Chapitre 16

Polynômes formels et Fractions rationnelles

FIN $\triangledown$

Table des matières

1 Anneau des polynômes à une indéterminée

Dans tout le chapitre, $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$.

1.1 Construction

La construction a pour but de vous faire remarquer que les polynômes sont des objets *algébriques* avant tout, et que ce ne sont pas des fonctions !
Commencer par évoquer un polynôme, et voir qu'on a parlé de fonctions polynomiales définies sur $\mathbb{R}$, mais aussi sur $\mathbb{C}$, sur $\mathscr{M}_n(\mathbb{K})$, etc. !

Définition 1.
Un polynôme à coefficient dans $\mathbb{K}$ est une suite presque nulle d'éléments de $\mathbb{K}$, c'est-à-dire une suite nulle àpcr.

`Remarque.`
Deux polynômes sont égaux si et seulement si leurs coefficients sont tous égaux terme à terme.

Définition 2 : *Somme et produit de polynômes.*
Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes, soit λ un élément de $\mathbb{K}$. On définit

(i) La somme de P et Q par $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$.

(ii) La multiplication de P par λ par $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$.

(iii) Le produit de P et Q par $P \times Q = (c_n)_{n\in\mathbb{N}}$ où pour tout $n \in \mathbb{N}$,

$$c_n \overset{\text{def.}}{=} \sum_{\substack{(k,\ell)\in\mathbb{N}\times\mathbb{N} \\ k+\ell=n}} a_k b_\ell = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{\ell=0}^{n} a_{n-\ell} b_\ell.$$

(produit de Cauchy).

`Remarque.`
On note souvent $P * Q$ pour ne pas confondre avec le produit terme à terme (multiplication produit).

Propriété 1.

L'ensemble des polynômes à coefficients dans $\mathbb{K}$ muni de $+$ et de $\times$ est un anneau commutatif, de neutre pour $+$ la suite nulle et de neutre pour $\times$ la suite $(\delta_{0,n})_{n\in\mathbb{N}}$.

Définition 3.

On appelle indéterminée, et on note X le polynôme $(\delta_{1,n})_{n\in\mathbb{N}}$.

Propriété 2.

$X^k = (\delta_{k,n})_{n\in\mathbb{N}}$.

► ***Démonstration.***

On fait la preuve par récurrence sur k.

L'**initialisation** est claire : par convention, X^0 est le neutre pour $\times$, i.e. $(\delta_{0n})_{n\in\mathbb{N}}$.

L'**hérédité n'est pas beaucoup plus compliquée...** Écrivons $X^{k+1} = X\times X^k = (a_n)_{n\in\mathbb{N}}$.

Alors pour tout n dans $\mathbb{N}$,

$$\begin{aligned}
a_n &= \sum_{i=0}^{n} \delta_{1,i}\delta_{k,n-i} \\
&= \sum_{i=0}^{n} \delta_{1,i}\delta_{i,n-k} \text{ car } k = n-i \Leftrightarrow i = n-k \\
&= \delta_{1,n-k} \\
&= \delta_{n,k+1} \text{ car } 1 = n-k \Leftrightarrow n = k+1.
\end{aligned}$$

D'où l'hérédité et le résultat. ***QED*** ◄

Propriété 3.

1. X est appelée l'indéterminée. C'est un polynôme.
2. Pour tout polynôme P à coefficients dans $\mathbb{K}$, non nul, il existe $d \in \mathbb{N}$, $(a_0, \dots, a_d) \in \mathbb{K}^{d+1}$ tels que $a_d \neq 0$ et $P = \displaystyle\sum_{k=0}^{d} a_k X^k$; un tel entier d est unique et il est appelé *degré* du polynôme P.

`Remarque.`

ATTENTION ! Ne JAMAIS noter $X \mapsto P(X)$, ici P n'est **PAS** une fonction, c'est un pur objet algébrique.

Définition 4.
Soit P un polynôme de degré d, $P(X) = \sum_{k=0}^{d} a_k X^k$.

- **(i)** Pour tout k dans $[\![0, d]\!]$, $a_k X^k$ est appelé monôme de degré k de P.
- **(ii)** Le coefficient a_d est appelé coefficient dominant de P. $a_d X^d$ est appelé monôme dominant de P.
- **(iii)** Si $a_d = 1$, on dit que P est unitaire.

