n}$ et $b \times c = \prod_{n=1}^{+\infty} (p_n)^{\beta_n + \gamma_n}$.
Quand α_n est non nul, β_n est nul, et vice versa (nombres n'ayant aucun diviseur commun possible).
On obtient alors que chaque α_n est plus petit que son γ_n associé.

2.3.5 Théorème de Fermat (seconde preuve).

p est un entier premier et a un entier premier avec p alors $a^{p-1} = 1$ modulo p.

p est fixé, et a aussi
On prend l'ensemble des entiers de 1 à $p-1$ pour la multiplication modulo p.
On définit l'application $n \longrightarrow a..n$ (multiplication modulo p).
Cette application va de l'ensemble dans lui même ($a.n$ ne peut pas être nul moudlo p puisqu a et n sont premiers avec p).
Elle est bijective de $\{1,\ 2, \dots p-1\}$ dans lui même.

> *On peut se contenter de prouver son injectivité, car on travaille d'un ensemble de cardinal fini dans liui même.*
> *Or, si $a.n$ et $a.m$ ont la même image, c'est que $a.(n-m)$ est nul modulo p.*
> *Comme a est premier avec p; la seule solution est $n-m$ est multiple de p.*
> *Or, $n-m$ est entre $p-1$ et $1-p$.*
> *La seule solution est bien $a - m = 0$.*
>
> *On peut aussi proposer la bijection réciproque.*
> *En effet, quitte à écrire une identité de Bézout entre a et p ($a.u + p.v = 1$), on peut montrer que l'application $k \longrightarrow u.k$ est la réciproque de $n \longrightarrow a.n$ (le tout modulo p).*

La liste $[1,\ 2, \dots p-1]$ est donc la même que la liste $[a,\ a.2, \dots, a.(p-1)]$, mais pas dans le même ordre.
Par commutativité et associativité de la multiplication, les deux produits $\prod_{k=1}^{p-1} k$ et $\prod_{k=1}^{p-1} (a.k)$ sont donc

égaux.
On a donc $\prod_{k=1}^{p-1} k = \prod_{k=1}^{p-1} (a.k) \ mod\ p$ puis $\prod_{k=1}^{p-1} k = a^{p-1}.\prod_{k=1}^{p-1} k \ mod\ p$ en sortant le a.
La différence $(a^{p-1}-1).\prod_{k=1}^{p-1} k$ est donc un multiple de p.
Comme p est premier, il n'a aucun facteur commun avec $\prod_{k=1}^{p-1} k$ et c'est $a^{p-1}-1$ qui est multiple de p.

Application : test de Fermat (hors programme).
La contraposée du petit théorème de Fermat dans le cas particulier $a=2$ dit
si a^{p-1} ne vaut pas 1 modulo p, alors p n'est pas premier.
On nous donne p, on commence par calculer a^{p-1} (informatiquement, c'est un nombre binaire avec un seul 1 et une grand quantité de 0).
On regarde le reste de la division modulo p (une division ou même des congruences).
Si il ne vaut pas 1, alors p n'est pas premier.
Si il vaut 1, alors c'est peut être bon signe, mais ça ne prouve rien.

Le nombre 561 est un nombre de Carmichaël (et il y en a une infinité) :
pour tout entier k, $k^{561}-k$ est un multiple de 561.

```
def carm(n) :
....for k in range(n) : #inutile d'aller plus loin
........if (k**n - k ) != 0 : #test de Fermat
............return False
....return True #on a tout testé
```

3 Analyse réelle et complexe.

3.1 Topologie de $\mathbb{R}$.

Par construction [4] de $\mathbb{R}$, on sait que toute partie de $\mathbb{R}$ admet une borne supérieure (plus petit majorant).

3.1.1 Caractérisation séquentielle de la borne supérieure d'une partie non vide majorée.

Le réel α est la borne supérieur de la partie A non vie majorée si et seulement si c'est un majorant de A vers lequel converge une suite d'éléments de A.

Sens indirect.
On suppose que α est un majorant de A et qu'une suite (a_n) d'éléments de A converge vers α ($\forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \geqslant N_\varepsilon,\ \alpha-\varepsilon \leqslant a_n \leqslant \alpha+\varepsilon$).
Déjà α est un majorant.
Tout autre majorant m de A vérifie $\forall a \in A,\ a \leqslant m$. En particulier $\forall n \in \mathbb{N},\ a_n \leqslant m$.
Par passage à la limite, $\alpha \leqslant m$.
Ceci confrme que de tous les majorants, α est le plus petit.

Si on veut éviter le passage à la limite, on raisonne avec la définition « contraposée » : si un réel μ est plus petit que α, alors ce n'est plus un majorant de A.
Soit en effet μ vérifiant $\mu < \alpha$. On prend alors $a_{N_{(\alpha-\mu)/2}}$. C'est un élément de A et il vérifie

$$\mu < \frac{\alpha+\mu}{2} = \alpha - \frac{\alpha-\mu}{2} \leqslant a_{N_{(\alpha-\mu)/2}} \leqslant \alpha - \frac{\alpha-\mu}{2}$$

4. admise dans le cours, pouvant passer par les « coupures de Dedekind » ou par les « classes d'équivalences de suites de Cauchy » : https://fr.wikipedia.org/wiki/Construction_des_nombres_r%C3%A9els

Sens direct.
On suppose que α est la borne supérieure de A (plus petit majorant).
Par définition de majorant, tout élément de A est plus petit que α.
D'autre part, pour tout n, le réel $\alpha - 2^{-n}$ est strictement plus petit que α. Ce n'est donc plus un majorant de A.
Il existe donc au moins un élément a de A qui vérifie $\alpha - 2^{-n} < a$ (et même $\alpha - 2^{-n} < a$). On en prend un qu'on note a_n.
On a ainsi construit une suite d'éléments de A qui vérifie $\forall n,\ \alpha - 2^{-n} \leqslant a_n \leqslant \alpha$.
Par encadrement, cette suite converge, et sa limite est égale à α.

On note que si la borne supérieure α est un maximum (c'est à dire un élément de A qui majore tous les autres), il suffit de prendre $a_n = \alpha$ pour tout n (suite constate).

En revanche, si la borne supérieure n'est pas dans A, on peut même prendre une suite strictement croissante d'éléments de A qui converge vers α.
Comme $\alpha - 1$ n'est plus un majorant de A, il existe au moins un élément a_0 de A vérifiant $\alpha - 1 \leqslant a_0 \leqslant \alpha$ et même $\alpha - 1 \leqslant a_0 < \alpha$.
Comme $\alpha - \dfrac{\alpha - a_0}{2}$ n'est plus un majorant de A, il existe au moins un élément a_1 de A vérifiant $\alpha - \dfrac{\alpha - a_0}{2} \leqslant a_1 \leqslant \alpha$ et même $\alpha - \dfrac{\alpha - a_0}{2} \leqslant a_1 < \alpha$.
Comme $\alpha - \dfrac{\alpha - a_n}{2}$ n'est plus un majorant de A, il existe au moins un élément a_2 de A vérifiant $\alpha - \dfrac{\alpha - a_1}{2} \leqslant a_2 \leqslant \alpha$ et même $\alpha - \dfrac{\alpha - a_1}{2} \leqslant a_2 < \alpha$.
On construit de proche en proche une suite (a_n) d'éléments de A vérifiant

$$\forall n \in \mathbb{N},\ \alpha - \frac{1}{2^n} \leqslant \alpha - \frac{\alpha - a_n}{2} \leqslant a_{n+1} < \alpha$$

La suite (a_n) est strictement croissante et converge par encadrement vers α.

3.1.2 $\mathbb{Q}$ et $\mathbb{R} - \mathbb{Q}$ sont denses dans $\mathbb{R}$.

1 - Tout intervalle de $\mathbb{R}$ non réduit à un point[a] contient au moins un rationnel.
2 - Tout intervalle de $\mathbb{R}$ non réduit à un point contient au moins un irrationnel.
3 - Tout intervalle de $\mathbb{R}$ non réduit à un point contient une infinité de rationnels et d'irrationnels.
4 - Tout réel est limite d'une suite de rationnels.
5 - Tout réel est limite d'une suite d'irrationnels.

[a] **Par la locution « non réduit à un point, on interdit aussi « intervalle vide » tel que $]0,\ 0[$**

1 - Prenons un intervalle $[\alpha,\ \beta]$ avec $\alpha < \beta$.
On considère $q = \left[\dfrac{1}{\beta - \alpha}\right] + 1$ (entier vérifiant donc $\dfrac{1}{q} \leqslant \beta - \alpha$) et $p = [\beta.q]$ (entier également).
Par définition de la partie entière ($t - 1 \leqslant [t] \leqslant t$) on a $\beta.q - 1 \leqslant p \leqslant \beta.q$. On divise par q positif

$$\alpha = \beta - (\beta - \alpha) \leqslant \beta - \frac{1}{q} \leqslant \frac{p}{q} \leqslant \beta$$

On tient un rationnel entre α et β.

2 - En appliquant le résultat précédent à l'intervalle $[\alpha - \sqrt{2},\ \beta - \sqrt{2}]$, on trouve un rationnel $\frac{p}{q}$ entre $\alpha - \sqrt{2}$ et $\beta - \sqrt{2}$ et donc un irrationnel $\dfrac{p}{q} + \sqrt{2}$entre α etβ.

3 - En appliquant le résultat à chaque intervalle $\left[\frac{(2.k.\alpha+(2^{n+1}-2.k).\beta}{2^{n+1}},\ \frac{(2.k+1).\alpha+(2^{n+1}-2.k-1).\beta}{2^{n+1}}\right]$ avec n entier et k de 0 à n, on a des intervalles disjoints inclus dans $[\alpha,\ \beta]$. On a donc une infinité de rationnels dans $[\alpha,\ \beta]$.

4 - Le réel a est limite de la suite $(2^{-n}.[2^n.a])_{n\in\mathbb{N}}$ (approximation binaire par défaut).
En effet, la définition de la partie entière ($\forall t,\ t-1<[t]\leqslant t$) donne après division par 2^t : $a-2^{-n}<2^{-n}.[2^n.a]\leqslant a$ et le théorème d'encadrement permet de conclure.

5 - Si on veut des irrationnels, on prend $(2^{-n}.[2^n.a]+2^{-n-\frac{1}{2}})_{n\in\mathbb{N}}$.

3.1.3 Sous-groupes de $(\mathbb{R},\ +)$.

Si A est un sous-groupe de $(\mathbb{R},+)$ alors il y a deux possibilités :
- $\exists a\in\mathbb{R},\ A=a.\mathbb{Z}=\{a.k\ k\in\mathbb{Z}\}$ **(sous-groupe discret)**
- $\forall(\alpha,\ \beta)\in\mathbb{R}^2,\ (\alpha<\beta)\Rightarrow(\exists a\in A,\ \alpha<a<\beta)$ **(sous groupe dense[a])**

a. tout intervalle de $\mathbb{R}$ non réduit à un point contient au moins un élément de A et donc une infinité

On se donne A, sous groupe de $(\mathbb{R},\ +)$. On pose alors $A^-=A\cap]-\infty,\ [$. On a alors deux cas avec sous cas.

◦ Si A^-est vide, alors par passage au symétrique, $A\cap]0,\ +\infty[$ est vide aussi et A se réduit à $\{0\}$ qu'on peut écrie $0.\mathbb{Z}$.

◦ Si A^- est non vide, alors en tant que partie de $\mathbb{R}$ non vide majorée, elle admet une borne supérieure.

• Si cette borne supérieure est nulle, alors A est partout dense dans $\mathbb{R}$.
En effet, si on se donne α et β avec $\alpha<\beta$ alors le réel $\alpha-\beta$ est strictement négatif et ne peut pas être un majorant de A^- (sinon, 0 ne serait plus le plus petit majorant de A^-). Il existe donc un x_0 dans A^- vérifiant $\alpha-\beta<x_0\leqslant 0$. Mais x_0 ne peut valoir 0 car il est dans A^-.
On considère alors l'entier $\left[\frac{\alpha}{x_0}\right]$ et le réel $\left[\frac{\alpha}{x_0}\right].x$.
Par appartenance de x_0 (et de son opposé $-x_0$) à A et stabilité additive, $\left[\frac{\alpha}{x_0}\right].x$ est dans A.
On part ensuite de l'encadrement classique $t-1\leqslant[t]\leqslant t$ appliqué à $t=\frac{\alpha}{x_0}$ et on le multiplie par x_0 négatif

$$\frac{\alpha}{x_0}.x_0-x_0\geqslant\left[\frac{\alpha}{x_0}\right].x\geqslant\frac{\alpha}{x_0}.x$$

$$\beta=\alpha-(\alpha-\beta)\geqslant\alpha-x_0\geqslant\left[\frac{\alpha}{x_0}\right].x\geqslant\alpha$$

L'élément $\left[\frac{\alpha}{x_0}\right].x$ de A est entre α et β.
On a donc montré $Sup(A^-)=0\Rightarrow(A\ est\ dense\ dans\ R)$.

Exemples moins ou plus compliqués : $A=\mathbb{R}$, $A=\mathbb{Q}$, $A=\mathbb{Z}+\pi.\mathbb{Z}$.

• Si cette borne est non nulle, alors elle est atteinte.

Par l'absurde : si la borne supérieure α de A^- non nulle n'est pas atteinte, alors par définition de « plus petit majorant », $\forall\varepsilon>0,\ \exists a_\varepsilon\in A,\ \alpha-\varepsilon<a_\varepsilon\leqslant\alpha$ et même $\forall\varepsilon>0,\ \exists a_\varepsilon\in A,\ \alpha-\varepsilon<a_\varepsilon<\alpha$ puisque α n'est pas dans A.
Mais alors avec les deux cas particuliers $\varepsilon_0=|\alpha|$ puis $\varepsilon_1=\alpha-a_{\varepsilon_0}$ on dispose de deux éléments a_{ε_0} et a_{ε_1} de A vérifiant

$$2.\alpha=\alpha-|\alpha|<a_{\varepsilon_0}=\alpha-(\alpha-a_{\varepsilon_0})<a_{\varepsilon_1}<\alpha$$

On déduit que la différence $a_{\varepsilon_0} - a_{\varepsilon_1}$ est dans A (groupe) et vérifie $\alpha < a_{\varepsilon_0} - a_{\varepsilon_1} < 0$, ce qui contredit la définition de $\alpha = Sup(A)$.

Maintenant que α est dans A alors le réel positif $|\alpha|$ y est aussi, et tous ses multiples y sont (sous-groupe de $(\mathbb{R},\ +)$. On a donc $|\alpha|.\mathbb{Z} \subset A$.
On montre la réciproque par la même méthode que tout les sous-groupes de $(\mathbb{Z},\ +)$.
Soit a un élément de A,on l'encadre entre deux multiples consécutifs de α : $n.|\alpha| \leqslant a < n.|\alpha| + |\alpha|$ (avec $n = \left[\frac{a}{|\alpha|}\right]$).
Par soustraction, on a l'encadrement $-|\alpha| = \alpha \leqslant a - (n+1).|\alpha| < 0$ et par stabilité, $a - (n+1).|\alpha|$ est dans A et même dans A^-.
Par définition de la borne supérieure de A^-, la seule possibilité est $a - (n+1).|\alpha| = \alpha$. Elle conduit à $a = n.|\alpha|$.
Tous les éléments de A sont les multiples de $|\alpha|$. Le sous groupe est de la forme $a.\mathbb{Z}$.

3.1.4 Adhérence d'une partie.

$\overline{A}$ est l'ensemble des réels qui sont limites d'au moins une suite de points de A.

La notation ne devra pas être confondue avec le complémentaire qu'on notera alors A^c.

Pour tout couple de parties $(A,\ B)$ de $\mathbb{R}$ on a
1 - $A \subset \overline{A}$
2 - $(A \subset B) \Rightarrow (\overline{A} \subset \overline{B})$
3 - $\overline{\emptyset} = \emptyset$
4 - $\overline{A \cup B} = \overline{A} \cup \overline{B}$
5 - $\overline{\overline{A}} = \overline{A}$

1 - Tout point a de A est limite de la suite constante (a), faite d'élément(s) de A.

2 - On suppose $A \subset B$. On prend α dans $\overline{A}$. Il est limite d'une suite (a_n) d'éléments de A donc d'éléments de B. Il est donc dans $\overline{B}$.

3 - Il n'existe pas de suite d'éléments de $\emptyset$. Aucun point ne peut donc être limite d'une suite de points de $\emptyset$.

4 - On a déjà $A \subset A \cup B$ et donc par (2) on a $\overline{A} \subset \overline{A \cup B}$.
De la même façon, $\overline{B} \subset \overline{A \cup B}$, et donc la réunion $\overline{A} \cup \overline{B}$ est incluse dans $\overline{A \cup B}$.

Réciproquement, si on prend x dans $\overline{A \cup B}$, il est limite d'une suite (c_n) d'éléments de $A \cup B$.
L'un des deux ensembles suivants est alors infini, puisque leur réunion donne $\mathbb{N}$:

$$P = \{p \in \mathbb{N} \mid c_p \in A\}\ et\ Q = \{q \in \mathbb{N} \mid c_q \in B\}$$

Sans perte de généralité, on suppose que c'est P qui est infini. On en réindexe les éléments par ordre croissant

$$\varphi(0) = ppe(P),\ \varphi(1) = ppe(P - \{\varphi(0)\}),\ \varphi(2) = ppe(P - \{\varphi(0), \varphi(1)\}), \ldots \varphi(n+1) = ppe(P - \bigcup_{k=0}^{n} \{\varphi(k)\})$$

La sous-suite $(c_{\varphi(n)})$ est alors une suite d'éléments de A qui converge vers x. x est donc dans $\overline{A}$.

5 - L'inclusion $\overline{A} \subset \overline{\overline{A}}$ est un cas particulier de $B \subset \overline{B}$.
On prend maintenant c dans $\overline{\overline{A}}$. Par définition même, c est limite d'une suite (b_n) de points de $\overline{A}$.

Mais chaque b_n est donc lui aussi limite d'une suite de points de A : $b_n = \lim_{p\to+\infty}(a_{n,p})$ avec chaque $a_{n,p}$ dans A.
On construit alors une suite de points de A qui converge vers c.
Pour tout k il existe un élément de la suite (b_n) proche de c à 2^{-k} près.
Il suffit en effet d'appliquer la définition $\forall\varepsilon>0,\ \exists N_\varepsilon,\ \forall n\geqslant N_\varepsilon,\ |b_n-c|\leqslant\varepsilon$ à $\varepsilon=2^{-k}$ et de choisir $b_{N_{2^{-k}}}$.
Pour ce $b_{N_{2^{-k}}}$ cette fois, la convergence de la suite $(a_{N_{2^{-k}},p})_{p\in\mathbb{N}}$ vers $b_{N_{2^{-k}}}$ donne l'existence d'un $a_{N_{2^{-k}},p}$ de A vérifiant $|a_{N_{2^{-k}},p}-b_{N_{2^{-k}}}|\leqslant 2^{-k}$ (prendre $\varepsilon=2^{-k}$ là encore dans la définition de cette convergence).
Par inégalité triangulaire, on a $|c-a_{N_{2^{-k}},P_{2^{-k}}}|\leqslant 2.2^{-k}$.
Par encadrement, la suite de $\left(a_{N_{2^{-k}},P_{2^{-k}}}\right)_k$ est à veleurs dans A et converge vers c.
c est donc adhérent à A.

On peut aussi commencer par prouver le critère « par voisinages »
$(\alpha\in\overline{A})\Leftrightarrow(\forall\varepsilon>0,\ [c-\varepsilon,\ c+\varepsilon]\cap A\neq\emptyset)$
puis « couper les ε en deux.

3.2 Suites réelles.

3.2.1 Si une suite converge, sa limite est unique.

On prend une suite réelle (u_n) qui converge à la fois vers α et β. On va montrer par l'absurde que α est égal à β.