`Remarque.`
Par convention, le polynôme nul est de degré $-\infty$.

`Notation.`
L'indéterminée X étant fixée, on note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficient dans $\mathbb{K}$. On note, pour n dans $\mathbb{N}$, $\mathbb{K}_n[X]$ l'ensemble des polynômes de degrés inférieurs à n.

`Remarque.`
$\mathbb{K}_n[X]$ n'est **pas** un anneau ! En effet, il n'est pas stable par produit.

Propriété 4.
Soient P et Q deux polynômes de $\mathbb{K}[X]$. Alors

- **(i)** $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$, avec égalité si $\deg(P) \neq \deg(Q)$.
- **(ii)** $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Les considérations sur le degré sont souvent très puissantes : elles permettent de démontrer rapidement de nombreux résultats, comme par exemple le résultat suivant.

Propriété 5.
L'anneau $(\mathbb{K}[X], +, \times)$ est intègre.

Définition 5.
Soient P et Q deux polynômes, $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$. On définit la

composée de P et Q, notée $P \circ Q$, par

$$P \circ Q(X) = \sum_{k=0}^{n} a_k \left(\sum_{i=0}^{m} b_i X^i \right)^k .$$

Propriété 6.

Si Q n'est pas constant, $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

1.2 Divisibilité et division euclidienne

On a vu que dans certains anneaux, comme $\mathbb{Z}$, on pouvait faire de l'arithmétique. Ces gentils anneaux sont appelés anneaux à valuation.

Définition 6.

Soient A et B deux polynômes à coefficients dans $\mathbb{K}$. On dit que B divise A ou que B est un diviseur de A, et on écrit $B|A$ s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.

`Remarque.`

On dit aussi que A est divisible par B ou que A est un multiple de B et on écrit $A \in B\mathbb{K}[X]$.

Propriété 7.

(i) La relation de divisibilité sur les polynômes est une relation réflexive et transitive.

(ii) Pour tous A et B de $\mathbb{K}[X]$,

$$(A|B \text{ et } B|A) \iff (\exists \lambda \in \mathbb{K} \setminus \{0\},\ A = \lambda B).$$

(iii) Si A divise B et A divise C, alors pour tous U et V polynômes de $\mathbb{K}[X]$, A divise $BU + CV$.

(iv) Si A divise B et C divise D, alors AB divise CD.

Définition 7.

Si A divise B et B divise A, on dit que A et B sont **associés**.

Propriété 8.

Si A divise B et $\deg(A) = \deg(B)$, alors A et B sont associés.

► ***Démonstration.***

On écrit que $B = QA$ avec $Q \in \mathbb{K}[X]$. Alors $\deg(B) = \deg(Q) + \deg(A)$, donc, comme $\deg(A) = \deg(B)$, $\deg(Q) = 0$, i.e. $Q \in \mathbb{K}^*$. Donc A et B sont associés. ***QED*** ◄

Théroème 9 (de la division euclidienne).

Qu'on donne un polynôme B de $\mathbb{K}[X]$. Supposons que B n'est pas le polynôme nul. Alors pour tout polynôme A de $\mathbb{K}[X]$, on peut trouver un unique couple (R, Q) de $\mathbb{K}[X] \times \mathbb{K}[X]$ tel que

$$A = R + BQ \quad \text{ET} \quad \deg(R) < \deg(B).$$

► ***Démonstration.***

Unicité. Par les degrés.

Existence. Comme $B \neq 0$, nommons $r \in \mathbb{N}$ tel que $r = \deg(B)$.

La partie "existence" de la déduction s'énonce aussi : pour tout $n \in \mathbb{N}$, $\mathcal{P}_n$. Où, pour tout $n \in \mathbb{N}$, on a noté

$\mathcal{P}_n$: « pour tout $A \in \mathbb{K}[X]$, si $\deg(A) \leqslant n$ alors il existe un couple (R, Q) de $\mathbb{K}[X] \times \mathbb{K}[X]$ tel que

$$A = R + BQ \quad \text{ET} \quad \deg(R) < \deg(B)\ .\text{»}$$

Dans le cas où $r \geqslant 1$, on raisonne par récurrence en suivant le traitement de l'algorithme de division euclidienne étudié en salle (initialisation à $n = r - 1$). ***QED*** ◄

Lemme 10 (division dans un sur-corps).