On suppose en effet $|\alpha-\beta|>0$ (négation de $\alpha=\beta$) et

$$\forall\varepsilon>0,\ \exists N_\varepsilon\in\mathbb{N},\ \forall n\geqslant N_\varepsilon,\ |u_n-\alpha|\leqslant\varepsilon\ et\ \forall\varepsilon>0,\ \exists N_\varepsilon\in\mathbb{N},\ \forall n\geqslant N_\varepsilon,\ |u_n-\alpha|\leqslant\varepsilon$$

On prend pour ε le cas particulier $\varepsilon=\dfrac{|\alpha-\beta|}{3}>0$.
On prend ensuite pour n le cas particulier $n_0=Max(N_{|\alpha-\beta|/3},\ M_{|\alpha-\beta|/3})$. Il est à la fois plus grand que $N_{|\alpha-\beta|/3}$ et que $M_{|\alpha-\beta|/3}$. On a donc à la fois $|u_{n_0}-\alpha|\leqslant\dfrac{|\beta-\alpha|}{3}$ et $|u_{n_0}-\beta|\leqslant\dfrac{|\beta-\alpha|}{3}$.
On fait un enchainement d'inégalités :

$$|\alpha-\beta|=|\alpha-u_{n_0}+u_{n_0}-\beta|\leqslant|\alpha-u_{n_0}+u_{n_0}-\beta|\leqslant\frac{|\alpha-\beta|}{2}+\frac{|\alpha-\beta|}{3}$$

On simplifie la majoration $|\alpha-\beta|\leqslant\dfrac{2.|\alpha-\beta|}{3}$ par $|\alpha-\beta|$ (strictement positif) et on obtient la contradiction attendue : $1\leqslant\dfrac{2}{3}$.

3.2.2 Lemme d'extraction : toute extraction grimpe au moins aussi vite que l'identité.

Soit φ une extraction, c'est à dire une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$.
On montre alors (par récurrence sur n) : $\forall n\in\mathbb{N},\ \varphi(n)\geqslant n$.

Initialisation : $\varphi(0)$ est un entier naturel, il est donc supérieur ou égal à 0.

Hérédité : on suppose pour un entier n donné quelconque : $\varphi(n)\geqslant n$.
Par croissance stricte de φ, on a $\varphi(n+1)>\varphi(n)\geqslant n$.
Par transitivité, l'entier $\varphi(n+1)$ est strictement plus grand que n.
Et le premier entier après n étant $n+1$, on déduit que $\varphi(n+1)$ est supérieur ou égal à $n+1$.

3.2.3 Toute suite extraite d'une suite convergente converge, vers la même limite.

On prend une suite (u_n) et on suppose qu'elle converge vers α.
On prend une extractionφ et on considère la suite (v_n) définie par $\forall n,\ v_n = u_{\varphi(n)}$ (suite extraite de u par extraction φ).
Cette suite extraite (v_n) converge aussi vers α.

On traduit la convergence de (u_n) vers α : $\forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \geqslant N_\varepsilon,\ |u_n - \alpha| \leqslant \varepsilon$.
Mais alors, pour εquelconque donné, on a pour n plus grand que N_ϵ(celui de la convergence de (u_n)) :

$$\varphi(n) \geqslant n \geqslant N_\varepsilon$$

Il s'ensuit qu'on a alors $|u_{\varphi(n)} - \alpha| \leqslant \varepsilon$. On a prouvé, pour la suite (v_n) égale à $(u_{\varphi(n)})$

$$\forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \geqslant N_\varepsilon,\ |v - \alpha| \leqslant \varepsilon$$

On reconnaît la convergence de la suite $(u_{\varphi(n)})$ vers α.

Ce résultat servira à démontrer la divergence de certaines suites.
Si la suite (u_n) admet deux sous-suites $(u_{\varphi(n)})$ et $(u_{\psi(n)})$ qui convergent vers deux limites distinctes, alors la suite (u_n) ne peut pas converger.

3.2.4 Théorème de recouvrement

Soit (u_n) une suite (réelle ou complexe). On définit deux suites extraites m $\forall n,\ v_n = u_{2.n}$ *et* $w_n u_{2.n+1}$.
On suppose que (v_n) et (w_n) convergent vers la même valeur α.
Alors la suite globale (u_k) converge aussi vers α.

On écrit les deux hypothèses :

$$\forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \geqslant P_\varepsilon,\ |u_{2.n} - \alpha| \leqslant \varepsilon \text{ et } \forall \varepsilon > 0,\ \exists I_\varepsilon \in \mathbb{N},\ \forall n \geqslant I_\varepsilon,\ |u_{2.n+1} - \alpha| \leqslant \varepsilon$$

On vérifie alors par disjonctions de cas

$$\forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall k \geqslant N_\varepsilon,\ |u_k - \alpha| \leqslant \varepsilon$$

avec $N_\varepsilon = Max(2.P_\varepsilon,\ 2.I_\varepsilon + 1)$.
En effet, si k est plus grand que N_ε il est à la fois plus grand que $2.P_\varepsilon$ et plus grand que $2.I_\varepsilon + 1$. On a deux cas :

k pair	k impair
on l'écrit $k = 2.n$	on l'écrit $k = 2.n + 1$
l'hypothèse $k \geqslant N_\varepsilon$donne$2.n \geqslant 2.N_\varepsilon$ donc $n \geqslant P_\varepsilon$	l'hypothèse $k \geqslant N_\varepsilon$donne$2.n + 1 \geqslant 2.I_\varepsilon + 1$ donc $n \geqslant I_\varepsilon$
on déduit $\lvert u_k - \alpha\rvert = \lvert u_{2.n} - \alpha\rvert \leqslant \varepsilon$	on déduit $\lvert u_k - \alpha\rvert = \lvert u_{2.n+1} - \alpha\rvert \leqslant \varepsilon$
dans les deux cas : $\lvert u_k - \alpha\rvert \leqslant \varepsilon$	

3.3 Théorèmes de convergence des suites réelles.

3.3.1 Si une suite converge, sa limite est unique.

Si la suite (a_n) converge à la fois vers α et β alors α est égal à β.

Par l'absurde, on suppose que la suite (a_n) converge à la fois vers α et β avec $\beta \neq \alpha$:

$$\forall \varepsilon > 0,\ \exists A_\varepsilon \in \mathbb{R},\ \forall n \geqslant A_\varepsilon,\ |a_n - \alpha| \leqslant \varepsilon$$

$$\forall \varepsilon > 0,\ \exists B_\varepsilon \in \mathbb{R},\ \forall n \geqslant B_\varepsilon,\ |b_n - \beta| \leqslant \varepsilon$$

Alors,pour n égale à $Max\left(A_{\frac{|\beta-\alpha|}{3}},\ A_{\frac{|\beta-\alpha|}{3}}\right)$ on a

$$\beta - \alpha| = |\beta - a_n + a_n - \alpha| \leqslant |\beta - a_n| + |a_n - \alpha| \leqslant \frac{|\beta-\alpha|}{2} + \frac{|\beta-\alpha|}{2}$$

et cette inégalité du type $x \leqslant \dfrac{x}{2}$ avec $x > 0$ est contradictoire.

3.3.2 Théorèmes algébriques (somme, produit de suites convergentes)

Si les suites (a_n) et (b_n) convergent et si λ est un réel, alors les suites $(a_n + b_n)$, $(\lambda.a_n)$ et $(a_n.b_n)$ convergent.
De plus, l'application qui à une suite convergente associe sa limite est un morphisme d'algèbres ($\lim(\lambda.a_n + b_n) = \lambda.\lim(a_n) + \lim(b_n)$ et $\lim(a_n \times b_n) = \lim(a_n) \times \lim(b_n)$).

On traduit la convergence des deux suites initiales :

$$\forall \varepsilon > 0,\ \exists A_\varepsilon \in \mathbb{R},\ \forall n \geqslant A_\varepsilon,\ |a_n - \alpha| \leqslant \varepsilon$$

$$\forall \varepsilon > 0,\ \exists B_\varepsilon \in \mathbb{R},\ \forall n \geqslant B_\varepsilon,\ |b_n - \beta| \leqslant \varepsilon$$

Pour ε donné strictement positif, on a à partir du rang $Max(A_{\varepsilon/2},\ B_{\varepsilon/2})$

$$|(a_n + b_n) - (\alpha + \beta)| \leqslant |a_n - \alpha| + |b_n - \beta| \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

On reconnaît la convergence de $(a_n + b_n)$ vers $\alpha + \beta$.

De même à partir du rang $A_{\frac{\varepsilon}{|\lambda|+1}}$

$$|\lambda.a_n - \lambda.\alpha| = |\lambda|.|a_n - \alpha| \leqslant \frac{|\lambda|}{|\lambda|+1}.\varepsilon \leqslant \varepsilon$$

On reconnaît la convergence de $(\lambda.a_n)$ vers $\lambda.\alpha$.

On pouvait se contenter de $A_{\frac{\varepsilon}{|\lambda|}}$ mais le raisonnement proposé évite de traiter à part le cas $\lambda = 0$.

Enfin, à partir du rang $Max\left(A_{\frac{\varepsilon}{2.(|\beta|+1)}},\ B_1,\ B_{\frac{\varepsilon}{2.(|\alpha|+1)}}\right)$ on a

$$|a_n.b_n - \alpha.\beta| = \big|(a_n - \alpha).b_n + \alpha.(b_n - \beta)\big| \leqslant |a_n - \alpha|.|b_n| + |\alpha|.|a_n - \beta|$$

$$|a_n.b_n - \alpha.\beta| \leqslant \frac{\varepsilon}{2.(|\beta|+1)}.|b_n| + |\alpha|.\frac{\varepsilon}{2.(|\alpha|+1)}$$

$$|a_n.b_n - \alpha.\beta| \leqslant \frac{\varepsilon}{2.(|\beta|+1)}.|b_n - \beta + \beta| + \frac{\varepsilon}{2}$$

$$|a_n.b_n - \alpha.\beta| \leqslant \frac{\varepsilon}{2.(|\beta|+1)}.(|b_n - \beta| + |\beta|) + \frac{\varepsilon}{2}$$

$$|a_n.b_n - \alpha.\beta| \leqslant \frac{\varepsilon}{2.(|\beta|+1)}.(1 + |\beta|) + \frac{\varepsilon}{2} = \frac{\varepsilon}{2} + \frac{\varepsilon}{2}$$

Toutes les preuves reposent sur une transformation du type $a_n.b_n - \alpha.\beta = (a_n - \alpha).b_n + \alpha.(b_n - \beta)$ ou $a_n.b_n - \alpha.\beta = a_n.(b_n - \beta) + \beta.(a_n - \alpha)$.
Ensuite, on peut sire que le produit $a_n.(b_n - \beta)$ d'une suite bornée par une suite de limite nulle.

3.3.3 Théorème de Cesàro : si une suite converge, sa moyenne converge aussi, vers la même limite.

Si une suite (a_n) converge vers une limite λ, alors sa moyenne de Cesàro (arithmétique) converge aussi vers λ.

Sa moyenne est la suite (c_n) définie par $c_n = \frac{1}{n+1}.\sum_{k=0}^{n} a_k$.

On commence par le cas où la suite (réelle ou complexe) (a_n) converge vers 0.

On quantifie cette hypothèse $\forall \varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \geqslant N_\varepsilon,\ |u_n| \leqslant \varepsilon$.

On se donne donc ε et on définit le rang $N_{\varepsilon/2}$, le réel $\sum_{k=0}^{N_{\varepsilon/2}-1} a_k$ (noté S_N) et le rang $\left[2.\frac{S_N}{\varepsilon}\right]$ (noté G_ε)

On se donne alors n plus grand que $Max(N_{\varepsilon/2},\ G_\varepsilon)$. On coupe alors la somme $\sum_{k=0}^{n} a_k$ par relation de Chasles et on majore par inégalité triangulaire appliquée plusieurs fois

$$\Big|\sum_{k=0}^{n} a_k\Big| \leqslant \Big|\sum_{k=0}^{N_{\varepsilon/2}-1} a_k + \sum_{k=N_{\varepsilon/2}}^{n} a_k\Big| = \Big|S_N\Big| + \sum_{k=N_{\varepsilon/2}}^{n} |a_k|$$

Par définition même de $N_{\varepsilon/2}$, tous les termes de la seconde somme sont plus petits que $\frac{\varepsilon}{2}$. Il n'y a plus qu'à les compter et à majorer sans se poser de question

$$\Big|\sum_{k=0}^{n} a_k\Big| \leqslant \Big|S_N\Big| + \sum_{k=N_{\varepsilon/2}}^{n} \frac{\varepsilon}{2} = \Big|S_N\Big| + (n - N_{\varepsilon/2} + 1).\frac{\varepsilon}{2} \leqslant \Big|S_N\Big| + (n+1).\frac{\varepsilon}{2}$$

On divise par $n+1$ (positif) pour avoir précisément la moyenne de Cesàro

$$c_n = \frac{1}{n+1}.\Big|\sum_{k=0}^{n} a_k\Big| \leqslant \frac{\Big|S_N\Big|}{n+1} + \frac{\varepsilon}{2}$$

On exploite maintenant l'hypothèse $n \geqslant R_\varepsilon$: $n \geqslant \left[2.\frac{S_N}{\varepsilon}\right]$; on a donc $n+1 \geqslant 2.\frac{S_N}{\varepsilon}$ et par produit en croix $\frac{S_N}{n+1} \leqslant \frac{\varepsilon}{2}$ On a maintenant comme attendu

$$c_n = \frac{1}{n+1}.\Big|\sum_{k=0}^{n} a_k\Big| \leqslant \frac{\Big|S_N\Big|}{n+1} + \frac{\varepsilon}{2} \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

C'est bien la convergence de la moyenne vers 0.

Si maintenant la suite (u_n) converge vers λ, on écrit $u_n = \lambda + (u_n - \lambda)$.

Comme la suite $(u_n - \lambda)$ converge vers 0, on lui applique le résultat précédent. Sa moyenne de Cesàro converge vers 0. Et cette moyenne est $\Big(\frac{1}{n+1}.\sum_{k=0}^{n}(u_n - \lambda)\Big)$ dans laquelle on retrouve $\Big(\Big(\frac{1}{n+1}.\sum_{k=0}^{n} u_k\Big) - \lambda\Big)$.

Ceci traduit la convergence de la moyenne de Cesàro $\Big(\frac{1}{n+1}.\sum_{k=0}^{n} u_k\Big)_n$ vers λ.

Cette manipulation $u_n = \lambda + (u_n - \lambda)$ est juste une translation et tient dans un argument propre : l'opérateur de Cesàro $(u_n) \longrightarrow \Big(\frac{1}{n+1}\sum_{k=0}^{n} u_k\Big)$ est linéaire.

3.3.4 Toute suite réelle majorée converge vers son plus petit majorant.

Toute suite réelle croissante majorée converge vers son plus petit majorant.

Soit (a_n) une suite réelle croissante *($a_{n+1} \geqslant a_n$ pour tout n)*, majorée par un certain M *($\forall n \in \mathbb{N},\ a_n \leqslant M$)*.

> On notera que M est un majorant de la suite *(mais pas forcément "le meilleur", il n'a donc aucune raison d'être la limite μ de la suite, celle ci sera inférieure ou égale à M).*

On pose $A = \{a_n \mid n \in \mathbb{N}\}$ *(ensemble des valeurs prises par la suite, projection sur l'axe Oy)*.
C'est une partie de $\mathbb{R}$ *(suite réelle)*, non vide *(on y trouve a_0)* et majorée *(par M)*.
Elle admet donc un "**plus petit majorant**" ou "**borne supérieure**" *(axiomatique de $\mathbb{R}$)*. On le note μ.

On va montrer que (a_n) converge vers μ avec la définition en $\forall\varepsilon, \exists N_\varepsilon$.
On se donne ε strictement positif.
Alors $\mu - \varepsilon$ n'est plus un majorant de A *(car plus petit que le plus petit majorant)*.
Il existe donc au moins un élément de A entre $\mu - \varepsilon$ et μ. Un tel élément sera un certain a_N pour un certain entier N.
On constate qu'on a alors pour tout n plus grand que N : $\mu - \varepsilon \leqslant a_N \leqslant a_n \leqslant \mu \leqslant \mu + \varepsilon$ *(en utilisant : ce qu'on sait de a_N, la croissance de la suite, que μ majore et enfin que ε est positif)*.
On a obtenu : $\forall\varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant N \Rightarrow |a_n - \mu| \leqslant \varepsilon$, c'est bien la convergence de la suite vers μ.

3.3.5 Toute suite convergente est bornée.

Toute suite convergente est bornée.

On prend une suite (a_n), convergente de limite α.
La définition est $\forall\varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geqslant N_\varepsilon \Rightarrow |a_n - \alpha| \leqslant \varepsilon$.
En particulier, à partir du rang N_1, on a $|a_n - \alpha| \leqslant 1$. Par inégalité triangulaire $|a_n| \leqslant |a_n - \alpha| + |\alpha| \leqslant 1 + |\alpha|$.
La suite est donc bornée à partir du rang N_1 par $1 + |\alpha|$. Or, avant, il n'y a qu'un nombre fini de termes.
Globalement, la suite est bornée par $Max(|a_0|,\ |a_1|, \ldots |a_{N_1 - 1}|,\ 1 + |\alpha|)$.

3.3.6 Si une suite d'entiers converge, alors sa limite est un entier.

Si une suite d'entiers converge, alors sa limite est un entier.

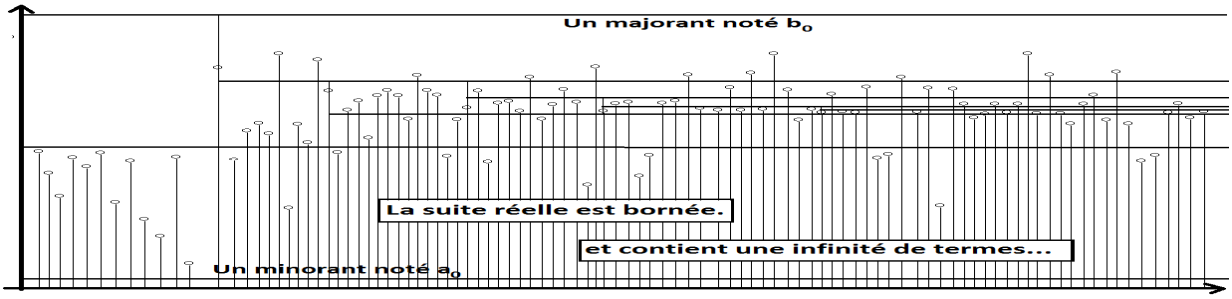
On suppose que la suite (k_n) est faite d'entiers et converge vers α : $\forall\varepsilon > 0,\ \exists N_\varepsilon \in \mathbb{N},\ \forall n \geqslant N_\varepsilon,\ |k_n - \alpha| \leqslant \varepsilon$.
A partir du rang $N_{\frac{1}{4}}$ on a$|k_p - k_q| = |k_p - \alpha + \alpha - k_q| \leqslant |k_p - \alpha| + |\alpha - k_q| \leqslant 2.\frac{1}{4}$. L'entier naturel $|k_p - k_q|$ est plus petit que $\dfrac{1}{2}$. Il est donc nulle.
La suite est constante à partir du rang $N_{\frac{1}{4}}$, égale à $k_{N_{\frac{1}{4}}}$. Elle converge donc vers $k_{N_{\frac{1}{4}}}$, et c'est un entier.

> On pouvait aussi supposer la limite α non entière, et appliquer la définition à $\varepsilon = \dfrac{Min(\alpha - [\alpha],\ [\alpha] + 1 - \alpha)}{2}$, moitié de la distance à l'entier le plus proche.

3.3.7 Théorème de Bolzano Weierstrass (version réelle).

Théorème de Bolzano-Weierstrass réel : de toute suite réelle bornée, on peut extraire au moins une sous-suite convergente.

Soir (u_n) une suite réelle bornée par deux réels qu'on va appeler α_0 et β_0 *(pour tout n de $\mathbb{N}$, on a $\alpha_0 \leqslant u_n \leqslant \beta_0$)*.



On pose alors :

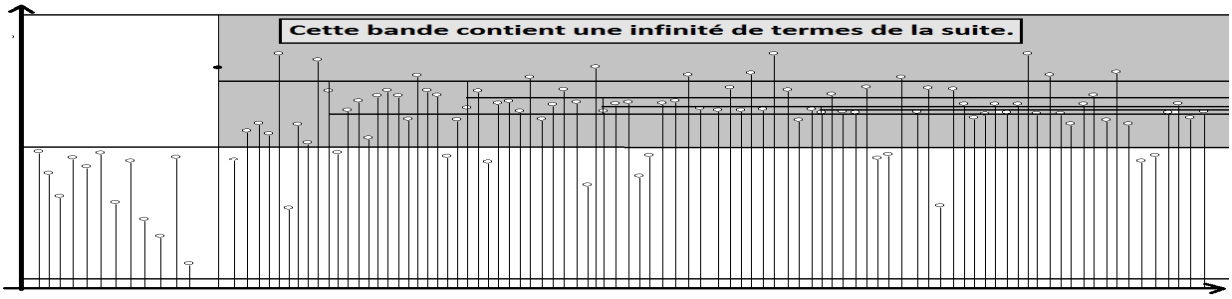
$\gamma_0 = \dfrac{\alpha_0 + \beta_0}{2}$	$A_0 = \{n \in \mathbb{N} \mid \alpha_0 \leqslant a_n \leqslant \gamma_0\}$	$B_0 = \{n \in \mathbb{N} \mid \gamma_0 < a_n \leqslant \beta_0\}$

On a immédiatement : $A_0 \cup B_0 = \mathbb{N}$. L'un des deux ensembles A_0 ou B_0 est donc infini *(et peut être même les deux)*.