Qu'on donne un polynôme B de $\mathbb{R}[X]$. Supposons que B n'est pas le polynôme nul. Alors pour tout polynôme A de $\mathbb{R}[X]$, le reste et le quotient de la division de A par B en tant que polynômes à coefficients réels sont respectivement égaux au reste et au quotient de la division de A par B en tant que polynômes à coefficients complexes.

Remarque.

Dans ce qui vient, la suite des restes de l'algorithme d'Euclide associé (A, B) en tant que polynômes à coefficients réels est égale à la suite des restes associé à (A, B) en tant que polynômes à coefficients complexes. Donc le PGCD unitaire ne varie pas si on regarde les coefficients du corps $\mathbb{R}$ comme des coefficients du sur-corps $\mathbb{C}$.

1.3 Fonctions polynomiales et racines

Définition 8.

Soit P un polynôme de $\mathbb{K}[X]$, $P(X) = \sum_{k=0}^{n} a_k X^k$. Soit $\alpha \in \mathbb{K}$. L'évaluation de P en α, notée $P(\alpha)$, est l'élément de $\mathbb{K}$

$$P(\alpha) = \sum_{k=0}^{n} a_k \alpha^k.$$

Remarque.

1. On n'écrit pas « prenons $X = \alpha$ » , mais « évaluons P en α » . C'est différent, car X n'est pas une variable dans une fonction, mais une indéterminée.
2. On peut en fait évaluer un polynôme dans des ensembles plus larges, sur des structures appelées $\mathbb{K}$-algèbres (comme les matrices).

Propriété 11.

Soit P dans $\mathbb{K}[X]$, α dans $\mathbb{K}$. Le reste de la division euclidienne de P par $X - \alpha$ est $P(\alpha)$.

► ***Démonstration.***

On sait, par le théorème de la division euclidienne, que l'on dispose de (Q, R) dans $\mathbb{K}[X]$ tels que $P = (X - \alpha)Q + R$, et $\deg(R) < 1$ donc R est constant.

En évaluant l'égalité en α, $P(\alpha) = 0 + R(\alpha)$, donc $R = R(\alpha) = P(\alpha)$. ***QED*** ◄

Corollaire 12.

Soit P dans $\mathbb{K}[X]$, α dans $\mathbb{K}$. Alors $X - \alpha$ divise $P(X)$ si et seulement si $P(\alpha) = 0$.

▶ ***Démonstration.***

$\boxed{\Rightarrow}$ Si $X - \alpha | P$, alors on dispose de Q dans $\mathbb{K}[X]$ tel que $P(X) = (X - \alpha)Q(X)$. En évaluant en α, $P(\alpha) = 0$.

$\boxed{\Leftarrow}$ On sait que l'on dispose de Q dans $\mathbb{K}[X]$ tel que $P(X) = (X - \alpha)Q + P(\alpha)$. Donc si $P(\alpha) = 0$, $P(X) = (X - \alpha)Q$, donc $X - \alpha$ divise P.

QED ◀

Définition 9.

On dit alors que α est une **racine** de P.

Définition 10 : *Et prop.*

Soit P dans $\mathbb{K}[X] \setminus \{0\}$, α dans $\mathbb{K}$. L'ensemble $\{m \in \mathbb{N},\ (X - \alpha)^m | P\}$ possède un plus grand élément. On l'appelle multiplicité de α dans P.

- si cette multiplicité vaut 0, α n'est pas racine de P,
- si cette multiplicité vaut 1, on dit que α est une racine simple de P,
- si cette multiplicité est $\geqslant 2$, on dit que α est racine multiple de P.

Propriété 13.

Soit P dans $\mathbb{K}[X] \setminus \{0\}$, α dans $\mathbb{K}$. $m \in \mathbb{N}$. Les assertions suivantes sont équivalentes :

1. α est de multiplicité m dans P.

2. $(X - \alpha)^m$ divise P mais $(X - \alpha)^{m+1}$ ne divise pas P.