Si A_0 est infini	on pose $\varphi(0) = ppe(A_0)$	$N_0 = A_0 - \{\varphi(0)\}$	$\alpha_1 = \alpha_0$	$\beta_1 = \gamma_0$
Si A_0 est fini alors B_0 est infini	on pose $\varphi(0) = ppe(B_0)$	$N_0 = B_0 - \{\varphi(0)\}$	$\alpha_1 = \gamma_0$	$\beta_1 = \beta_0$

Dans les deux cas, on a

$\alpha_0 \leqslant \alpha_1 \leqslant u_{\varphi(0)} \leqslant \beta_1 \leqslant \beta_0$	$\beta_1 - \alpha_1 = \dfrac{\beta_0 - \alpha_0}{2}$	$Card(N_0) = +\infty$	$\forall n \in N_0,\ \alpha_1 \leqslant u_n \leqslant \beta_1$



On pose ensuite :

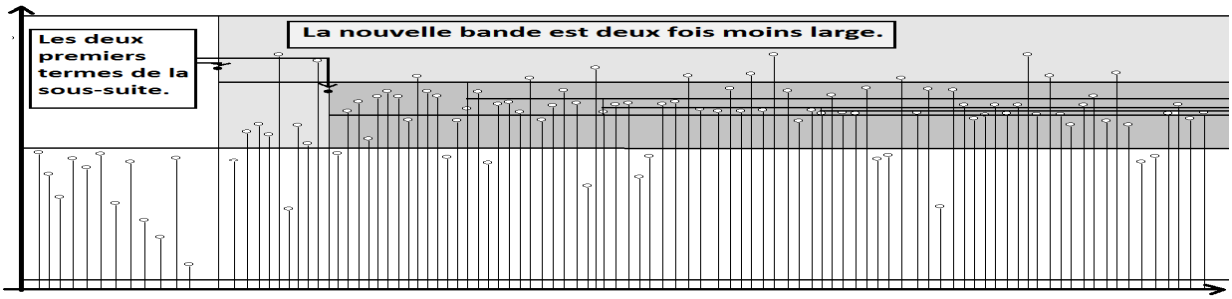
$\gamma_1 = \dfrac{\alpha_1 + \beta_1}{2}$	$A_1 = \{n \in N_0 \mid \alpha_1 \leqslant u_n \leqslant \gamma_1\}$	$B_1 = \{n \in N_0 \mid \gamma_1 < u_n \leqslant \beta_1\}$

On a alors $A_1 \cup B_1 = N_0$, ce qui prouve que l'un au moins des deux ensembles est infini. On refait la même disjonction de cas :

Si A_1 est infini	alors $\varphi(1) = ppe(A_1)$	$N_1 = A_1 - \{\varphi(1)\}$	$\alpha_2 = \alpha_1$	$\beta_2 = \gamma_1$
sinon (B_1 est infini)	alors $\varphi(1) = ppe(B_1)$	$N_1 = B_1 - \{\varphi(1)\}$	$\alpha_2 = \gamma_1$	$\beta_2 = \beta_1$

Dans les deux cas, on a

$\alpha_0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant u_{\varphi(1)} \leqslant \beta_2 \leqslant \beta_1 \leqslant \beta_0$	$\beta_2 - \alpha_2 = \dfrac{\beta_0 - \alpha_0}{4}$	$\varphi(0) < \varphi(1)$
	$Card(N_1) = +\infty$	$\forall n \in N_1,\ \alpha_2 \leqslant u_n \leqslant \beta_2$



Passons maintenant à la construction effective par récurrence de l'extraction φ.
On suppose qu'au rang p, on a obtenu

$\alpha_0 \leqslant \ldots \leqslant \alpha_p \leqslant u_{\varphi(p-1)} \leqslant \beta_p \leqslant \ldots \leqslant \beta_0$	$\beta_p - \alpha_p = \dfrac{\beta_0 - \alpha_0}{2^p}$	$\varphi(0) < \varphi(1) < \ldots < \varphi(p-1)$
	$Card(N_{p-1}) = +\infty$	$\forall n \in N_{p-1},\ \alpha_p \leqslant u_n \leqslant \beta_p$

On pose encore

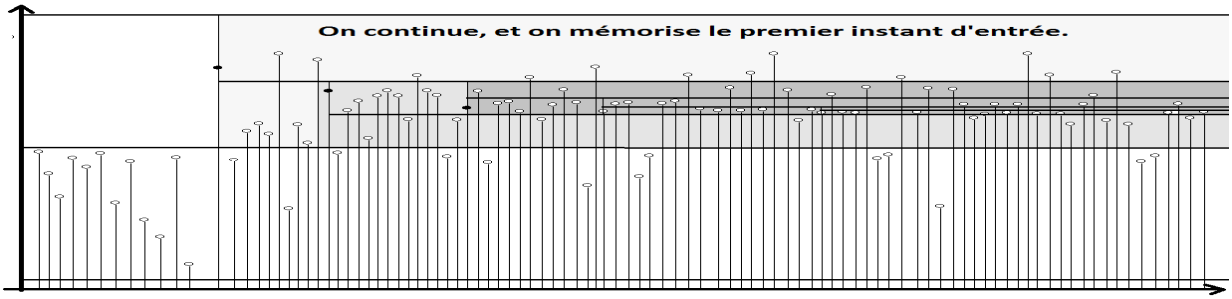
$\gamma_p = \dfrac{\alpha_p + \beta_p}{2}$	$A_p = \{n \in N_{p-1} \mid \alpha_p \leqslant u_n \leqslant \gamma_p\}$	$B_p = \{n \in N_{p-1} \mid \gamma_p < u_n \leqslant \beta_p\}$

Ayant encore $A_p \cup B_p$ de cardinal infini *(c'est N_{p-1})*, on choisit suivant que A_p ou B_p est infini :

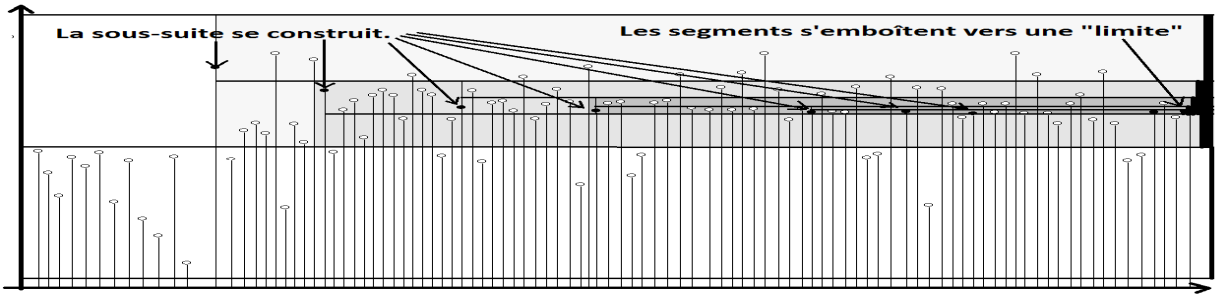
Si A_p est infini	alors $\varphi(p) = ppe(A_p)$	$N_p = A_p - \{\varphi(p)\}$	$\alpha_{p+1} = \alpha_p$	$\beta_{p+1} = \gamma_p$
sinon	alors $\varphi(p) = ppe(B_p)$	$N_p = B_p - \{\varphi(p)\}$	$\alpha_{p+1} = \gamma_p$	$\beta_{p+1} = \beta_p$

On est assuré qu'on a encore

$\alpha_0 \leqslant \ldots \leqslant \alpha_{p+1} \leqslant u_{\varphi(p)} \leqslant \beta_{p+1} \leqslant \ldots \leqslant \beta_0$	$\beta_{p+1} - \alpha_{p+1} = \dfrac{\beta_0 - \alpha_0}{2^{p+1}}$	$\varphi(0) < \ldots < \varphi(p-1) < \varphi(p)$
	$Card(N_p) = +\infty$	$\forall n \in N_p,\ \alpha_{p+1} \leqslant u_n \leqslant \beta_{p+1}$



φ est une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ *(c'est pour s'en assurer qu'on prend à chaque fois $N_p = A_p - \{\varphi(p)\}$ ou $N_p = B_p - \{\varphi(p)\}$, ce qui ne fait qu'enlever un élément à un ensemble infini)*.
On reconnaît que les deux suites encadrantes (α_p) et (β_p) forment un couple de suites réelles adjacentes. Elles convergent donc toutes deux vers une même limite λ.
Pour tout p, on a $\alpha_{p+1} \leqslant u_{\varphi(p)} \leqslant \beta_{p+1}$, ce qui permet par théorème d'encadrement de forcer $(u_{\varphi(p)})$ à converger aussi vers λ.
On a donc bien extrait *(explicitement* [5]*)* une sous-suite de (u_n) qui converge *(vers λ)*.



5. *la construction choisie ici la fait converger vers la plus petite valeur d'adhérence, il se peut qu'on ait le choix dans le cas de suites ayant plusieurs valeurs d'adhérence*

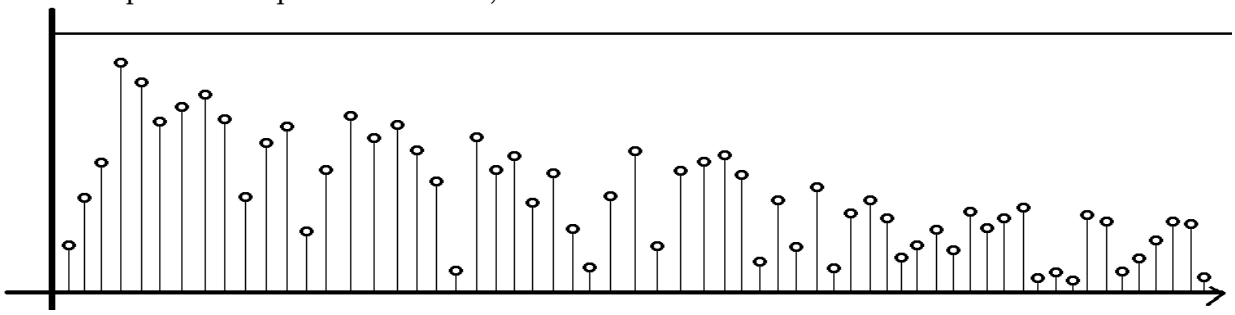
3.3.8 Théorème de Bolzano-Weierstrass (version complexe).

Théorème de Bolzano-Weierstrass complexe : de toute suite complexe bornée, on peut extraire au moins une sous-suite convergente.

On prend une suite complexe bornée (z_n) qu'on écrit sous la forme $(u_n + i.v_n)$ avec les deux suites u et v réelles.
Comme la suite z est bornée, les deux suites u et v le sont aussi.
Comme la suite (u_n) est bornée, on peut en extraire au moins une sous-suite $(u_{\varphi(p)})$ qui converge *(vers un réel λ)*.
La sous-suite $(v_{\varphi(p)})$ est alors bornée *(extraite d'une suite bornée)*. Par le théorème de Bolzano-Weierstrass réel, on peut en extraire une sous-(sous-)suite $(v_{\varphi(\psi(q))})$ qui converge *(vers un réel μ)*.
La sous-(sous-)suite $(u_{\varphi(\psi(q))})$ continue à converger vers λ.
Par théorème algébrique, $(u_{\varphi(\psi(q))} + i.v_{\varphi(\psi(q))})$ converge vers $\lambda + i.\mu$.
L'extraction $\varphi \circ \psi$ permet de faire converger une suite extraite de (z_n).

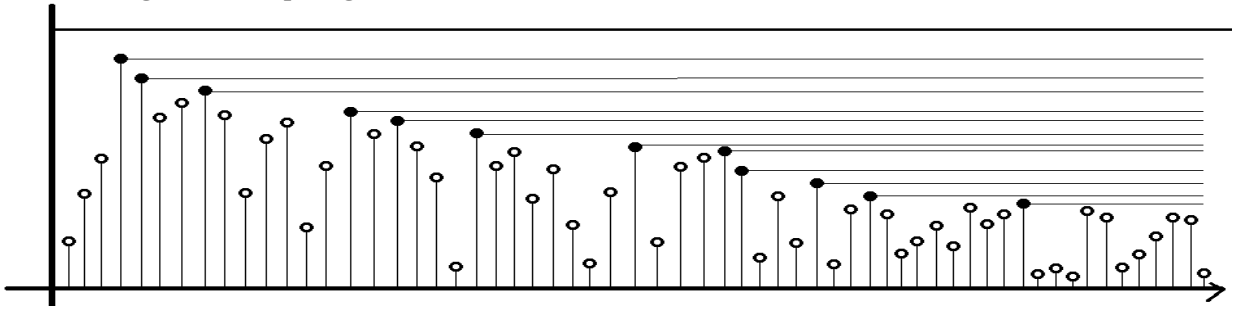
Les deux extractions doivent se faire l'une après l'autre et non pas "en parallèle".

Pour les suites réelles bornées, il existe aussi une autre démonstration :
si l'on ne peut pas extraire "facilement" une sous-suite décroissante, alors on peut extraire une sous-suite croissante.
On prend donc une suite réelle (u_n) bornée par α_0 et β_0.
On définit l'ensemble d'indices suivant : $\mathbb{A} = \{n \in \mathbb{N} \mid \forall p \geqslant n,\ u_p \leqslant u_n\}$ (il s'agit des indices des termes qui majorent tous les termes qui suivent).
$\mathbb{A}$ est une partie de $\mathbb{N}$ qui est soit infinie, soit finie.



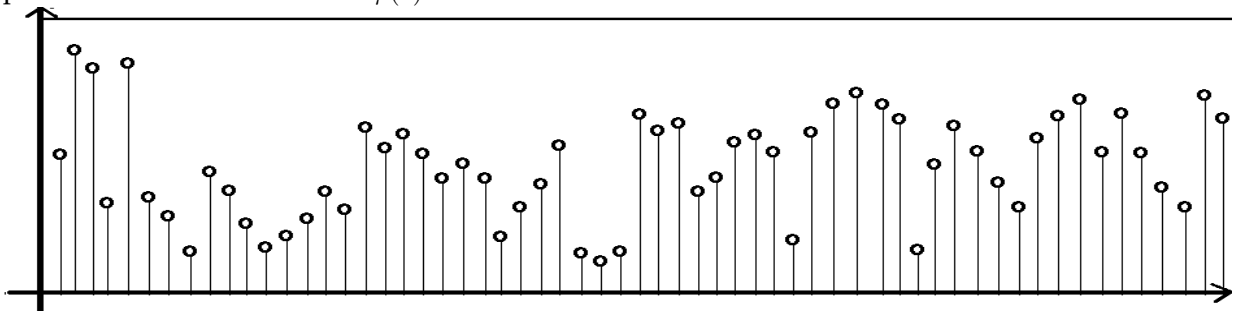
• **Premier cas :** si $\mathbb{A}$ est infini, alors on en indexe les éléments par ordre croissant : $\varphi \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{A} \\ n & \longmapsto & \varphi(n) \end{array}$
($\varphi(0)$ est le plus petit élément de $\mathbb{A}$, $\varphi(1)$ est le plus petit élément de $\mathbb{A} - \{\varphi(0)\}$ et ainsi de suite).

Par construction, chaque indice $\varphi(k)$ vérifie $\forall p \geqslant \varphi(k),\ u_p \leqslant u_{\varphi(k)}$; en particulier $u_{\varphi(k+1)} \leqslant u_{\varphi(k)}$.
La suite $(u_{\varphi(k)})$ est décroissante. Elle est extraite de la suite (a_n), donc elle est minorée.
Elle converge vers son plus grand minorant.

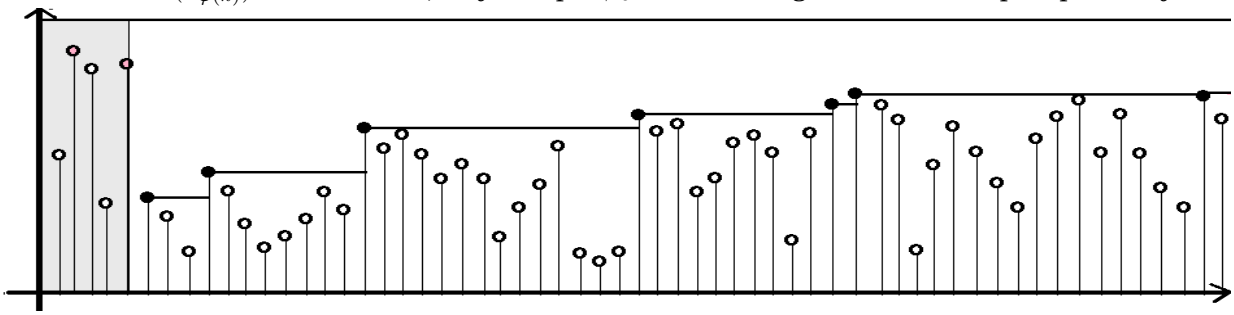


• **Second cas :** si $\mathbb{A}$ est fini, alors au delà d'un certain entier M, tous les entiers sont dans $\mathbb{A}^c$.
On pose alors $\varphi(0) = M + 1$. Par définition de $\varphi(0) \notin \mathbb{A}$, il existe au moins un élément p plus grand que $\varphi(0)$ vérifiant $u_p > u_{\varphi(0)}$. On prend le premier d'entre eux (qui ne peut pas être égal à $\varphi(0)$ par inégalité

stricte) et on le note $\varphi(1)$.
On recommence : $\varphi(1)$ n'est pas dans $\mathbb{A}$, il existe donc au moins un indice p vérifiant $u_p > u_{\varphi(1)}$. Le premier d'entre eux sera noté $\varphi(2)$.



De proche en proche, on construit φ vérifiant $\varphi(k+1) > \varphi(k)$ pour tout k (ainsi que $\varphi(k+1) > \varphi(k)$).
La sous-suite $(u_{\varphi(k)})$ est croissante, majorée (par β_0). Elle converge donc vers son plus petit majorant.

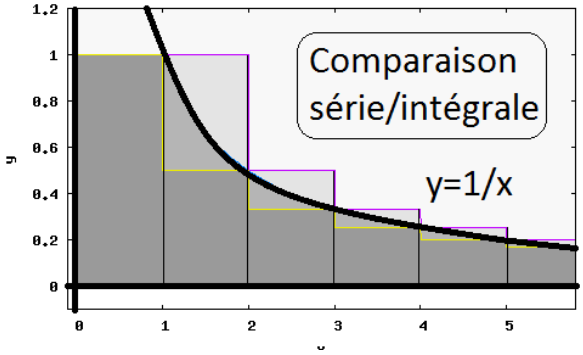


Dans les deux cas, on a construit une sous-suite monotone bornée, donc convergente.

3.4 Séries numériques.

3.4.1 Divergence de la série harmonique, équivalent simple.

La série harmonique est définie par $H_n = \sum_{k=1}^{n} \frac{1}{k}$
Cette série diverge vers $+\infty$ quand n tend vers $+\infty$.
On a même $H_n \sim_{n\to+\infty} \ln(n)$
Le plus classique est de faire une comparaison série intégrale.



k est un entier entre 1 et n. Par décroissance de $t \to \frac{1}{t}$, on a

$$\frac{1}{k+1} \leqslant \frac{1}{t} \leqslant \frac{1}{k}$$

pour tout t de $[k,\ k+1]$. On intègre de k à $k+1$:

$$\frac{1}{k+1} \leqslant \int_k^{k+1} \frac{dt}{t} \leqslant \frac{1}{k}$$

On somme l'inégalité de droite de $k=1$ à n

$$\int_1^{n+1} \frac{dt}{t} \leqslant H_n$$

et celle de gauche de 1 à $n+1$:

$$H_n - 1 \leqslant \int_1^{n} \frac{dt}{t}$$

En mettant bout à bout, on a l'encadrement $\ln(n+1) \leqslant H_n \leqslant 1+\ln(n)$
Par théorème de minoration, H_n diverge vers $+\infty$.

Si on divise par $\ln(n)$ on a aussi par encadrement : $\dfrac{H_n}{\ln(n)} \to 1$ c'est à dire $H_n \sim_{n\to+\infty} \ln(n)$.

Une autre preuve simple repose sur une estimation de $H_{2.n} - H_n$ avec minoration des $\dfrac{1}{k}$ par $\dfrac{1}{2.n}$:

$$H_{2.N} - H_n = \sum_{k=1}^{2.n} \frac{1}{k} - \sum_{k=1}^{n} \frac{1}{k} = \sum_{k=n+1}^{2.n} \frac{1}{k} \geqslant \sum_{k=n+1}^{2.n} \frac{1}{2.n} = n.\frac{1}{2.n}$$

On termine en disant que si la suite (H_n) convergeait vers un réel λ par passage à la limite on aurait $\lambda - \lambda \geqslant \dfrac{1}{2}$.

La suite est croissante et ne converge pas. la seule possibilité est « elle tend vers $+\infty$ ».

3.4.2 Comparaison série intégrale.

3.4.3 Séries de Riemann.

La série de terme général $\dfrac{1}{n^a}$ converge si et seulement si a est strictement plus grand que 1.
a est un réel fixé, et on considère la série de terme général $\dfrac{1}{n^a}$.
On étudie donc la suite des sommes partielles $\Big(\displaystyle\sum_{n=1}^{N} \frac{1}{n^a}\Big)_{N\in\mathbb{N}}$.
C'est une suite croissante puisqu'on passe d'une somme à la suivante en ajoutant un terme positif $(N+1)^{-a}$.
Pour a plus grand que 1 on effectue une comparaison série intégrale.
Pour chaque entier naturel n, et pour chaque t entre $n-1$ et n on a $t^{-a} \geqslant n^{-a}$ par décroissance de l'application.
On intègre de $n-1$ à n (intervalle de longueur 1) : $\int_{n-1}^{n} \frac{dt}{t^a} \geqslant \int_{n-1}^{n} \frac{dt}{n^a} = \frac{1}{n^a}$
On somme de 2 à N en appliquant la relation de Chasles sur les intégrales et on ajoute le terme 1 de chaque côté

$$1 + \Big[\frac{t^{1-a}}{1-a}\Big]_{t=1}^{N} = 1 + \int_1^N \frac{dt}{t^a} \geqslant 1 + \sum_{n=2}^{N} \frac{1}{n^a} = \sum_{n=1}^{N} \frac{1}{n^a}$$

Sachant que $1-a$ est négatif, le membre de gauche se majore même par $1 + \dfrac{1}{a-1}$.
La suite de droite est croissante, majorée, elle converge.

Pour a plus petit que 1, on peut refaire une comparaison série intégrale.
Mais il est plus simple d'écrire

$$\sum_{n=1}^{N} \frac{1}{n^a} \geqslant \sum_{n=1}^{N} \frac{1}{n}$$

et de rappeler que la série harmonique (membre de droite) diverge vers $+\infty$.

3.4.4 Séries à termes généraux positifs équivalents en $+\infty$.

Séries à termes généraux positifs équivalents en $+\infty$: soient deux suites (a_n) et (b_n) réelles strictement positives, équivalentes en $+\infty$[a], alors la série de terme général (a_n) est de même nature que la série de terme général (b_n)[b].

a. le quotient a_n/b_n tend vers 1
b. si l'une converge, l'autre converge aussi, si l'une diverge, l'autre diverge aussi

On considère deux suites réelles strictement positives *(ou pour le moins strictement positives à partir d'un certain rang) :* (a_n) *et* (b_n). Leurs séries associées sont notées (A_N) et (B_N) *(c'est à dire* $A_N = \sum_{n=0}^{N} a_n$*)*.
On suppose que le quotient bien défini $\frac{a_n}{b_n}$ converge vers 1 quand n tend vers l'infini.
On sait déjà que (A_N) et (B_N) sont croissantes ($A_{N+1} - A_N = a_N > 0$), elles convergent si et seulement si elles sont majorées.
Comme le quotient a_n/b_nconverge *(vers* 1*)*, il est majoré. On note β un de ses majorants.
Comme le quotient b_n/a_nconverge *(vers* 1*)*, il est majoré. On note α un de ses majorants.
On a donc $\alpha.a_n \leqslant b_n \leqslant \beta.a_n$ pour tout n *(produits en croix strictement positifs)*.
On somme de 0 à N *(entier naturel donné)* : $\alpha.A_N \leqslant B_N \leqslant \beta.A_N$.
Si la série (A_N) diverge, c'est en croissant vers $+\infty$ et la relation $\alpha.A_N \leqslant B_N$ pousse aussi B_N vers $+\infty$.
Si la série (B_N) diverge, c'est en croissant vers $+\infty$ et la relation $B_N \leqslant \beta.A_N$ pousse aussi $\beta.A_N$ *(et aussi* A_N*)* vers $+\infty$.
Les deux autres implications s'obtiennent par contraposée.

Attention, le théorème ne dit rien en revanche sur les valeurs des éventuelles limites.
On peut quand même approfondir : dans le cas où les deux divergent, on a alors $A_N \sim_{N\to+\infty} B_N$ *(vitesse de divergence des termes généraux)*, et dans le cas où les deux convergent $\sum_{n=N}^{+\infty} a_n \sim_{N\to+\infty} \sum_{n=N}^{+\infty} b_n$ *(vitesse de convergence des restes)*.

3.5 Applications continues.

3.5.1 Caractérisation par les suites de la continuité de f en a.

Caractérisation séquentielle de la continuité :
f est continue en a si et seulement elle transforme toute suite de limite a en suite de limite $f(a)$.

On va raisonner non pas par double implication, mais par $A \Rightarrow B$ suivi de $\overline{A} \Rightarrow \overline{B}$.

C'est le « seulement si » et « si ».

On suppose f continue en a :

$$\forall \varepsilon > 0,\ \exists \eta_{\varepsilon,a} > 0,\ \forall x,\ |x-a| \leqslant \eta_{\varepsilon,a} \Rightarrow |f(x) - f(a)| \leqslant \varepsilon$$

On prend une suite (u_n) qui converge vers a : $\forall \varepsilon > 0,\ \exists N_\varepsilon,\ \forall n,\ n \geqslant N_\varepsilon \Rightarrow |u_n - a| \leqslant \varepsilon$.
On montre que $(f(u_n))$ converge à son tour vers $f(a)$: $\forall \varepsilon > 0,\ \exists P_\varepsilon,\ \forall n,\ n \geqslant P_\varepsilon \Rightarrow |f(u_n) - f(a)| \leqslant \varepsilon$.
Il suffit de prendre pour εdonné : $P_\varepsilon = N_{\eta_{\varepsilon,a}}$ et d'enchaîner :

$$n \geqslant N_{\eta_{\varepsilon,a}} \Rightarrow |u_n - a| \leqslant \eta_{\varepsilon,a} \Rightarrow |f(u_n) - f(a)| \leqslant \varepsilon$$

On suppose f non continue en a :

$$\exists \varepsilon_0 > 0,\ \forall \eta > 0,\ \exists x_\eta,\ |x-a| \leqslant \mu \text{ et } |f(x) - f(a)| > \varepsilon_0$$

Comme ceci est valable pour tout η, on particularise avec $\eta = \dfrac{1}{n+1}$.

Pour chacun d'entre eux, il existe un x qu'on va nommer x_n, qui vérifie : $|x_n - a| \leqslant \dfrac{1}{n+1}$ et $|f(x_n) - f(a)| \geqslant \varepsilon_0$.
La première assertion assure par encadrement que la suite (x_n) converge vers a.
La seconde assure que la suite $(f(x_n))$ ne converge pas vers $f(a)$.

Le résultat suivant ne fait pas partie du cours mas se démontre de la même façon :
f est uniformément continue de I dans $\mathbb{R}$ si et seulement si pour tout couple de suites $((a_n),\ (b_n))$ à valeurs dans I, si $b_n - a_n$ tend vers 0 quand n tend vers l'infini, alors $f(a_n) - f(b_n)$ tend aussi vers 0.

3.5.2 Applications lipschitziennes sur un intervalle I de $\mathbb{R}$.

Applications lipschitziennes :
si f est lipschitzienne de I dans $\mathbb{R}$ (ou $\mathbb{C}$) alors elle est uniformément continue de I dans $\mathbb{R}$ (et donc continue en tout point de I).
Une somme d'applications lipschitziennes est lipschitzienne.
Une composée d'applications lipschitziennes est lipschitzienne.
Un produit d'applications lipschitziennes et bornées est lipschitzien.

On suppose qu'il existe un réel K vérifiant : $\forall (a,\ b) \in I^2,\ |f(b) - f(a)| \leqslant K.|b - a|$ (les taux d'accroissement sont majores).
On montre alors sans effort :

$$\forall \varepsilon > 0,\ \exists \eta_\varepsilon > 0,\ \forall (x,\ y) \in I^2,\ |x - y| \leqslant \eta_\varepsilon \Rightarrow |f(x) - f(y)| \leqslant \varepsilon$$

Il suffit en effet, pour ε fixe de poser $\eta_\varepsilon = \dfrac{\varepsilon}{K}$ (si K est nul, f est constante, et on n'a même pas besoin de choisir η_ε.

L'application $x \longrightarrow \sqrt{x}$ est uniformément continue de $[0,\ 1]$ dans $\mathbb{R}$ (utiliser le théorème de Heine, ou montrer proprement que $\eta_\varepsilon = \varepsilon^q$ convient) alors qu'elle n'est pas lipschitzienne (regarder pour K donne le taux d'accroissement entre 0 et $\frac{1}{(K+1)^q}$).

Le passage de la continuité uniforme à la continuité en tout point est direct :
si on a $\forall \varepsilon > 0,\ \exists \eta_\varepsilon > 0,\ \forall (x,\ y) \in I^2,\ |x - y| \leqslant \eta_\varepsilon \Rightarrow |f(x) - f(y)| \leqslant \varepsilon$
alors on a

$$\forall a \in I,\ \forall \varepsilon > 0,\ \exists \mu_{a,\varepsilon} > 0,\ \forall x \in I,\ |x - a| \leqslant \eta_\varepsilon \Rightarrow |f(x) - f(ay)| \leqslant \varepsilon$$

Si f est lipschitzienne de rapport K de I dans $\mathbb{R}$ et g de rapport H de I dans $\mathbb{R}$ également, alors on écrit pour tout couple $(a,\ b)$ de $I \times I$:

$$|(f+g)(b) - (f+g)(a)| \leqslant |f(b) - f(a)| + |g(b) - g(a)| \leqslant H.|b - a| + K.|b - a| = (H + K).|b - a|$$

Si f est lipschitzienne de rapport K de I dans J et g de rapport H de J dans $\mathbb{J}$, alors on écrit pour tout couple $(a,\ b)$ de $I \times I$:

$$|g(f(b)) - g(f(a))| \leqslant H.|f(b) - f(a)| \leqslant H.K.|b - a|$$

Si f est lipschitzienne de rapport K de I dans J et g de rapport H de I dans $\mathbb{R}$, alors on écrit pour tout couple $(a,\ b)$ de $I \times I$:

$$|g(b).f(b) - f(a).g(a)| = |g(b).f(b) - g(a).f(b) + g(a).f(b) - f(a).g(a)|$$

$$|g(b).f(b) - f(a).g(a)| \leq |g(b) - g(a)|.|f(b)| + |f(b) - f(a)|.|g(a)|$$

$$|g(b).f(b) - f(a).g(a)| \leq H.|b - a|.|f(b)| + K.|b - a|.|g(a)|$$

Si on suppose donc en sus que f est bornée (par $||f||$) et que g est bornée (par $||g||$), on aboutit à

$$|g(b).f(b) - f(a).g(a)| \leq (H.||f|| + K.||g||).|b - a|$$

C'est la définition de $g \times f$ est lipschitzienne puisque le réel $H.||f|| + K.||g||$ est bien indépendant de a et b.

On notera que sans l'hypothèse « bornées », on a un contre-exemple avec $x \longrightarrow x$ et $x \longrightarrow x$ de $\mathbb{R}$ dans lui même. Chacune est lipschitzienne, mais le produit ne l'est plus, car les taux tels que $\frac{b^2 - 0^2}{b - 0}$ ne sont pas bornés.

3.5.3 Théorème de la borne atteinte (premier théorème de compacité).

Toute application numérique continue sur un segment est bornée et atteint ses bornes.

On prend donc f continue de $[a,\ b]$ *(segment de* $\mathbb{R}$*)*, dans $\mathbb{R}$.
On va montrer déjà de deux façons qu'elle est majorée.

En appliquant ensuite le raisonnement à $-f$, on montrera ensuite qu'elle est bornée. A moins que vous ne préfériez l'appliquer à $|f|$ tout de suite.

Méthode utilisant le théorème de Bolzano Weierstrass.
On va établir : $\exists M \in \mathbb{R},\ \forall x \in [a,\ b],\ f(x) \leqslant M$ **par l'absurde**.
On suppose donc $\forall M \in \mathbb{R},\ \exists x \in [a,\ b],\ f(x) > M$.
En particulier pour tout n de $\mathbb{N}$, il existe un x de $[a,\ b]$ vérifiant $f(x) > n$. On en prend un qu'on nomme u_n.
On a ainsi construit une suite (u_n) de $[a,\ b]$ vérifiant $f(u_n) > n$ pour tout n.
C'est une suite réelle *(on est dans* $[a,\ b]$*)*, bornée *(par* a *et* b*)*.
Elle admet donc au moins une sous-suite $(u_{\varphi(n)})$ qui converge *(vers une limite réelle qu'on va noter* α*)*.
Comme pour tout n on a $a \leqslant u_{\varphi(n)} \leqslant b$, alors par passage *(large)* à la limite, α est dans $[a,\ b]$.
Comme f est continue en tout point de $[a,\ b]$, elle l'est en particulier en α et on a donc $f(u_{\varphi(n)}) \to_{n \to +\infty} f(\alpha)$.
Mais dans le même temps, la minoration $f(u_{\varphi(n)}) \geqslant \varphi(n) \geqslant n$ donne $f(u_{\varphi(n)}) \to_{n \to +\infty} +\infty$.
On tient notre contradiction.

Méthode utilisant juste le principe de la borne supérieure.
Pour tout n, on pose $A_n = \{x \in [a,\ b] \mid f(x) \geqslant n\}$ *(les points dont l'image dépasse* n*)*.
Chaque A_n est une partie de $\mathbb{R}$, majorée par b.
Si chacune est non vide *(c'est que que commence la preuve par l'absurde)*, alors chacune admet une borne supérieure *(plus petit majorant)*, que l'on note α_n.
Par continuité de f, chaque borne supérieure α_n est dans son A_n.

On étudie la limite à droite en α_n, comme les x plus grands que α_n sont hors de A_n, ils vérifient $f(x) < n$ et par passage à la limite, $f(\alpha_n) \leqslant n$. On étudie la limite à gauche en α_n, comme c'est la borne supérieure de A_n, il existe des éléments x de A_n inférieurs ou égaux à α_n vérifiant $f(x) \geqslant n$, et par passage à la limite, $f(\alpha_n) \geqslant n$. Par antisymétrie, $f(\alpha_n) = n$.

Comme A_{n+1} est inclus dans A_n, tout majorant de A_n est un majorant de A_{n+1}.
En particulier α_n est un majorant de A_{n+1}, et donc le plus petit majorant α_{n+1} est plus petit que α_n.
La suite (α_n) est donc décroissante.
Elle est minorée par a puisque tous les α_n sont dans $[a,\ b]$.
En tant que suite décroissante minorée, elle admet une borne inférieure que l'on va noter β.
Comme tous les α_n vérifient $a \leqslant \alpha_n \leqslant b$, la limite β est dans $[a,\ b]$.
Par continuité de f en β : $f(\alpha_n) \to_{n\to+\infty} \beta$.
Mais on avait $f(\alpha_n) \geqslant n$ pour tout n, et donc par minoration $f(\alpha_n) \to_{n\to+\infty} +\infty$.

On tient notre contradiction.
C'est donc qu'au moins un des A_n est vide, pour un certain entier N.
Ayant $\{x \in [a,\ b] \mid f(x) \geqslant n\} = \emptyset$, on a bien $\forall x \in [a,\ b],\ f(x) < n$.

On sait maintenant que l'ensemble image $\{f(x) \mid x \in [a,\ b]\}$ *(noté I)* est une partie de $\mathbb{R}$ majorée *(et non vide)*.
On note μ sa borne supérieure *(plus petit majorant)*. On va montrer que cette borne supérieure est atteinte, c'est à dire l'existence d'un γ de $[a,\ b]$ vérifiant $f(\gamma) = \mu$.
On se donne un entier naturel n. Par définition de "plus petit majorant", le réel $\mu - 2^{-n}$ n'est plus un majorant de I. Il existe donc au moins un élément x de $[a,\ b]$ vérifiant $\mu - 2^{-n} \leqslant f(x) \leqslant \mu$. On en note un c_n.
On a donc une suite (c_n) d'éléments de $[a,\ b]$ vérifiant $\mu - 2^{-n} \leqslant f(c_n) \leqslant \mu$ pour tout n.
Chaque c_n est dans $[a,\ b]$. On a donc une suite réelle bornée. On en extrait une sous-suite $(c_{\psi(n)})$ qui converge vers un certain γ *(qui est dans $[a,\ b]$ par passage à la limite sur "$a \leqslant c_n \leqslant b$ pour tout n")*.
Par continuité de f en γ : $f(c_{\psi(n)}) \to_{n\to+\infty} f(\gamma)$.
Par encadrement dans $\mu - 2^{-\psi(n)} \leqslant f(c_{\psi(n)}) \leqslant \mu$, on a $f(c_{\psi(n)}) \to_{n\to+\infty} \mu$.
Par unicité de la limite : $f(\gamma) = \mu$.
La borne supérieure de f sur $[a,\ b]$ est un maximum, atteint.

On fait de même avec la borne inférieure.

3.5.4 Théorème des valeurs intermédiaires.

Théorème des valeurs intermédiaires : soit f continue de $[a,\ b]$ (intervalle de $\mathbb{R}$) dans $\mathbb{R}$, alors toute valeur comprise entre $f(a)$ et $f(b)$ est atteinte au moins une fois par f entre a et b.

L'image d'un intervalle par une application numérique continue est encore un intervalle.

On commence par un lemme. Soit f continue de $[a,\ b]$ dans $\mathbb{R}$, négative en a et positive en b, alors f s'annule au moins une fois entre a et b.
Démonstration du lemme par principe de la borne supérieure.
On pose $A = \{x \in [a,\ b] \mid f(x) \leqslant 0\}$.
C'est une partie de $[a,\ b]$, donc une partie de $\mathbb{R}$.
Elle est non vide car elle contient au moins a.
Elle est majorée par b.
Elle admet donc une borne supérieure *(plus petit majorant)*, noté α.
On va montrer par double encadrement et continuité que $f(\alpha)$ est nul.
• Par définition de la borne supérieure, il existe une suite (γ_n) de points de A qui tend vers α. Par continuité de f en α : $f(\gamma_n) \to_{n\to+\infty} f(\alpha)$.
Par appartenance à A : $f(\gamma_n) \leqslant 0$ pour tout n. Par passage à la limite : $f(\alpha) \leqslant 0$.
• Par continuité et stricte positivité de f en b, il existe un intervalle $[b-\beta,\ b]$ sur lequel f est plus grande que $f(b)/2$ *(définition de la continuité avec $\varepsilon = f(b)/2 > 0$)*.
La borne supérieure α est donc inférieure ou égale à $b - \beta$, et donc elle n'est pas égale à b.

Les réels $\frac{n.\alpha+b}{n+1}$ sont donc strictement entre α et b, donc hors de A. Ainsi $f\left(\frac{n.\alpha+b}{n+1}\right) > 0$ pour tout n.
Cette suite tend vers α quand n tend vers l'infini. Par continuité sa limite est $f(\alpha)$, mais par passage à la limite, cette limite est positive ou nulle.
Par double inégalité, $f(\alpha)$ est nul.

Démonstration par dichotomie (suites adjacentes).
On pose $a_0 = a$ et $b_0 = b$.
Pour tout entier naturel n, on pose $c_n = \frac{a_n + b_n}{2}$ et on étudie le signe de $f(c_n)$.
Si $f(c_n)$ est négatif *(comme $f(a_n)$)*, on pose $a_{n+1} = c_n$ et $b_{n+1} = b_n$.
Si $f(c_n)$ est positif *(comme $f(b_n)$)*, on pose $a_{n+1} = a_n$ et $b_{n+1} = c_n$.
Par construction, les suites (a_n) et (b_n) sont adjacentes *((a_n) croît et (b_n) décroît et la différence $b_n - a_n$vaut $\frac{b-a}{2^n}$ et tend vers 0)*.
Elles convergent vers une même limite α.
Pour tout n, on a $f(a_n) \leqslant 0$ et $f(b_n) \geqslant 0$.
Par continuité elles convergent vers $f(\alpha)$.
Par passage à la limite, $f(\alpha)$ est à la fois négatif et positif. Il est nul.