3. Il existe Q dans $\mathbb{K}[X]$ tel que $P(X) = (X - \alpha)^m Q(X)$ et $Q(\alpha) \neq 0$.

▶ ***Démonstration.***

(i)$\Leftrightarrow$(ii) On remarque que

$$\begin{aligned}
\text{(ii)} &\Leftrightarrow \max(\{k \in \mathbb{N},\ (X-\alpha)^k | P\} = m \\
&\Leftrightarrow (X-\alpha)^m | P \text{ et } \forall k > m,\ (X-\alpha)^k \nmid P \\
&\Leftrightarrow (X-\alpha)^m | P \text{ et } (X-\alpha)^{m+1} \nmid P.
\end{aligned}$$

(i)$\Rightarrow$(iii) α est de multiplicité m dans P donc $(X-\alpha)^m$ divise P. Donc on dispose de Q dans $\mathbb{K}[X]$ tel que $P = (X-\alpha)^m Q$. Si on avait $Q(\alpha) = 0$, alors $(X-\alpha)$ diviserait Q donc $(X-\alpha)^{m+1}$ diviserait P, impossible ! Donc $Q(\alpha) \neq 0$.

(iii)$\Rightarrow$(i) Si on dispose de Q dans $\mathbb{K}[X]$ tel que $P(X) = (X-\alpha)^m Q(X)$ et $Q(\alpha) \neq 0$, alors $(X-\alpha)^m | P$.
Si $(X-\alpha)^{m+1}$ divise P, alors on dispose de R dans $\mathbb{K}[X]$ tel que $P(X) = (X-\alpha)^{m+1} R(X)$, donc $(X-\alpha)^m Q(X) = (X-\alpha)^{m+1} R(X)$, donc (par intégrité) $Q(X) = (X-\alpha) R(X)$, donc $Q(\alpha) = 0$, absurde ! D'où (i).

QED ◄

Cette proposition peut nous rappeler la caractérisation de la valuation pour les entiers ! On a d'ailleurs la proposition suivante :

Propriété 14.
Soient P et Q dans $\mathbb{K}[X]$, $\alpha \in \mathbb{K}$. Si $m \in \mathbb{N}$ est la multiplicité de α dans P et n la multiplicité de α dans Q, alors la multiplicité de α dans PQ est $m+n$.

Lemme 15.
Qu'on donne $\alpha \in \mathbb{K}$, $P \in \mathbb{K}[X]$. Supposons $P(\alpha) \neq 0$. Ainsi, pour tout $m \in \mathbb{N}^*$, pour tout $Q \in \mathbb{K}[X]$, si $(X-\alpha)^m$ divise PQ, alors $(X-\alpha)^m$ divise Q.

PREUVE : Récurrence.

Propriété 16.
Soit P dans $\mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_n$ n éléments distincts de $\mathbb{K}$, de multiplicités supérieures à $m_1, \dots, m_n \in \mathbb{N}^*$ respectivement. Alors $(X-\alpha_1)^{m_1} \dots (X-\alpha_n)^{m_n}$ divise P.

► ***Démonstration.***

Démontre par récurrence que pour tout n dans $\mathbb{N}$: pour tout $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$, pour tout $(m_1, \dots, m_n) \in (\mathbb{N}^*)^n$, si les α_i sont distincts et que les $(X - \alpha_i)^{m_i}$ divisent P, alors $(X - \alpha_1)^{m_1} \dots (X - \alpha_n)^{m_n}$ divise P.

Initialisation. Pour $n = 1$, si $\alpha_1 \in \mathbb{N}$, de multiplicité m_1 dans P, $(X - \alpha)^{m_1}$ divise bien P.

Hérédité. Soit n dans $\mathbb{N}$ tel que $\mathcal{P}_n$.

Soient $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$ dans $\mathbb{K}$ des éléments distincts de multiplicités respectives m_1, $\dots$,m_n,m_{n+1}. ***QED*** ◄

Théroème 17.

Un polynôme de degré n possède au plus n racines comptées avec multiplicités.

`Remarque.`

Comptons avec multiplicité les racines de certains polynômes afin de se faire à l'idée de ce que cela signifie.

Corollaire 18.