Quitte à étudier $-f$, on peut montrer que si f *(continue)* change de signe entre a et b, alors elle s'annule au moins une fois.
La contraposée de ce résultat est parfois utile :
Si une application continue de $[a,\ b]$ dans $\mathbb{R}$ ne s'annule pas, alors elle reste de signe constant.

On prend maintenant une simple application continue f de $[a,\ b]$ dans $\mathbb{R}$.
On prend un certain réel γ entre $f(a)$ et $f(b)$.
On veut montrer que f atteint la valeur γ en au moins un point c de $[a,\ b]$.
On considère l'application auxiliaire $f - \gamma$ *(simple translation)*. Elle est encore continue de $[a,\ b]$ dans $\mathbb{R}$.
En a elle vaut $f(a) - \gamma$ et en b elle vaut $f(b) - \gamma$. Ces deux réels sont de signes opposés.
Par le lemme précédent *(démontré de deux façons)*, $f - \gamma$ s'annule au moins une fois. Au point c où elle s'annule, f prend la valeur intermédiaire γ.

On prend un intervalle I *("ensemble sans trou")* et une application continue f de I dans $\mathbb{R}$. Il faut montrer que $f(I)$ est un intervalle.
Comme un intervalle peut être d'une des diverses formes possibles $[\alpha,\ \beta]$, $[\alpha,\ \beta[$, $]\alpha,\ \beta]$, $]\alpha,\ \beta[$, $]\alpha,\ +\infty[$, $[\alpha,\ +\infty[$, $]-\infty,\ \beta]$, $]-\infty,\ \beta[$ et enfin $]-\infty,\ +\infty[$ *(et pourquoi pas $\emptyset$)*, il faut utiliser la caractérisation d'un intervalle : si deux réels u et v sont dans l'intervalle, alors tout réel t entre u et v est encore dans l'intervalle.
On prend donc u et v dans l'ensemble image $f(I)$, puis un réel t entre les deux. Objectif : t est dans $f(I)$, c'est à dire "*t a au moins un antécédent dans I*".
Comme u et v sont dans $f(I)$, ils s'écrivent respectivement $f(a)$ et $f(b)$ pour a et b dans I.
Mais alors le segment $[a,\ b]$ est inclus dans I car I est un intervalle. f est donc continue sur $[a,\ b]$.
Toute valeur comprise entre $f(a)$ et $f(b)$ *(comme justement t)* est atteinte au moins une fois en un point c de $[a,\ b]$, donc de I.

3.5.5 Injectivité et monotonie des applications numériques.

Injectivité et monotonie des applications numérique :
• si une application de $\mathbb{R}$ dans $\mathbb{R}$ est strictement monotone, alors elle est injective,
• si une application continue de $[a,\ b]$ dans $\mathbb{R}$ est injective, alors elle est monotone.

La première démonstration est de la pure logique ; on va montrer que toute application numérique strictement croissante est injective *(le cas "strictement décroissant" est similaire)*.
On montre le sens suivant de l'injectivité : $\forall(a,\ b),\ (a \neq b) \Rightarrow (f(a) \neq f(b))$.
On prend donc deux réels distincts a et b.
Comme l'ordre sur $\mathbb{R}$ est total, on n'a que deux possibilités : $a < b$ ou $b < a$.
Par stricte croissance de f, chaque cas conduit respectivement à $f(a) < f(b)$ ou $f(b) < f(a)$.
Dans tous les cas, on a bien $f(a) \neq f(b)$.

Pour la seconde, on va utiliser le théorème des valeurs intermédiaires sur une application auxiliaire.
On prend f de $[a,\ b]$ dans $\mathbb{R}$, que l'on suppose injective. Sans restreindre la généralité, on suppose $f(a) < f(b)$. On va montrer que f est strictement croissante sur tout l'intervalle et pas juste "*entre les deux extrémités*".
On prend donc x et y dans $[a,\ b]$ vérifiant $x < y$ *(objectif : $f(x) < f(y)$)*.
On construit l'application axillaire

$$t \to f\big((1-t).y + t.b\big) - f\big((1-t).x + t.a\big)$$

que l'on va noter φ *(pour t entre 0 et 1)*.
Quand t va de 0 à 1, le réel $(1-t).y + t.b$ *(respectivement $(1-t).x + t.a$)* restent entre y et b *(respectivement entre x et a)*, donc reste dans $[a,\ b]$. Il s'ensuit que par composition et soustraction, l'application φ est continue, de $[0,\ 1]$ dans $\mathbb{R}$.
On calcule $\varphi(0) = f(y) - f(x)$ et $\varphi(1) = f(b) - f(a)$ *(positif)*.
Par l'absurde, si $f(y)$ n'est pas plus grand que $f(x)$, alors $\varphi(0)$ est négatif ou nul.
Par le théorème des valeurs intermédiaires, il existe un t de $[0,\ 1]$ vérifiant $\varphi(t) = 0$.
On traduit pour ce t : $f\big((1-t).y + t.b\big) = f\big((1-t).x + t.a\big)$.
Par injectivité de f : $(1-t).y + t.b = (1-t).x + t.a$, soit $t = \dfrac{y-x}{(y-x)-(b-a)}$ *(simple calcul)*.
Ce réel est bien défini, car $y - x$ *(distance entre les abscisses)* est strictement plus petit que $b - a$ *(longueur de l'intervalle)*. Mais justement, le numérateur est positif et le dénominateur négatif, donc t est négatif.
C'est en contradiction avec "$t \in [0,\ 1]$".
C'est donc que $f(y)$ est bien plus grand que $f(x)$.

3.6 Calcul différentiel.

3.6.1 Théorème de Rolle.

Théorème de Rolle : soit φ continue de $[a,\ b]$ dans $\mathbb{R}$ et dérivable au moins sur $]a,\ b[$, vérifiant $\varphi(a) = \varphi(b)$, alors il existe au moins un point c de $]a,\ b[$ vérifiant $\varphi'(c) = 0$.

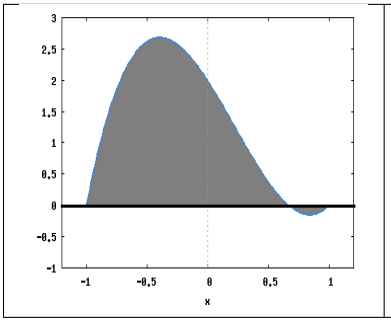
On commence par le théorème de Rolle, avec φ continue de $[a,\ b]$ dans $\mathbb{R}$ et dérivable au moins sur $]a,\ b[$.
On ajoute l'hypothèse $\varphi(a) = \varphi(b)$.
Par théorème de compacité *(continue sur un segment)*, φ est bornée et atteint ses bornes *(maximum atteint en α et minimum atteint en β)*.
• Si le maximum est atteint en α de $]a,\ b[$ *(ouvert)*, alors on étudie la dérivabilité de φ à droite de α et à gauche. Chaque $\dfrac{\varphi(\alpha)-\varphi(x)}{\alpha - x}$ pour x entre a et α est positif *(maximum)*. La limite quand x tend vers α par valeur inférieure est positive ou nulle (et c'est $\varphi'(\alpha)$). Chaque $\dfrac{\varphi(\alpha)-\varphi(x)}{\alpha - x}$ pour x entre α et b est négatif *(maximum)*. La limite quand x tend vers α par valeur supérieure est négative ou nulle *(et c'est encore $\varphi'(\alpha)$)*. Par antisymétrie, $\varphi'(\alpha)$ est nul.

• Si le maximum est atteint en α qui n'est pas dans $]a,\ b[$, c'est que α est en a ou en b puisque $\varphi(a) = \varphi(b)$.
On regarde alors le points β où le minimum est atteint, avec deux sous cas :

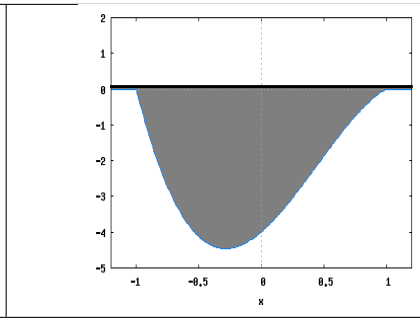
◦ β est strictement entre a et b. On refait alors le raisonnement précédent : chaque $\dfrac{\varphi(\beta)-\varphi(x)}{\beta-x}$ pour x entre a et β est négatif et la limite quand x tend vers β par valeur inférieure est positive ou nulle, tandis que chaque $\dfrac{\varphi(\beta)-\varphi(x)}{\beta-x}$ pour x entre β et b est négatif, la limite quand x tend vers β par valeur supérieure est positive ou nulle. Par antisymétrie de l'ordre, $\varphi'(\beta)$ est nul.

◦ β est en a ou b. φ est alors constante. Et sa dérivée est nulle en tout point de $]a,\ b[$.
Dans nos différents cas et sous cas, il suffit de prendre $c=\alpha$ ou $c=\beta$ ou enfin $c=\dfrac{a+b}{2}$, on a bien $\varphi'(c)=0$.

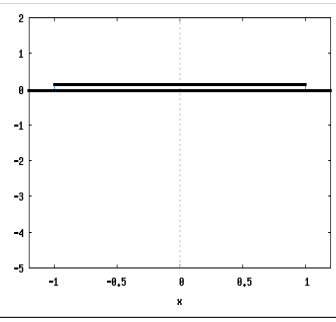
Pour les applications de $\mathbb{R}$ dans $\mathbb{C}$, le résultat n'est plus valable comme le prouve l'application $x\to e^{i.x}$ sur le segment $[0,\ 2.\pi]$.



cas $\alpha\in]a,\ b[$



cas $\alpha=a$, $\beta\in]a,\ b[$



cas $\alpha=a$ et $\beta=b$

3.6.2 Théorème des accroissements finis.

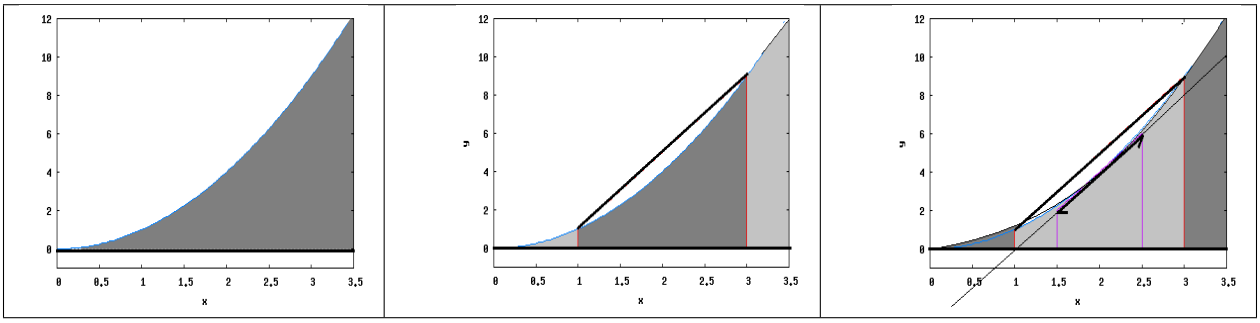
Théorème des accroissements finis : soit f continue de $[a,\ b]$ dans $\mathbb{R}$ et dérivable au moins sur $]a,\ b[$, alors il existe au moins un point c de $]a,\ b[$ vérifiant

$$f(b)-f(a)=f'(c).(b-a)$$

Si l'on n'a plus d'hypothèse $f(a)=f(b)$, on peut créer une fonction auxiliaire qui étudie en fait la distance entre la corde et le graphe :

$$x\to f(x)-\Big(\frac{f(b)-f(a)}{b-a}.(x-a)+f(a)\Big)$$

que l'on va noter φ.
Cette application est continue sur $[a,\ b]$, dérivable au moins sur $]a,\ b[$, et surtout, vérifie $\varphi(a)=\varphi(b)$ *(d'ailleurs égal à 0)* par construction.
Le théorème de Rolle donne l'existence d'au moins un c vérifiant $\varphi'(c)=0$. Cette dernière égalité donne précisément $f'(c)=\dfrac{f(b)-f(a)}{b-a}$.



le graphe	la corde	la tangente

une accroissement infinitésimal coïncide avec un accroissement “fini”, ce qui s’écrit $\left(\frac{dy}{dx}\right)_{x=c} = \frac{\Delta y}{\Delta x}$

3.6.3 Théorème de Rolle en cascade.

Théorème de Rolle en cascade : soit f n fois dérivable de I (intervalle de $\mathbb{R}$) dans $\mathbb{R}$, admettant la même valeur en $n+1$ points, alors il existe au moins un point où $f^{(n)}$ s’annule.

Le théorème de Rolle en cascade se démontre par récurrence sur le nombre de points où la fonction prend la même valeur.
Le cas $n = 0$ correspond exactement au théorème de Rolle : la fonction dérivable qui prend la même valeur en deux points a une dérivée qui s’annule au moins une fois.

Pour l’hérédité, on suppose que toute application numérique qui prend la même valeur en $n+1$ points d’un intervalle a sa dérivée n^{ieme} qui s’annule au moins une fois. On prend alors une application f *($n+1$ fois dérivable)* qui prend la même valeur en $n+2$ points d’un intervalle, qu’on va noter a_0 jusqu’à a_{n+1}, et qu’on va supposer triés par ordre croissant.
On applique le théorème de Rolle sur chacun des intervalles $[a_k,\ a_{k+1}]$ *(f y est continue, dérivable, et prend la même valeur aux deux extrémités)*. Pour chacun, il existe au moins un point α_k de l’intervalle ouvert $]a_k,\ a_{k+1}[$ où f' s’annule :

$$a_0 < \alpha_0 < a_1 < \alpha_1 < a_2 \ldots < \alpha_n < a_{n+1}$$

L’application f' est alors $n+1$ fois dérivable et prend la même valeur *(nulle)* en $n+1$ points distincts *(les α_k pour k de 0 à n)*. Par hypothèse de récurrence, sa dérivée n^{ieme} s’annule au moins une fois.

3.6.4 Sens de variation d’une fonction numérique dérivable sur un intervalle.

Théorème sur les variations des fonctions sur un intervalle par le signe de la dérivée : une application numérique dérivable dont la dérivée est positive sur un intervalle y est croissante.

On prend à présent f dérivable de I *(intervalle de $\mathbb{R}$)* dans $\mathbb{R}$, et on suppose f' positive ou nulle sur I.
On va prouver “directement” que f est croissante.
On se donne a et b dans I vérifiant $a < b$ (objectif $f(a) < f(b)$).
On est en droit sous nos hypothèses d’appliquer le théorème des accroissements finis à f entre a et b : il existe un c vérifiant $f(b) - f(a) = (b-a).f'(c)$. Tous les termes du second membre sont positifs, le premier membre l’est aussi, et c’était notre objectif.

Le sens “f dérivable et croissante implique f' positive” est bien plus simple à prouver, puisqu’il résulte d’un passage à la limite (dont l’existence est supposée) dans les taux d’accroissement de la forme

$\frac{f(x+h)-f(x)}{h}$ quand h tend vers 0.

3.6.5 Formule de L'Hospital (hors-programme car on peut s'en passer).

Formule de l'Hospital : si f et g sont continues de $[a,\ b]$ dans $\mathbb{R}$, dérivables au moins sur $]a,\ b[$, avec g' strictement positive, alors il existe au moins un point c vérifiant

$$\frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(c)}{g'(c)}$$

Cette fois, on a f et g continues de $[a,\ b]$ dans $\mathbb{R}$, dérivables au moins sur $]a,\ b[$, et on suppose de plus g' strictement positive sur $]a,\ b[$.
Il s'ensuit que g est strictement croissante, on a donc $g(b) > g(a)$.

On n'obtient pas le résultat voulu en appliquant le théorème des accroissements finis à f puis à g, il faut un "changement d'échelle commun".

On définit l'application auxiliaire φ inspirée de la preuve du théorème des accroissements finis

$$x \to f(x) - \Big(\frac{f(b)-f(a)}{g(b)-g(a)}.\big(g(x)-g(a)\big) + f(a)\Big)$$

Elle est continue de $[a,\ b]$ dans $\mathbb{R}$, dérivable sur $]a,\ b[$, et prend la même valeur *(nulle)* en a et b. Sa dérivée $x \to f'(x) - \frac{f(b)-f(a)}{g(b)-g(a)}.g'(x)$ s'annule au moins une fois en un point c de $]a,\ b[$. En ce point, on a par produits en croix : $\frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(c)}{g'(c)}$.

Dans le cas où g est l'application identité, on retrouve le théorème des accroissements finis.

3.6.6 Existence des développements limités pour une application n fois dérivable en a.

Existence de développement limite :
si f est n fois dérivable en a, alors elle admet en a un développement limite d'ordre n, de la forme

$$f(a+h) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k + o(h^n)$$

quand h tend vers 0.

Les hypothèses sont
- définie sur un voisinage de a : $[a-\alpha,\ a+\alpha]$,
- à valeurs dans $\mathbb{R}$ (ou même $\mathbb{C}$),
- $n-1$ fois dérivable sur ce voisinage
- et même encore une fois en a (et pas forcément ailleurs, mais dans tous presque les cas que l'on traite, f sera C^∞.

La vraie formulation du développement limité est $\dfrac{f(a+h) - \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)}{h^n} = o(1)$ ou si vous avez du mal avec les notations rigoureuses des o :

$$\frac{f(a+h) - \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)}{h^n} \underset{h \to 0}{\longrightarrow} 0$$

Pour que cette formule ait un sens, il faut $h \in]0,\ \alpha]$ ou $h \in [-\alpha,\ 0[$, pour la cohérence, et ceci est totalement compatible avec « h tend vers 0 ».

On va poser dans nos deux démonstration (oui, je vous en offre deux) :

$$\varphi = h \longrightarrow f(a+h) - \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)$$

C'est la fonction différence entre f et son développement de Taylor.
Et c'est elle qui va devoir tendre très très vite vers 0.

Méthode utilisant la règle de l'Hospital :
Comme on a des hypothèses de dérivabilité suffisantes, on peut remplacer :

$$\frac{f(a+h) - \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)}{h^n} = \frac{\varphi(h)}{h^n} = \frac{\varphi'(c)}{n.c^{n-1}} = \frac{\varphi"(d)}{n.(n-1).d^{n-2}} = \frac{\varphi^{(3)}(e)}{n.(n-1).(n-2).e^{n-3}}$$

et on continue jusqu'à $\frac{\varphi^{(n-1)}(t)}{n!.t}$ pour un t convenable entre 0 et h.
Que reste-t-il dans $\varphi^{(n-1)}$? déjà $f^{(n-1)}(a+t)$ et du polynôme il ne reste que

$f(a+h)$	et	$f(a)$	$+h.f'(a)$	$+\frac{h^2}{2}.f"(a)$	$+\frac{h^3}{6}.f^{(3)}(a)$	$+\ldots$	$+\frac{h^k}{k!}.f^{(k)}(a)$	$+\ldots$	$+\frac{h^n}{n!}.f^{(n)}(a)$
$f'(a+h)$			$f'(a)$	$+h.f"(a)$	$+\frac{h^2}{2}.f^{(3)}(a)$	$+\ldots$	$+\frac{h^{k-1}}{(k-1)!}.f^{(k)}(a)$	$+\ldots$	$+\frac{h^{n-1}}{(n-1)!}.f^{(n)}(a)$
$f"(a+h)$				$f"(a)$	$+h.f^{(3)}(a)$	$+\ldots$	$+\frac{h^{k-2}}{(k-2)!}.f^{(k)}(a)$	$+\ldots$	$+\frac{h^{n-2}}{(n-2)!}.f^{(n)}(a)$
$\ldots$					$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$f^{(n-1)}(a+h)$								$f^{(n-1)}(a)$	$+h.f^{(n)}(a)$
$f^{(n)}(a+h)$									$f^{(n)}(a)$

On a donc

$$\frac{f(a+h) - \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)}{h^n} = \frac{f^{(n-1)}(a+h) - f^{(n-1)}(a) - h.f^{(n)}(a)}{n!.h} = \frac{1}{n!}.\Big(\frac{f^{(n-1)}(a+t) - f^{(n-1)}(a)}{t} - f^{(n)}(a)\Big)$$

Quand h tend vers 0, t le fait aussi et $\frac{f^{(n-1)}(a+t) - f^{(n-1)}(a)}{t}$ tend $f^{(n)}(a)$. La différence tend vers 0, et la « constante » $n!$ n'y change rien.

Bref, $\frac{f(a+h) - \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)}{h^n}$ tend vers 0 quand h tend vers 0.

C'est la définition de « je suis un petit o de h^n ». ☺

○ *Avec cette preuve dans laquelle on applique $n-1$ fois la formule simple de l'Hospital, on comprend que le développement limité d'ordre n est un résultat d'une grande précision. Plus n est grand, plus c'est fin.*

○ *On me demandera peut être : pourquoi ne pas être allé jusqu'à ce qui suit*

$$\frac{f(a+h) - \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)}{h^n} = \frac{\varphi(h)}{h^n} = \frac{\varphi'(c)}{n.c^{n-1}} = \ldots = \frac{\varphi^{(n-1)}(t)}{n!.t} = \frac{\varphi^{(n)}(u)}{n!} = \frac{f^{(n)}(a+u) - f^{(n)}(a)}{n!}$$

C'est alors facile : quand h tend vers 0, u tend aussi vers 0 et $f^{(n)}(a+u) - f^{(n)}(a)$ tend vers 0. facile, non ? facile, mais demandant une hypothèse plus forte que le théorème que j'ai énoncé et encadré. Dans votre preuve, vous avez besoin de f est de classe C^n (la dérivée n^{ieme} existe partout sur $[a-\alpha,\ a+\alpha]$ et elle est continue) ; moi, j'ai juste besoin de « la dérivée n^{ieme} existe en a ». C'est moins exigeant.

Preuve par accroissements finis.
C'est presque la même. On applique le théorème des accroissements finis à φ *(la fonction du numérateur)* entre $à$ et h, puis à φ' et ainsi de suite.
On agrandit un peu notre tableau plus haut avec des informations :
$\varphi(0)=0$, $\varphi'(0)=0$, $\varphi"(0)=0$ jusqu'à $\varphi^{(n-1)}(0)=0$.

fonction	calcul		
φ	$\varphi(0)=0$	entre 0 et h	$\exists\theta_1\in]0,\ 1[,\ \varphi(h)-\varphi(0)=h.\varphi'(\theta_1.h)$
φ'	$\varphi'(0)=0$	entre 0 et $\theta_1.h$	$\exists\theta_2\in]0,\ 1[,\ \varphi'(\theta_1.h)-\varphi'(0)=\theta_1.h.\varphi"(\theta_2.\theta_1.h)$
$\varphi"$	$\varphi"(0)=0$	entre 0 et $\theta_2.h$	$\exists\theta_3\in]0,\ 1[,\ \varphi"(\theta_2.\theta_1.h)-\varphi"(0)=\theta_1.\theta_2.h.\varphi^{(3)}(\theta_3.\theta_2.\theta_1.h)$
			...

Quand ensuite on reporte ces lignes les unes dans les autres, on obtient

$$\varphi(h)=h.\varphi'(\theta_1.h)=h^2.\theta_1.\varphi"(\theta_2.\theta_1.h)=h^3.(\theta_1)^2.\theta_2.\varphi^{(3)}(\theta_3.\theta_2.\theta_1.h)=h^4.(\theta_1)^3.(\theta_2)^2.\theta_3.\varphi^{(3)}(\theta_4.\theta_3.\theta_2.\theta_1.h)$$

Qu'obtient on à la $(n-1)^{ieme}$ itération ?

$$\varphi(h)=h^{n-1}.(\theta_1)^{n-1}.(\theta_2)^{n-2}.(\theta_3)^{n-3}\dots\theta_{n-1}.\varphi(\theta_n.\theta_{n-1}\dots\theta_1.h)$$

On va poser $\Theta_n=\theta_n.\theta_{n-1}\dots\theta_1$ *(entre 0 et 1)* et même $\vartheta_n=(\theta_1)^{n-1}.(\theta_2)^{n-2}.(\theta_3)^{n-3}\dots\theta_{n-1}$ *(l'un est un θ majuscule, et l'autre est un θ calligraphique)*.
Mais $\varphi^{(n-1)}$ est encore dérivable en a *(et juste en a)* de dérivée nulle en 0. On peut donc écrire un développement limité d'ordre 1 *(définition de la dérivabilité autrement que par le calcul)* :

$$\varphi^{(n-1)}(\Theta_n.h)=\varphi^{(n-1)}(0)+\Theta_n.h.\varphi^{(n)}(0)+o(\Theta_n.h)_{h\to0}=o(\Theta_n.h)_{h\to0}$$

On reporte tout : $\varphi(h)=\vartheta_n.h^{n-1}.o(\Theta_n.h)_{h\to0}$. Il reste à dire que tous ce qui s'appelle θ avec ou sans majuscule, $\varphi(h)=o(h^n)_{h\to0}$.

3.6.7 Formule de Taylor avec reste de Lagrange (hors programme).

Formule de Taylor avec reste de Lagrange :
Pour f $n+1$ fois dérivable de $[a,\ a+h]$ dans $\mathbb{R}$, on a

$$\exists\theta\in]0,\ 1[,\ f(a+h)=\sum_{k=0}^{n}\frac{h^k}{k!}.f^{(k)}(a)+\frac{h^{n+1}}{(n+1)!}.f^{(n+1)}(a+\theta.h)$$

Pour f $n+1$ fois dérivable de $[a,\ b]$ dans $\mathbb{R}$, on a

$$\exists c\in]a,\ b[,\ f(b)=\sum_{k=0}^{n}\frac{(b-a)^k}{k!}.f^{(k)}(a)+\frac{h^{n+1}}{(n+1)!}.f^{(n+1)}(c)$$

La formule n'est pas valable pour les fonctions à valeurs dans $\mathbb{C}$.

On peut obtenir la formule en une seule étape, avec une fonction bien choisie, mais pas évidente à construire soi même.
a et b donnés, on définit $\phi=x\longrightarrow\sum_{k=0}^{n}f^{(k)}(x).\frac{(b-x)^k}{k!}$ et $\psi=x\longrightarrow\frac{(b-x)^{n+1}}{(n+1)!}$:

On la dérive, elle télescope génialement (faites le) : $\phi' = x \longrightarrow f^{(n+1)}(x).\dfrac{(b-x)^n}{n!}$.

Et $\psi' = x \longrightarrow -\dfrac{(b-x)^n}{n!}$

On lui applique alors le théorème de l'Hôpital au quotient $\dfrac{\phi(b)-\phi(a)}{\psi(b)-\psi(a)}$ entre a et b :

il existe c vérifiant $\dfrac{\phi(b)-\phi(a)}{\psi(b)-\psi(a)} = \dfrac{\phi'(c)}{\psi'(c)}$.

On remplace par leurs valeurs : $\dfrac{f(b)-\sum_{k=0}^{n} f^{(k)}(a).\dfrac{(b-a)^k}{k!}}{-\dfrac{(b-a)^{n+1}}{(n+1)!}} = \dfrac{\dfrac{(b-c)^n}{n!}.f^{(n+1)}(c)}{-\dfrac{(b-c)^n}{n!}}$ *(attention, dans $\phi(b)$ il reste un terme)*.

On simplifie les $(b-c)^n$ et les factorielles $\dfrac{f(b)-\sum_{k=0}^{n} f^{(k)}(a).\dfrac{(b-a)^k}{k!}}{\dfrac{(b-a)^{n+1}}{(n+1)!}} = f^{(n+1)}(c)$.

On fait passer de l'autre côté, et on tient la formule !

Démonstration totalement hors programme car nécessitant d'utiliser la règle de l'Hospital, et le recours à une fonction artificielle.

Bonus hors programme, pour vous entrainer :

prenez cette fois la même fonction ϕ et remplacer ψ par $x \longrightarrow \dfrac{(b-a)^{n+1-p}}{(n+1-p)!}$, appliquez encore le théorème de l'Hospital et vous avez la formule de Taylor-Schlömilch :

$$\exists c \in]a,\ b[,\ f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k}.f^{(k)}(a) + \frac{(b-c)^p.(b-a)^{n+1-p}}{n!.(n+1-p)}..f^{(n+1)}(c)$$

Pour p égal à 0, c'est notre formule, et pour $p = n$, elle porte le nom de formule de Taylor avec reste de Cauchy.

Je dois vous avouer n'avoir trouvé aucun sujet de concours allant chercher ce résultat.

Complément plus intéressant : la comparaison des formules de Taylor :

$f(a+h) =$	$\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)$	$+\frac{h^{n+1}}{n!}.\int_0^1 (1-t)^n.f^{(n+1)}(a+t.h).dt$	intégrale
$f(a+h) =$	$\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)$	$+\frac{h^{n+1}}{(n+1)!}.f^{(n+1)}(a+\theta.h)$	Lagrange
$\left\lvert f(a+h) -\right.$	$\left.\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)\right\rvert$	$\leqslant \frac{\lvert h\rvert^{n+1}}{(n+1)!}.\lvert\lvert f_{n+1}\rvert\rvert$	Lagrange
$f(a+h) =$	$\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)$	$+o(h^n)_{h\to 0}$	Young (D.L.)

Elles se ressemblent.

• Si on part de la formule de Taylor avec reste intégrale et qu'on majore $f^{(n+1)}(a+t.h)$ dans l'intégrale par $||f^{(n+1)}||$ puis intègre $\dfrac{1}{n!}.\int_0^1 (1-t)^n.dt = \dfrac{1}{(n+1)!}$, on obtient l'inégalité de Taylor-Lagrange.

• Si on part de l'égalité de Taylor Lagrange et qu'on majore le reste, on trouve l'égalité de Taylor-Lagrange.

• Si on part de la formule avec reste intégrale et qu'on dit que $f^{(n+1)}$ est constante, on trouve la formule de Taylor Lagrange.

• La formule avec reste intégrale prend une moyenne pondérée le long d'un intervalle, alors que Taylor Lagrange va la chercher en un point.
• Si on dit que $\frac{|h|^{n+1}}{(n+1)!}.||f^{(n+1)}||$ est un $O(h^{n+1})$, on peut le faire dégénérer en $o(h^n)$ [6] moins précis, et on a la formule de Taylor Young, appelée aussi développement limité.

Mais elles ont des hypothèses différentes.

$f(a+h) =$	$\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a) \quad + \frac{h^{n+1}}{n!}.\int_0^1 (1-t)^n.f^{(n+1)}(a+t.h).dt$	intégrale
	f est C^{n+1} sur $[a,\ b]$ (continuité de $f^{(n+1)}$)	
$f(a+h) =$	$\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a) \quad + \frac{h^{n+1}}{(n+1)!}.f^{(n+1)}(a+\theta.h)$	Lagrange
	f est D^{n+1}, (existence de $f^{(n+1)}$ c'est tout)	
$\left\|f(a+h) -$	$\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)\right\| \quad \leqslant \frac{\|h\|^{n+1}}{(n+1)!}.\|\|f_{n+1}\|\|$	Lagrange
	f est D^{n+1} et même à valeurs dans $\mathbb{C}$	
$f(a+h) =$	$\sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a) \quad + o(h^n)_{h\to 0}$	Young (D.L.)
	f est juste D^{n-1} et une fois encore dérivable en a	

La formule avec reste intégrale a besoin de la continuité de $f^{(n+1)}$ pour pouvoir intégrer par parties.

C'est la formule de Taylor-Young *(développement limité)* qui en demande le moins, pas besoin de dérivée $(n+1)^{ieme}$. Mais en même temps, c'est celle qui sert le moins. Elle sert juste à lever des formes indéterminées.

Et des applications différentes. Les deux premières formules sont des égalités. On peut les appliquer en n'importe quel point. Et elles donnent le signe du reste, une majoration...
L'inégalité de Taylor Lagrange majore le reste mais n'en donne pas le signe.
La formule de Taylor-Young permet juste de calculer les limites et lever des indéterminations, obtenir des équivalents. Mais vous ne pouvez pas l'utiliser pour $h$donné. Même « petit » avec les tonnes de guillemets. Le seul h pour lequel elle donne une égalité est $h=0$. Mais sinon, elle dit juste que la méga indétermination $\frac{f(b) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k}{h^n}$ tend quand même vers 0 quand h tend vers 0.

3.7 Calcul intégral.

3.7.1 Intégration par parties.

Intégration par parties : si u et v sont deux applications de classe C^1 [a] de $[a,\ b]$ dans $\mathbb{R}$ (ou même $\mathbb{C}$), alors on a

$$\int_a^b u'(t).v(t).dt = \Big[u(t).v(t)\Big]_{t=a}^{t=b} - \int_a^b u(t).v'(t).dt$$

a. applications dérivables dont les dérivées sont aussi continues

6. si, il existe des termes qui sont $o(h^n)$ mais pas encore $O(h^{n+1})$, comme $h^{n+\frac{1}{2}}$, et je veux que les plus faibles comprennent au moins cette échelle en 0 et ne soient pas à chaque fois à devoir apprendre par cœur des trucs sans les « voir »

On écrit $\int_a^b u'(t).v(t).dt = \int_a^b \Big(u'(t).v(t) + u(t).v'(t)\Big).dt - \int_a^b u(t).v'(t).dt$.
Le terme $\int_a^b \Big(u'(t).v(t) + u(t).v'(t)\Big).dt$\$ est de la forme $\int_a^b f'(t).dt$ avec $f = u.v$. Il se calcule en $\Big[f(t)\Big]_{t=a}^{t=b}$.

3.7.2 Formule de Taylor avec reste intégrale.

Formule de Taylor avec reste intégrale : soit f de classe C^{n+1} [a] de $[a,\ a+h]$ dans $\mathbb{R}$, alors

$$f(a+h) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k + \frac{h^{n+1}}{n!}.\int_0^1 (1-t)^n.f^{(n+1)}(a+t.h).dt$$

Inégalité de Taylor-Lagrange : si f est de classe C^{n+1} avec sa dérivée $n+1^{ieme}$ bornée en valeur absolue par M_{n+1} sur $[a,\ a+h]$ au moins, alors on a

$$\left|f(a+h) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k\right| \leqslant \frac{M_{n+1}.|h|^{n+1}}{(n+1)!}$$

a. f est $n+1$ fois dérivable et sa dérivée $n+1^{ieme}$ est continue

La démonstration la plus naturelle se fait par récurrence sur n.
Pour l'initialisation à $n=0$, on prend f dérivable à dérivée continue. On calcule l'intégrale $\int_0^1 h.f'(a+t.h).dt$ qui s'intègre précisément en $\Big[f(a+t.h)\Big]_{t=0}^{t=1}$ *(il suffit de dériver $t \to f(a+t.h)$).* On a donc bien $\int_0^1 h.f'(a+t.h).dt = f(a+h) - f(a)$ et il ne reste qu'à faire passer $f(a)$ de l'autre côté.

On suppose à un ordre n que la formule est correcte, et on suppose de surcroît que f est de classe C^{n+2}.
On calcule l'intégrale $\int_0^1 \frac{(1-t)^n}{n!}.h^{n+1}.f^{(n+1)}(a+t.h).dt$ par parties :

$$\left[\begin{array}{ccc} \frac{(1-t)^n}{n!} & \leftarrow & -\frac{(1-t)^{n+1}}{(n+1)!} \\ h^{n+1}.f^{(n+1)}(a+t.h) & \rightarrow & h^{n+2}.f^{(n+2)}(a+t.h) \end{array}\right]$$ *(fonctions continues de t)*

Le terme

$$\Big[-h^{n+1}.f^{(n+1)}(a+t.h).\frac{(1-t)^{n+1}}{(n+1)!}\Big]_{t=0}^{t=1}$$

donne uniquement $h^{n+1}.\frac{f^{(n+1)}(a)}{(n+1)!}$ qui fait passer $\sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k$ à $\sum_{k=0}^{n+1} \frac{f^{(k)}(a)}{k!}.h^k$.

Le terme

$$\int_0^1 \frac{(1-t)^{n+1}}{(n+1)!}.h^{n+2}.f^{(n+2)}(a+t.h).dt$$

avec ses deux signes moins est le reste d'ordre $n+1$.
La récurrence s'achève ainsi.

La démonstration judicieuse passe par la définition d'une application bien choisie à a, h et n fixés.
On définit donc $\varphi = t \to \sum_{k=0}^{n} \frac{(1-t)^k}{k!}.h^k.f^{(k)}(a+t.h)$ *(définie et dérivable sur $[0,\ 1]$).*
On calcule : $\varphi(0) = \sum_{k=0}^{n} \frac{h^k}{k!}.f^{(k)}(a)$ et $\varphi(1) = f(a+t.h)$ [7].

7. rappelons que $(1-1)^0$ vaut 1 ainsi que 0!

On dérive : $\varphi = t \to \sum_{k=0}^{n} \Big(-\frac{k.(1-t)^{k-1}}{k!}.h^k.f^{(k)}(a+t.h) + \frac{(1-t)^k}{k!}.h^{k+1}.f^{(k+1)}(a+t.h)\Big)$ *(dérivée d'une somme de produits)*.

En séparant en deux et en ré-indexant la première somme $-\sum_{k=0}^{n} \frac{k.(1-t)^{k-1}}{k!}.h^k.f^{(k)}(a+t.h)$ *(qui ne contient plus de terme d'indice* 0*)*, on a une somme télescopique où il ne reste que le terme $\frac{(1-t)^k}{k!}.h^{k+1}.f^{(k+1)}(a+t.h)$ pour k égal à $n+1$.

En écrivant $\varphi(1) - \varphi(0) = \int_0^1 \varphi(t).dt$, on obtient la formule de Taylor avec reste intégrale.

Cette formule est valable aussi pour les fonctions à valeurs complexes.

On prend f $n+1$ fois dérivable avec f^{n+1} bornée en valeur absolue par M_{n+1}.
On écrit la formule de Taylor avec reste intégrale, on fait passer la somme de l'autre côté.
La distance $\Big|f(a+h) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}.h^k\Big|$ est alors égale à

$$\Big| \int_0^1 \frac{(1-t)^n}{n!}.h^{n+1}.f^{(n+1)}(a+t.h).dt\Big|$$

Par inégalité triangulaire *(valeur absolue de l'intégrale plus petite que l'intégrale de la valeur absolue)*, on majore par

$$\int_0^1 \Big|\frac{(1-t)^n}{n!}.h^{n+1}.f^{(n+1)}(a+t.h)\Big|.dt$$

On sort de la valeur absolue ce qui est déjà assurément positif :

$$\int_0^1 \frac{(1-t)^n}{n!}.|h|^{n+1}.|f^{(n+1)}(a+t.h)|.dt$$

On majore $|f^{(n+1)}(a+t.h)|$ par M_{n+1} et on calcule :

$$\int_0^1 \frac{(1-t)^n}{n!}.|h|^{n+1}.M_{n+1}.dt$$

vaut $\frac{|h^{n+1}|}{n!}.M_{n+1}.\frac{1}{n+1}$. On aboutit à la majoration demandée.

Contrairement à des égalités de Taylor-Lagrange, cette inégalité est valable aussi pour les fonctions à valeurs complexes.

3.7.3 Intégrales de Wallis (hors programme, mais classique).

Pour tout n, on pose

$$W_n = \int_0^{\pi/2} \sin^n(t).dt = \int_0^{\pi/23} \cos^n(\theta).d\theta$$

Ces intégrales forment une suite décroissante de limite nulle. On a

$$W_{n+2} = \frac{n+1}{n+2}.W_n$$

On peut obtenir une formule pour $W_{2.n}$ et $W_{2.n+1}$ (voir ci-dessous). Pour tout n, on a

$$(n+1).W_n.W_{n+1} = \frac{\pi}{2}$$

On trouve enfin

$$W_n \sim_{n\to+\infty} \sqrt{\frac{\pi}{2.n}}$$

Les deux intégrales en sinus et cosinus sont égales visuellement, ou par $t = \frac{\pi}{2} - \theta$.

On prouve la décroissance de la suite (W_n) en écrivant

$$W_n - W_{n+1} = \int_0^{\pi/2} \sin^n(t).(1-\sin(t)).dt$$

La suite W est décroissante, minorée par 0, elle converge (sa limite va être donnée plus loin).

On intègre W_{n+2} par parties $\begin{array}{|c|c|c|}\hline \sin(t) & \hookleftarrow & -\cos(t) \\ \hline \sin^{n+1}(t) & \hookrightarrow & (n+1).\sin^n(t).\cos(t) \\ \hline \end{array}$:

$$W_{n+2} = \Big[-\sin^{n+1}(t).\cos(t) \Big]_0^{\pi/2} + (n+1).\int_0^{\pi/2} \sin^n(t).\cos^2(t).dt$$

Le terme rectangle est nul, et en remplaçant $\cos 2$(t) par $1-\sin^2(t)$, on obtient $W_{n+2} = (n+1).(W_n - W_{n+2})$ puis la relation de récurrence demandée.

En mettant en boucle cette relation, on peut obtenir :

$$W_{2.n} = \frac{1.3.5\ldots(2.n-1)}{2.4.6\ldots(2.n)}.\frac{\pi}{2} = \frac{(2.n)!}{2^{2.n+1}(n!)^2}.\pi \ et\ W_{2.n+1} = \frac{2^{2.n}(n!)^2}{(2.n+1)!}$$

Ces deux formules servent peu.