Si $\mathbb{K}$ est un corps infini, alors

$$\Big(\forall \lambda \in \mathbb{K},\ P(\lambda) = 0\Big) \implies P = 0.$$

`Exemple 1.1.`

(i) Soit P dans $\mathbb{K}[X]$. Alors pour tout $\lambda \in \mathbb{K}$, l'équation $P(x) = \lambda$ a un nombre fini de solutions.

(ii) Quels sont les polynômes tels que pour tout n dans $\mathbb{N}$, $P(n) = n$?

Un autre objet est utile pour comprendre les racines des polynômes : il s'agit de la dérivation.

1.4 Dérivation

Définition 11.
Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme ; où $n \in \mathbb{N}^*$. On appelle polynôme dérivé de P le polynôme nommé P' et défini par

$$P'(X) = \sum_{k=1}^{n} k a_k X^{n-1} = \sum_{\ell=0}^{k-1} (\ell+1) a_{\ell+1} X^{\ell}.$$

On définit aussi la dérivée n-ième de P par récurrence.

Propriété 19.
Soit P dans $\mathbb{K}[X]$, ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), $f : x \mapsto P(x)$ la fonction de la variable réelle associée. Si g est la fonction associée à P', alors g est la dérivée, au sens des fonctions, de f.

Propriété 20.
Pour tous P et Q polynômes de $\mathbb{K}[X]$, pour tout λ dans $\mathbb{K}$ et n dans $\mathbb{N}$,

(i) $(P+Q)' = P' + Q'$

(ii) $(\lambda P)' = \lambda P'$

(iii) $(PQ)' = P'Q + PQ'$

(iv) (formule de Leibniz) $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

"PREUVE : dire que c'est essentiellement calculatoire, et juste dire que les choses marchent bien, et surtout que la dérivation marche comme on veut qu'elle marche !"
Ce qui va vraiment changer, c'est la formule de Taylor, qui est une formule **exacte** pour les polynômes.

Théroème 21 (Formule de Taylor pour les polynômes).

Qu'on donne $\alpha \in \mathbb{K}$, $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Ainsi,

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k.$$

De plus, il y a unicité de la décomposition de P comme combinaison linéaire à coefficients dans $\mathbb{K}$ des polynômes $(X-\alpha)^k$.

► ***Démonstration.***

V1. **Existence** : Vérifier l'égalité pour $P = X^\ell$ puis conclure par combinaison linéaire à cause de la linéarité de la dérivation à tout ordre et de l'évaluation en tout point.

Unicité : Raisonner par l'absurde pour nier qu'il n'existe pas de plus petit indice pour lequel les coefficients sont inégaux (simplification puis évaluation en α) ou pour nier qu'il n'existe pas de plus grand indice pour lequel les coefficients sont inégaux (simplification puis prise du coefficient *canonique* d'un degré bien choisi).

V2. **Existence** : $P(\alpha + X)$ est un polynôme de degré au plus n. donc il se décompose comme combinaison linéaire des X^k. Puis on peut substituer $X-\alpha$ à X.

Unicité : Dérivations successives et évaluations ; après avoir exprimé, notamment à l'aide de la dérivation d'un produit ou en revenant à la définition, les dérivées successives des polynômes $(X-\alpha)^k$. Rappelons que la définition de la dérivée formelle d'un polynôme passe par sa décomposition linéaire canonique.

QED ◄

Cette formule de Taylor permet de comprendre d'une autre manière la notion de multiplicité.

Propriété 22.
Qu'on donne $\alpha \in \mathbb{K}$, $m \in \mathbb{N}$ et $P \in \mathbb{K}[X]$. Ainsi, α est de multiplicité m dans P si, et seulement si

$$\left(\forall k < m,\ P^{(k)}(\alpha) = 0\right) \quad \text{ET} \quad P^{(m)}(\alpha) \neq 0.$$

Cette caractérisation en termes de dérivées n'est pas anecdotique, elle permet de démontrer par exemple la proposition suivante :

Propriété 23.

Qu'on donne $\alpha \in \mathbb{C}$, $m \in \mathbb{N}$ et $P \in \mathbb{C}[X]$. On suppose que tous les coefficients de P sont réels. Ainsi, α est de multiplicité m dans P si, et seulement si, $\overline{\alpha}$ est de multiplicité m dans P.

Il est temps de faire un bilan : qu'a-t-on vu ?

(i) La notion de divisibilité, de divison euclidienne.