On part de $(n+2).W_{n+2} = (n+1).W_n$, on multiplie par W_{n+1} et la suite $n \longrightarrow (n+1).W_{n+1}.W_n$est constante.
Comme on a sa valeur en 0, on la connaît pour tout n.

Avec $W_{n+1}.W_n = \frac{\pi}{2.(n+1)}$ et la convergence de (W_n) vers une limite α , on a forcément $\alpha = 0$.

Par décroissance, on écrit $W_{n+1} \leqslant W_n \leqslant W_{n-1}$ puis $W_n.W_{n+1} \leqslant (W_n)^2 \leqslant W_n.W_{n-1}$ et enfin

$$\frac{n}{n+1}.(n+1).W_n.W_{n+1} \leqslant n.(W_n)^2 \leqslant n.W_n.W_{n-1}$$

La relation $(n+1).W_{n+2} = (n+2).W_n$ appliquée à deux rangs différents donne la convergence du terme du milieu vers $1/\pi$.

La formule de Stirling est ensuite une conséquence avec un travail soutenu. Elle est au programme de seconde année

$$n! \sim_{n\to+\infty} \left(\frac{n}{e}\right)^n.\sqrt{2.n.\pi}$$

3.7.4 Moyenne d'une application continue sur un segment.

Si f est continue de $[a,\ b]$ dans $\mathbb{R}$ alors $\int_a^b f(t).dt$ existe, et il existe un réel c entre a et b vérifiant

$$\int_a^b f(t).dt = (b-a).f(c)$$

4 Algèbre linéaire.

4.1 Espaces vectoriels.

4.1.1 Lemme d'agrandissement.

Lemme d'agrandissement : dans un espace vectoriel $(E,+,.)$, soit un famille libre $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$ et un vecteur $\overrightarrow{u}$. La famille $(\overrightarrow{a_1},\dots\overrightarrow{a_n},\overrightarrow{u})$ est liée si et seulement si $\overrightarrow{u}$ est combinaison linéaire de $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$.

On prend donc une famille libre $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$ *(la seule combinaison linéaire pouvant donner $\overrightarrow{0}$ est $\sum_{k=1}^{n} 0.\overrightarrow{ak}$).*

• Si le vecteur $\overrightarrow{u}$ est combinaison de $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$, alors l'un des vecteurs de $(\overrightarrow{a_1},\dots\overrightarrow{a_n},\overrightarrow{u})$ est combinaison des autres et la famille est liée.

• *L'autre sens est plus intéressant.*

On suppose la famille $(\overrightarrow{a_1},\dots\overrightarrow{a_n},\overrightarrow{u})$ liée par une relation du type $\alpha_1.\overrightarrow{a_1}\dots\alpha_n.\overrightarrow{a_n}+\alpha_0.\overrightarrow{u}=\overrightarrow{0}$ avec au moins un des α_i non nul. Il est impossible que α_0 soit nul, sinon on a une relation du type $\alpha_1.\overrightarrow{a_1}\dots\alpha_n.\overrightarrow{a_n}=\overrightarrow{0}$ avec au moins un des α_i non nul, ce qui contredit "famille libre".

On divise alors : $\overrightarrow{u}=\sum_{k=1}^{n}\frac{-\alpha_k}{\alpha_0}.\overrightarrow{a_k}$, et $\overrightarrow{u}$ est combinaison de la famille $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$.

4.1.2 Théorème fondamental de la dimension finie.

Dans un espace vectoriel engendré par n vecteurs, toute famille de $n+1$ vecteurs est liée.
Corolaire : les bases d'un espace vectoriel[a] ont toutes le même cardinal, appelé dimension de cet espace vectoriel.

a. engendré par une famille finie, sinon tous les cardinaux considérés sont infinis

On se place dans un espace vectoriel $(E,+,.)$ muni d'une famille génératrice $(\overrightarrow{a_1},\dots\overrightarrow{a_n})$ *(tout vecteur $\overrightarrow{u}$ est combinaison linéaire des $\overrightarrow{a_k}$).* On prend une famille $(\overrightarrow{v_0},\dots\overrightarrow{v_n})$. L'objectif est de montrer qu'elle est liée.

On démontre le résultat par récurrence sur n.

On initialise à $n=0$.

On prend un espace vectoriel engendré par 0 vecteur. Ce ne peut être que $(\{\overrightarrow{0}\},+,.)$. La seule famille de un vecteur envisagée est $(\overrightarrow{0})$ et elle est liée par $1.\overrightarrow{0}=\overrightarrow{0}$.

On poursuit par principe à $n = 1$.
On prend, dans un espace vectoriel engendré par un vecteur $\overrightarrow{a_1}$ une famille de deux vecteurs $(\overrightarrow{v_0}, \overrightarrow{v_1})$.
Les deux vecteurs sont colinéaires, la famille est liée.

On suppose maintenant pour un n donné que toute famille de $n+1$ vecteurs dans un espace vectoriel engendré par n vecteurs est liée *(hypothèse notée H_n)*.
On se place alors dans un espace vectoriel $(E, +, .)$ engendré par $(\overrightarrow{a_1}, \dots \overrightarrow{a_{n+1}})$ et on y prend $n+2$ vecteurs $(\overrightarrow{v_0}, \dots \overrightarrow{v_{n+1}})$. Il faut prouver en utilisant H_n que cette famille est liée.
On décompose suivant la famille génératrice *(sans garantie d'unicité, mais ça ne sert à rien)* :

$$\left\{\begin{array}{ccccccc|} \overrightarrow{v_0} & = & \alpha_0^1.\overrightarrow{a_1} & +\dots & +\alpha_0^n.\overrightarrow{a_n} & +\alpha_0^{n+1}.\overrightarrow{a_{n+1}} & \\ \overrightarrow{v_1} & = & \alpha_1^1.\overrightarrow{a_1} & +\dots & +\alpha_1^n.\overrightarrow{a_n} & +\alpha_1^{n+1}.\overrightarrow{a_{n+1}} & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \overrightarrow{v_n} & = & \alpha_n^1.\overrightarrow{a_1} & +\dots & +\alpha_n^n.\overrightarrow{a_n} & +\alpha_n^{n+1}.\overrightarrow{a_{n+1}} & \\ \overrightarrow{v_{n+1}} & = & \alpha_{n+1}^1.\overrightarrow{a_1} & +\dots & +\alpha_{n+1}^n.\overrightarrow{a_n} & +\alpha_{n+1}^{n+1}.\overrightarrow{a_{n+1}} & \end{array}\right.$$

On étudie deux cas :
• premier cas : tous les α_i^{n+1} sont nuls. Alors, la famille des $\overrightarrow{v_i}$ est dans l'espace vectoriel engendré par $(\overrightarrow{a_1}, \dots \overrightarrow{a_n})$, et comme elle est formée de $n+2$ vecteurs *(soit plus que $n+1$)*, elle est liée par l'hypothèse H_n.
• second cas : l'un au moins des α_i^{n+1} est non nul. Quitte à ré-indexer la famille, on peut supposer que c'est α_{n+1}^{n+1} *(l'ordre des vecteurs n'intervient pas dans le caractère "libre ou lié" d'une famille)*. On définit alors les vecteurs suivants : $\overrightarrow{w_0} = \overrightarrow{v_0} - \dfrac{\alpha_0^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}$, $\overrightarrow{w_1} = \overrightarrow{v_1} - \dfrac{\alpha_1^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}$ jusqu'à $\overrightarrow{w_n} = \overrightarrow{v_n} - \dfrac{\alpha_n^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}$ *(les plus observateurs identifieront la méthode du pivot de Gauss)*.
Par construction, ces $n+1$ vecteurs s'expriment à l'aide de $\overrightarrow{a_1}$ jusqu'à $\overrightarrow{a_n}$ *(on a tout fait pour effacer la "composante" suivant $\overrightarrow{a_{n+1}}$)*.

Par hypothèse de rang n, cette famille des $\overrightarrow{w_i}$ est liée par une relation du type $\sum_{i=0}^{n} \mu_i.\overrightarrow{w_i} = \overrightarrow{0}$ avec au moins un des μ_i non nul.
On remplace alors $\sum_{i=0}^{n} \mu_i.\left(\overrightarrow{v_i} - \dfrac{\alpha_i^{n+1}}{\alpha_{n+1}^{n+1}}.\overrightarrow{v_{n+1}}\right) = \overrightarrow{0}$ que l'on peut écrire $\sum_{i=0}^{n+1} \mu_i.\overrightarrow{v_i} = \overrightarrow{0}$ *(avec $\mu_{n+1} = -\sum_{i=0}^{n} \mu_i.\dfrac{\alpha_i^{n+1}}{\alpha_{n+1}^{n+1}}$ si l'on y tient vraiment, mais c'est sans importance)*, avec l'un au moins de μ_i non nul *(pour un i de 0 à n déjà)*.
On reconnaît que la famille $(\overrightarrow{v_0}, \dots \overrightarrow{v_{n+1}})$ est liée, et la récurrence s'achève.

On passe au corolaire. On se place dans un espace vectoriel $(E, +, .)$ engendré par une famille finie $(\overrightarrow{a_1}, \dots \overrightarrow{a_n})$.

> C'est ce qu'on appelle un espace vectoriel de dimension finie, même si cette définition vient avant la notion même de dimension.

On sait déjà que les familles libres ne peuvent pas avoir plus de n vecteurs.
Les bases étant libres, leur cardinal sera inférieur ou égal à n.
On prend alors deux bases $(\overrightarrow{e_1}, \dots \overrightarrow{e_p})$ et $(\overrightarrow{\varepsilon_1}, \dots \overrightarrow{\varepsilon_q})$ *(objectif : $p = q$)*.
Comme $(\overrightarrow{e_1}, \dots \overrightarrow{e_p})$ est génératrice de $(E, +, .)$, la famille libre $(\overrightarrow{\varepsilon_1}, \dots \overrightarrow{\varepsilon_q})$ ne peut pas avoir un cardinal strictement supérieur à p *(théorème précédent)*. On a donc $q \leqslant p$.
Comme $(\overrightarrow{\varepsilon_1}, \dots \overrightarrow{\varepsilon_q})$ est génératrice, la famille libre $(\overrightarrow{e_1}, \dots \overrightarrow{e_p})$ ne peut pas avoir un cardinal strictement supérieur à q. On a donc $p \leqslant q$.
Par antisymétrie de l'ordre sur les entiers naturels : $p = q$.

4.1.3 Formule de Grassmann, dimension d'une somme de sous-espaces.

Formule de Grassmann : si A et B sont deux sous-espaces vectoriels de dimension finie d'un espace vectoriel $(E,+,.)$, alors on a

$$\dim(A+B)=\dim(A)+\dim(B)-\dim(A\cap B)$$

Cette formule rappelle la formule $Card(A\cup B)=Card(A)+Card(B)-Card(A\cap B)$ pour deux ensembles. Mais la démonstration est différente.

Preuve par les cardinaux des bases.

On rappelle que $A\cap B$ est un sous-espace vectoriel de $(E,+,.)$ *(en tant que sous-espace vectoriel de A déjà de dimension finie)*.

On construit une base de $A\cap B$ *(par principe de la base incomplète)* : $(\overrightarrow{e_1},\dots\overrightarrow{e_n})$ *(famille libre et génératrice de $A\cap B$)*.

Comme cette famille est libre dans $A\cap B$, elle l'est aussi dans A.

On la complète en base de A : $(\overrightarrow{e_1},\dots\overrightarrow{e_n},\overrightarrow{a_{n+1}}\dots\overrightarrow{a_p})$.

De même, en tant que famille libre de B, on la complète en base de B : $(\overrightarrow{e_1},\dots\overrightarrow{e_n},\overrightarrow{b_{n+1}}\dots\overrightarrow{b_q})$.

On montre maintenant que $(\overrightarrow{e_1},\dots\overrightarrow{e_n},\ \overrightarrow{a_{n+1}}\dots\overrightarrow{a_p},\ \overrightarrow{b_{n+1}}\dots\overrightarrow{b_q})$ est une base de $A+B$.

• On commence par l'appartenance à $A+B$: tous ces vecteurs sont dans A ou dans B donc dans $A+B$.

• On poursuit avec "**génératrice**". On prend un vecteur $\overrightarrow{u}$ de $A+B$. Par définition, il est de la forme $\overrightarrow{u}=\overrightarrow{a}+\overrightarrow{b}$ avec $\overrightarrow{a}$ dans A et $\overrightarrow{b}$ dans B. Par définition des deux bases, $\overrightarrow{a}$ s'écrit $\sum_{i=1}^{n}\alpha_i.\overrightarrow{e_i}+\sum_{j=n+1}^{p}\alpha_j.\overrightarrow{a_j}$.

De même, $\overrightarrow{b}$ s'écrit $\sum_{i=1}^{n}\beta_i.\overrightarrow{e_i}+\sum_{k=n+1}^{q}\beta_k.\overrightarrow{b_k}$. On somme :

$$\overrightarrow{u}=\sum_{i=1}^{n}(\alpha_i+\beta_i).\overrightarrow{e_i}+\sum_{j=n+1}^{p}\alpha_j.\overrightarrow{a_j}+\sum_{k=n+1}^{q}\beta_k.\overrightarrow{b_k}$$

Il est bien combinaison de $(\overrightarrow{e_1},\dots\overrightarrow{e_n},\ \overrightarrow{a_{n+1}}\dots\overrightarrow{a_p},\ \overrightarrow{b_{n+1}}\dots\overrightarrow{b_q})$.

• On termine avec "**libre**". On suppose qu'une combinaison $\sum_{i=1}^{n}\lambda_i.\overrightarrow{e_i}+\sum_{j=n+1}^{p}\alpha_j.\overrightarrow{a_j}+\sum_{k=n+1}^{q}\beta_k.\overrightarrow{b_k}$ est nulle. On bascule $\sum_{i=1}^{n}\lambda_i.\overrightarrow{e_i}+\sum_{j=n+1}^{p}\alpha_j.\overrightarrow{a_j}=-\sum_{k=n+1}^{q}\beta_k.\overrightarrow{b_k}$. Ce vecteur, qu'on va noter $\overrightarrow{c}$ est à la fois dans A *(forme de gauche)* et dans B *(forme de droite)*. Il est donc dans $A\cap B$, et s'écrit comme combinaison de $(\overrightarrow{e_1},\dots\overrightarrow{e_n})$.

On a donc à ce stade $\overrightarrow{c}=\sum_{i=1}^{n}\lambda_i.\overrightarrow{e_i}+\sum_{j=n+1}^{p}\alpha_j.\overrightarrow{a_j}=-\sum_{k=n+1}^{q}\beta_k.\overrightarrow{b_k}=\sum_{i=1}^{n}\gamma_i.\overrightarrow{e_i}$. En reprenant la dernière égalité, on a $\sum_{k=n+1}^{q}\beta_k.\overrightarrow{b_k}+\sum_{i=1}^{n}\gamma_i.\overrightarrow{e_i}=\overrightarrow{0}$. Comme $(\overrightarrow{e_1},\dots\overrightarrow{e_n},\overrightarrow{b_{n+1}}\dots\overrightarrow{b_q})$ est une base de B, elle est libre et on a $\beta_k=0$ pour tout k et $\gamma_i=0$ pour tout i. On reporte : $\overrightarrow{c}$ est nul. On re-reporte : $\overrightarrow{0}=\sum_{i=1}^{n}\lambda_i.\overrightarrow{e_i}+\sum_{j=n+1}^{p}\alpha_j.\overrightarrow{a_j}$.

Comme $(\overrightarrow{e_1},\dots\overrightarrow{e_n},\overrightarrow{a_{n+1}}\dots\overrightarrow{a_p})$ est libre (dans A), on trouve cette fois que les λ_i et la α_j sont nuls. Finalement, tous les coefficients sont nuls.

Maintenant que $(\overrightarrow{e_1},\dots\overrightarrow{e_n},\overrightarrow{a_{n+1}}\dots\overrightarrow{a_p},\overrightarrow{b_{n+1}}\dots\overrightarrow{b_q})$ est une base de $A+B$, on compte le nombre d'éléments : $p+(q-n)$.

On a donc $\dim(A+B) = \dim(A) + (\dim(B) - \dim(A \cap B))$ comme attendu.

Preuve en utilisant la formule du rang.
On définit l'application $(\overrightarrow{a},\ \overrightarrow{b}) \to \overrightarrow{a} + \overrightarrow{b}$ de $A \times B$ dans E *(notée φ)*.
Par définition même, son ensemble image est $A+B$.
Son noyau est formé des couples $(\overrightarrow{a},\ \overrightarrow{b})$ de $A \times B$ vérifiant $\overrightarrow{a} + \overrightarrow{b} = \overrightarrow{0}$. On a alors $\overrightarrow{a} = -\overrightarrow{b}$. Ce vecteur est à la fois dans A et dans B. Le noyau est donc formé des couples $(\overrightarrow{c},\ -\overrightarrow{c})$ avec $\overrightarrow{c}$ dans $A \cap B$.
Ce noyau est isomorphe à $A \cap B$. Il a donc la même dimension.
La formule $\dim(A \times B) = \dim(Ker(\varphi)) + \dim(Im(\varphi))$ donne $\dim(A) + \dim(B) = \dim(A \cap B) + \dim(A+B)$.

4.2 Applications linéaires.

4.2.1 Image d'une famille liée.

L'image d'une famille liée est liée.

On suppose $(\overrightarrow{a_1}, \dots \overrightarrow{a_k})$ liée par une relation du type $\overrightarrow{a_i} = \sum_{j \neq i} \alpha_j . \overrightarrow{a_j}$.

Par linéarité de f, on a alors $f(\overrightarrow{a_i}) = \sum_{j \neq i} \alpha_j . f(\overrightarrow{a_j})$ et on reconnaît que la famille image est liée.

> Il se peut que la famille image soit liée sans que la famille initiale ne le soit. Il suffit de prendre pour f l'application nulle, ou que l'un des vecteurs de la famille soit dans le noyau de f (ou même une combinaison des vecteurs).

4.2.2 Image d'une famille libre.

L'image d'une famille libre par une application linéaire injective est libre.

On prend $(\overrightarrow{u_1}, \dots \overrightarrow{u_n})$ libre dans l'espace vectoriel $(E, +, .)$ et f injective.

On considère $(f(\overrightarrow{u_1}), \dots f(\overrightarrow{u_n}))$ dans l'espace vectoriel d'arrivée. On suppose $\sum_{k=1}^{n} \alpha_k . f(\overrightarrow{u_k}) = \overrightarrow{0_F}$ *(objectif : les α_k sont tous nuls)*.

Par linéarité de f , on obtient $f\Big(\sum_{k=1}^{n} \alpha_k . \overrightarrow{u_k}\Big) = \overrightarrow{0_F} = f(\overrightarrow{0_E})$.

Par injectivité de f, il vient $\sum_{k=1}^{n} \alpha_k . \overrightarrow{u_k} = \overrightarrow{0_E}$ puis par liberté de la famille $(\overrightarrow{u_1}, \dots \overrightarrow{u_n})$: $\forall k,\ \alpha_k = 0$.

Une application linéaire non injective peut transformer une famille libre en famille liée, il suffit de prendre un vecteur non nul du noyau, ou plus généralement une famille de vecteur qui réussit à engendrer un vecteur du noyau.

4.3 Noyau d'une application linéaire.

Noyau : le noyau d'une application linéaire f de $(E, +, .)$ dans $(F, +, .)$ est un sous-espace vectoriel de $(E, +, .)$.

• Le noyau est une partie de E, par définition même : $Ker(f) = \{\overrightarrow{u} \in E \mid f(\overrightarrow{u}) = \overrightarrow{0_F}\}$.
• Le vecteur nul de $(E, +, .)$ est dans le noyau : $f(\overrightarrow{0_E}) = f(0 \times \overrightarrow{0_E}) = 0 \times f(\overrightarrow{0_E}) = \overrightarrow{0_F}$.
• Le noyau est stable par combinaisons linaires :
on prend $\overrightarrow{u}$ et $\overrightarrow{v}$ dans le noyau, ainsi que deux scalaires α et β.

On calcule $f(\alpha.\overrightarrow{u}+\beta.\overrightarrow{v})=\alpha.f(\overrightarrow{u})+\beta.f(\overrightarrow{v})=\alpha.\overrightarrow{0_F}+\beta.\overrightarrow{0_F}=\overrightarrow{0_F}$.
On reconnaît que $\alpha.\overrightarrow{u}+\beta.\overrightarrow{v}$ est dans le noyau de f.

Ce résultat permet de démontrer rapidement qu'une partie de $(E,+,.)$ est un espace vectoriel, en montrant que c'est le noyau d'une application linaire bien choisie.

4.3.1 Noyau et injectivité.

Noyau et injectivité : une application linéaire f de $(E,+,.)$ dans $(F,+,.)$ est injective si et seulement si son noyau est réduit à $\overrightarrow{0_E}$.

Pour le premier sens, on prend f linéaire et injective de $(E,+,.)$ dans $(F,+,.)$.
On rappelle la définition : $Ker(f)=\{\overrightarrow{u}\in E \mid f(\overrightarrow{u})=\overrightarrow{0_F}\}$.
Déjà, $\overrightarrow{0_E}$ est dans le noyau, puisque $f(\overrightarrow{0_E})=f(0\times\overrightarrow{0_E})=0\times f(\overrightarrow{0_E})=\overrightarrow{0_F}$ par linéarité.
Tout autre élément $\overrightarrow{u}$ de $Ker(f)$ vérifie $f(\overrightarrow{u})=\overrightarrow{0_F}=f(\overrightarrow{0_E})$. Par injectivité, $\overrightarrow{u}$ est forcément égal à $\overrightarrow{0_E}$.

Pour le second sens, on suppose le noyau réduit au seul vecteur nul, et on montre l'injectivité de f.
On prend deux vecteurs $\overrightarrow{a}$ et $\overrightarrow{b}$ ayant la même image *(objectif : ils sont égaux)*. On écrit $f(\overrightarrow{a})=f(\overrightarrow{b})$, puis $f(\overrightarrow{a})-f(\overrightarrow{b})=\overrightarrow{0_F}$, et même $f(\overrightarrow{a}-\overrightarrow{b})=\overrightarrow{0_F}$ par linéarité. $\overrightarrow{a}-\overrightarrow{b}$ est dans le noyau, il est donc nul. On est bien arrivé à $\overrightarrow{a}=\overrightarrow{b}$.

On note que l'existence d'un noyau non trivial transmet le défaut d'injectivité partout.
Pour f linéaire de $(E,+,.)$ dans $(F,+,.)$, l'équation $f(\overrightarrow{u})=\overrightarrow{v}$ d'inconnue $\overrightarrow{u}$ et de paramètre $\overrightarrow{v}$ se résout ainsi :

$\overrightarrow{v}\in Im(f)$	$\exists\overrightarrow{u_0}\in E,\ f(\overrightarrow{u_0})=\overrightarrow{v}$	$S=\{\overrightarrow{u_0}+\overrightarrow{k}\mid\overrightarrow{k}\in Ker(f)\}=\overrightarrow{u_0}+Ker(f)$
		solution particulière plus solutions homogènes
$\overrightarrow{v}\notin Im(f)$	$\forall\overrightarrow{u}\in E,\ f(\overrightarrow{u})\neq\overrightarrow{v}$	$S=\emptyset$

De plus, si B est un sous-espace vectoriel de $(F,+,.)$ alors on a $Ker(f)\subset f^{-1}(B)$.
Enfin, si A est un sous-espace vectoriel de $(E,+,.)$ alors on a $f^{-1}(f(A))=A+Ker(f)$.

4.3.2 Noyaux emboités.

f est une applications linéaire de $(E,+,.)$ dans $(F,+,.)$, g est linéaire de $(F,+,.)$ dans $(G,+,.)$. On a alors

$$Ker(f)\subset Ker(g\circ f)$$

Si u est un endomorphisme de $(E,+,.)$ alors on a

$$\{\overrightarrow{0}\}=Ker(u^0)\subset Ker(u)\subset Ker(u^2)\subset\ldots\subset Ker(u^p)\subset Ker(u^{p+1})\subset\ldots$$

Par linéarité de g , si on a $f(\overrightarrow{a})=\overrightarrow{0_F}$ alors on a

$$g\circ f(\overrightarrow{a})=g(f(\overrightarrow{a}))=g(\overrightarrow{0_F})=\overrightarrow{0_G}$$

4.3.3 Noyau , image et composition.

f est une applications linéaire de $(E,+,.)$ dans $(F,+,.)$, g est linéaire de $(F,+,.)$ dans $(G,+,.)$. On a alors

$$g \circ f = 0_{L(E,G)} \Leftrightarrow (Im(f) \subset Ker(g))$$

4.4 Ensemble image d'une application linéaire.

4.5 Théorème et formule du rang.

Théorème du rang :
• version isomorphisme : toute application linéaire entre deux espaces vectoriels induit un isomorphisme entre un supplémentaire du noyau et l'ensemble image.
• version base : si f est une application linéaire de $(E,+,.)$ dans $(F,+,.)$, avec $(\overrightarrow{e_1},\dots\overrightarrow{e_k})$ une base de $Ker(f)$ qu'on complète en base de $(E,+,.)$: $(\overrightarrow{e_1},\dots\overrightarrow{e_k},\ \overrightarrow{e_{k+1}},\dots\overrightarrow{e_n})$, alors $(f(\overrightarrow{e_{k+1}}),\dots\overrightarrow{f(e_n)})$ est une base de $Im(f)$.
• version dimensions : si f est une application linéaire de $(E,+,.)$ dans $(F,+,.)$, alors

$$\dim(Im(f)) = \dim(E) - \dim(Ker(f))$$

On prend donc f linéaire de $(E,+,.)$ dans $(F,+,.)$, espaces vectoriels sur un même corps $(\mathbb{K},+,.)$ *(on ne supposera E de dimension finie que pour les versions "base" et "dimension", et la dimension de $(F,+,.)$ n'a aucune importance)*.

Version "isomorphisme".
On note S un supplémentaire de $Ker(f)$ dans E, on a donc $E = Ker(f) \oplus S$ *(tout vecteur de E se décompose d'une façon unique comme somme d'un vecteur de $Ker(f)$ et d'un vecteur de S)*.

On sait déjà que f reste linéaire sur le sous-espace vectoriel S.

On notera $\overline{f}$ l'application f quand on la considèrera de S dans F *(cas particulier)*.
L'image de tout vecteur de S est dans $Im(f)$, comme image d'un vecteur de E (c'est $Im(\overline{f}) \subset Im(f)$, et on verra $Im(\overline{f}) = Im(f)$).
$\overline{f}$ est alors injective de S dans $Im(f)$. On passe pour cela par le noyau de $\overline{f}$. On prend un vecteur $\overrightarrow{s}$ de S d'image nulle par $\overline{f}$. Il vérifie $\overline{f}(\overrightarrow{s}) = \overrightarrow{0}$. Le vecteur $\overrightarrow{s}$, vu comme vecteur de E est donc dans $Ker(f)$. Étant à la fois dans $Ker(f)$ et S, il est nul *(somme directe)*.
Enfin, $\overline{f}$ est surjective de S sur $Im(f)$. On prend un vecteur $\overrightarrow{v}$ dans $Im(f)$. Par définition, il a au moins un antécédent $\overrightarrow{u}$ dans E. Par définition de la somme *(directe)*, $\overrightarrow{u}$ s'écrit $\overrightarrow{k} + \overrightarrow{s}$ avec $\overrightarrow{k}$ dans $Ker(f)$ et $\overrightarrow{s}$ dans S. On a alors $\overrightarrow{v} = f(\overrightarrow{u}) = f(\overrightarrow{k} + \overrightarrow{s}) = f(\overrightarrow{k}) + f(\overrightarrow{s}) = \overline{f}(\overrightarrow{s})$. Le vecteur $\overrightarrow{v}$ de $Im(f)$ a donc un antécédent $\overrightarrow{s}$ dans S *(unique comme vu plus haut)*.

Version "bases".
On suppose $(E,+,.)$ de dimension finie n. Comme $Ker(f)$ est un sous-espace vectoriel de $(E,+,.)$, il est aussi de dimension finie, et par théorème de la base incomplète *(en partant de la famille vide)*, on peut le doter d'une base *(éventuellement vide si f est injective)* : $(\overrightarrow{e_1},\dots\overrightarrow{e_k})$ avec $k = \dim(Ker(f)) \leqslant n$.
Encore par théorème de la base incomplète, on agrandit en base de E : $(\overrightarrow{e_1},\dots\overrightarrow{e_k},\overrightarrow{e_{k+1}},\dots\overrightarrow{e_n})$.

On sait déjà que la famille image de cette base $(f(\overrightarrow{e_1}),\dots f(\overrightarrow{e_k}),f(\overrightarrow{e_{k+1}}),\dots f(\overrightarrow{e_n}))$ est génératrice de $Im(f)$. Comme $f(\overrightarrow{e_1})$ à $f(\overrightarrow{e_k})$ sont nuls, on a déjà $(f(\overrightarrow{e_{k+1}}),\dots f(\overrightarrow{e_n}))$ qui engendre $Im(f)$.

On montre à présent que cette famille est libre. On part d'une combinaison $\alpha_{k+1}.f(\overrightarrow{e_{k+1}}),\dots+\alpha_n.f(\overrightarrow{e_n})$ qu'on suppose nulle *(objectif : les α_i sont nuls)*. Par linéarité, on a donc $f(\alpha_{k+1}.\overrightarrow{e_{k+1}},\dots+\alpha_n.\overrightarrow{e_n})=\overrightarrow{0_F}$. On reconnaît que $\alpha_{k+1}.\overrightarrow{e_{k+1}},\dots+\alpha_n.\overrightarrow{e_n}$ est dans $Ker(f)$ et s'écrit donc $\beta_1.\overrightarrow{e_1}+\dots+\beta_k.\overrightarrow{e_k}$. On écrit alors

$$\beta_1.\overrightarrow{e_1}+\dots+\beta_k.\overrightarrow{e_k}-\alpha_{k+1}.\overrightarrow{e_{k+1}}-\dots-\alpha_n.\overrightarrow{e_n}=\overrightarrow{0_E}$$

Par liberté de la base : les α_i et les β_j sont nuls.

Version "dimensions".
Avec la démonstration précédente, il suffit de compter les cardinaux des bases :

base de $Ker(f)$	base de E	base de $Im(f)$
$(\overrightarrow{e_1},\dots\overrightarrow{e_k})$	$(\overrightarrow{e_1},\dots\overrightarrow{e_k},\overrightarrow{e_{k+1}},\dots\overrightarrow{e_n})$	$(f(\overrightarrow{e_{k+1}}),\dots f(\overrightarrow{e_n}))$
k	n	$n-k$

On a bien $\dim(Im(f))=\dim(E)-\dim(Ker(f))$.

> On préfèrera cette formulation à $\dim(Im(f))+\dim(Ker(f))=\dim(E)$, afin d'éloigner $Ker(f)$ et $Im(f)$ l'un de l'autre car ce ne sont pas des sous-espaces vectoriels d'un même espace vectoriel.

4.6 Déterminants.

4.6.1 Existence et unicité du déterminant.

4.6.2 Déterminant de VanDerMonde.

Déterminant de VanDerMonde : si les a_k (pour k de 0 à $n-1$) sont n complexes, alors le déterminant de la matrice $V[a_0,\dots a_n]$ de terme général $(a_i)^k$ (i et k de 0 à $n-1$) est égal à $\prod_{i<j}(a_j-a_i)$ (formé de $\frac{n.(n-1)}{2}$ termes).

On démontre ce résultat par récurrence sur n.
• Pour n égal à 0, la formule est cohérente par pure logique *(déterminant de matrice vide, produit vide)*.
• Pour n égal à 1, le déterminant est celui de $\left|\ (a_0)^0\ \right|$, il vaut 1, et le produit est encore vide.
• Pour n égal à 2, le déterminant se calcule : $\begin{vmatrix}1 & a_0\\ 1 & a_1\end{vmatrix}=(a_1-a_0)$, c'est bien le produit à un terme attendu.
• On peut aussi vérifier pour n égal à 3 :

$$\begin{vmatrix}1 & a_0 & (a_0)^2\\ 1 & a_1 & (a_1)^2\\ 1 & a_2 & (a_2)^2\end{vmatrix}=(a_1-a_0).(a_2-a_0).(a_2-a_1)$$

On suppose à présent le résultat vrai au rang n, et on prend la matrice de taille $n+1$:

$$V[a_0,\dots a_{n-1},x]=\begin{pmatrix}1 & a_0 & \dots & (a_0)^{n-1} & (a_0)^n\\ 1 & a_1 & \dots & (a_1)^{n-1} & (a_1)^n\\ \vdots & \vdots & & \vdots & \vdots\\ 1 & a_{n-1} & \dots & (a_{n-1})^{n-1} & (a_{n-1})^n\\ 1 & x & \dots & x^{n-1} & x^n\end{pmatrix}$$

Si deux des a_j sont égaux, le déterminant est nul, et bien égal à $\prod_{i<j\leqslant n}(a_j - a_i)$. On passe donc au cas où tous les a_j sont distincts.
On développe $\det(V[a_0, \dots a_{n-1}, x])$ par rapport à la dernière ligne. On a un polynôme en x, dont le terme dominant est $x^n.det(V[a_0, \dots a_{n-1}])$.
Ce polynôme est nul si x est égal à l'un des a_k, car il y a alors deux lignes égales.
Il se factorise donc par $\prod_{k=0}^{n-1}(x - a_k)$. Comme ce terme est d'ores et déjà de degré n, et comme on connaît le coefficient dominant, ce polynôme est

$$det(V[a_0, \dots a_{n-1}]).\prod_{k=0}^{n-1}(x - a_k)$$

On décide d'appeler x plus simplement a_n et on a bien

$$det(V[a_0, \dots a_n]) = det(V[a_0, \dots a_{n-1}]).\prod_{k=0}^{n-1}(a_n - a_k) = \prod_{i<j<n}(a_j - a_i).\prod_{k=0}^{n-1}(a_n - a_k) = \prod_{i<j\leqslant n}(a_j - a_i)$$

5 Algèbre bilinéaire.

6 Probabilités.

6.0.1 Variables aléatoires indépendantes.

6.0.2 Inégalité de Markov.

Inégalité de Markov : pour toute variable aléatoire A positive et tout réel a strictement positif :

$$P(A \geqslant a) \leqslant \frac{E(A)}{a}$$

On prend une variable aléatoire positive A et un réel a strictement positif.
On écrit la définition : $E(A) = \sum_x x.P(A = x)$.
On coupe en deux

$$E(A) = \sum_{x<a} x.P(A = x) + \sum_{a\leqslant x} x.P(A = x)$$

La première somme est positive, car la variable aléatoire est positive : $E(A) \geqslant \sum_{a\leqslant x} x.P(A = x)$
Dans la seconde, on minore : $a \leqslant x$ donc $a.P(A = x) \leqslant x.P(A = x)$.
On a donc à ce stade

$$E(A) \geqslant \sum_{a\leqslant x} a.P(A = x) = a.\sum_{a\leqslant x} P(A = x)$$

Or, la somme $\sum_{a\leqslant x} P(A = x)$ est précisément $P(A \geqslant a)$.
Il ne reste plus qu'à diviser par a strictement positif.

Pour a trop proche de 0, cette inégalité est sans intérêt, elle n'a son utilité que pour a plus grand que $E(X)$. Sinon, il est assez logique de dire que si la moyenne des notes positives est 10, il ne peut pas y avoir plus de cinquante pour cent des notes au delà de 20.

6.0.3 Inégalité de Bienaimé-Tchebychev.

Inégalité de Bienaimé-Tchebychev : pour toute variable aléatoire X et tout réel strictement positif ε, on a

$$P(|X - E(X)| \geqslant \varepsilon) \leqslant Var(X)/\varepsilon^2$$

On prend une variable aléatoire X, d'espérance $E(X)$ et de variance $Var(X)$.
La variable aléatoire $(X - E(X))^2$ est positive. Elle a pour espérance $Var(X)$.
On lui applique l'inégalité de Markov avec $A = (X - E(X))^2$ et $a = \varepsilon^2$:

$$P((X - E(X))^2 \geqslant \varepsilon^2) \leqslant \frac{E((X - E(X))^2)}{\varepsilon^2}$$

C'est exactement $P(|X - E(X)| \geqslant \varepsilon) \leqslant \frac{Var(X)}{\varepsilon^2}$.

7 Algorithmique.

7.1 Traitement de données.

7.1.1 Recherche du maximum/minimum d'un tableau non vide.

```
def maxi(L) : #list -> float
....m = L[0] #initialisation avec un élément
....for elt in L : #parcours de la liste
........if elt > m : #si le nouvel élément dépasse le record
............m = elt #on actualise le record
....return m
```

Si on veut le maximum et son index dans la liste :

```
def maxi(L) : #list of float -> float, int
....m, index = L[0], 0
....for k in range(len(L)) :
........if L[k] > m :
............m = L[k]
............index = k
....return m, index
```

7.1.2 Recherche de la présence d'un élément dans un tableau.

```
def presence(L, a) : #list, float -> boolean
....for elt in L :
........if elt == a :
............return True
....return False
```

7.1.3 Recherche du nombre d'occurences d'un élément dans un tableau.

```
def occurence(L, a) : #list, float -> int
....for elt in L :
........c = 0
........if elt == a :
............c += 1
....return c
```

7.1.4 Recherche de l'index d'un élément dans un tableau déjà trié.

```
def dichot(L, x) : #list, float -> int
....debut, fin = 0, len(L)
....while debut <= fin :
........milieu = (debut + fin)//2
........if L[milieu] == a :
............return milieu #on est tombé juste sur l'élément
........elif L[milieu] < x : #l'élément est entre milieu et fin
............debut = milieu + 1
........else : #l'élément est entre début et milieu
............fin = milieu - 1
....return -1 # l'élément n'existe pas
```

7.1.5 Mélange d'une liste.

```
from random import randrange
def melange(L) : #list -> list
....LC = L[ : ] #copie de la liste
....LM = [ ] #la liste qui va accueillir le mélange
....while LM : #tant que la liste LM contient des éléments
........a = LM.pop(randrange(len(LC)) #on enlève un élément au hasard de LC
........LM.append(a) #on met l'élément en fin de liste de LM
....return LM
```

On peut aussi importer `shuflle` du module `random` et il n'y a plus rien à faire.

7.1.6 Tri d'un tableau par insertion.

7.2 Méthodes numériques.

7.2.1 Résolution d'une équation $f(x) = 0$ (avec f continue) par dichotomie.

```
def dich(f, a, b, epsi=0.001) : #function, float, float, float -> float
....while b-a > epsi : #epsi vaut par défaut 0.001 si acune valeur n'est transmise
........c = (a+b)/2
........if f(c)*f(a) < 0 :
............b = c
........else :
............a = c
....return (a+b)/2
```

Ce programme n'est pas optimisé car à chaque boucle il fait deux appel à la fonction f.
Il faudrait commencer par un teste $f(b) * f(a) < 0$, afin que justement $f(b) * f(a) < 0$ soit un invariant

de boucle.

7.2.2 Calcul approché d'une intégrale par sommes de Riemann.

```
def riemann(a, b, f, n) : #float, float, function, int -> float
....G = 0
....pas = (b-a) / n
....for k in range(n) :
........G += f(a+ k*pas)
.....return pas*G
```

Cet algorithme fournit la somme de Riemann gauche.
On peut avoir besoin aussi de la somme de Riemann droite et de la somme de Riemann milieu.

```
def riemann(a, b, f, n) : #float, float, function, int -> float, float, float
....G = 0
....pas = (b-a) / n
....for k in range(n) :
........G += f(a+ k*pas)
........M += f(a +k*pas+pas/2)
....D = G-f(a)+f(b)
.....return pas*G, pas*D, pas*M
```

On rappelle qu'ensuite la méthode des trapèzes utilise $\frac{G+D}{2}$ (et converge « plus vite », avec une erreur en erreur en $\frac{(b-a)^3}{12.n^2}.||f"||_\infty$).

La somme de Riemann milieu converge aussi plus vite (erreur en $\frac{(b-a)^3}{24.n^2}.||f"||_\infty$).

Enfin, la méthode des paraboles (dite méthode de Simson) utilise $\frac{G+4.M+D}{6}$ et converge encore plus vite (erreur en $\frac{(b-a)^5}{2880.n^4}.||f^{(4)}||_\infty$).

7.2.3 Produit matriciel .

```
def produit(A, B) : #list of list, list of list -> list of list
....P = [[0 for k in range(len(B[0]] for i in range(len(A)]] #matrice nulle de bon format
....for i in range(len(A)) : #nombre de lignes de A
........for k in range(len(B[0]) : #nombre de colonnes de B
............S = 0 #accumulateur de somme
............for j in range(len(B)) : #la variable intermédiaire
................S += A[i][j]*B[j][k] #la formule du cours de maths
........P[i][k] = S
....return P
```