(ii) La notion de racine et la factorisation par $(X-a)^m$.

On a l'embryon d'une arithmétique, il faudrait donc tenter de définir toutes les notions qui nous manquent : pgcd, ppcm, polynômes premiers entre eux, et surtout décomposition en facteurs premiers !

2 Arithmétique dans $\mathbb{K}[X]$

2.1 PGCD, PPCM, polynômes premiers entre eux

Définition 12.

On considère deux polynômes A et B de $\mathbb{K}[X]$ non tous les deux nuls. Un PGCD de A et B est diviseur commun à A et B de degré maximal.

PREUVE : L'ensemble $\{\deg(D)\ :\ D \in \mathbb{K}\ /\ D|A\ ,\ D|B\}$ est une partie non vide majorée de $\mathbb{N}$.

Lemme 24 (Préservation des communs diviseurs).

Qu'on donne $A, B \in \mathbb{K}[X]$. Ainsi, pour tout $Q \in \mathbb{K}[X]$, les communs diviseurs de A et B sont les communs diviseurs de B et $A - QB$:

$$\forall D \in \mathbb{K}[X], \qquad (D|A) \wedge (D|B) \iff (D|B) \wedge (D|A - QB).$$

Propriété 25 (Les communs diviseurs).

Soient A et B deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls, Alors

1. I existe au moins un polynôme D tel que les communs diviseurs de A et B sont exactement les diviseurs de D.

2. De plus, les PGCD's de A et B sont les associés d'un tel polynôme.

Propriété 26 (Relation de Bézout).

Soient A et B deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls, D un pgcd de A et B.

Tout diviseur commun à A et B divise D. En particulier, tous les pgcd de A et B sont associés.

Il existe U et V tels que $D = AU + BV$.

Définition 13.

On note $A \wedge B$ l'unique pgcd unitaire de A et B.

PREUVE de la propriété de Bézout :

1. preuve théorique via l'ensemble des combinaisons linéaires : $A\mathbb{K}[X] + B\mathbb{K}[X]$.

2. preuve pratique via l'algorithme d'Euclide étendu.

`Exemple 2.1.`

Déterminer le PGCD de

(i) $X - \alpha$ et $X - \beta$. (exemple très important)

(ii) $X^n - 1$ et $X^p - 1$.

Commentaire : *Attention, à ne pas confondre :*

- *algorithme de la division euclidienne pour calculer le reste et le quotient.*
- *algorithme d'Euclide pour calculer les diviseurs communs et/ou le PGCD unitaire.*
- *algorithme d'Euclide étendu pour calculer un couple de coefficients de Bézout.*

Définition 14.

Deux polynômes A et B sont premiers entre eux si $A \wedge B = 1$.

Théroème 27 (Bézout).

Deux polynômes A et B sont premiers entre eux si et seulement s'il existe U et V deux polynômes tels que $AU + BV = 1$.

Théroème 28 (Gauss).

Si A divise BC et $A \wedge B = 1$ alors A divise C.

Définition 15.

On considère deux polynômes A et B de $\mathbb{K}[X]$ tous les deux non nuls. Un PPCM de A et B est un commun multiple de A et B **non nul** de degré minimal.

Propriété 29 (Les communs multiples).

Soient A et B deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls, Alors

1. Il existe au moins un polynôme M tel que les communs multiples de A et B sont exactement les multiples de M.
2. De plus, les PPCM's de A et B sont les associés d'un tel polynôme.

Définition 16.

On note $A \vee B$ l'unique ppcm unitaire de A et B.

PREUVE :

1. preuve théorique via l'ensemble des multiples communs à A et B : $A\mathbb{K}[X] \cap B\mathbb{K}[X]$.
2. considérer $M = \dfrac{AB}{A \wedge B}$. Soit N un multiple commun à A et à B. Alors $N = PA = QB$. Donc $P\dfrac{A}{A \wedge B} = Q\dfrac{B}{A \wedge B}$, donc $\dfrac{A}{A \wedge B}$ divise Q, donc $N = K\dfrac{AB}{A \wedge B}$, c'est gagné.

Définition 17.

Un pgcd de n polynômes $P_1, \dots, P_n$ non tous nuls est un diviseur commun D à $P_1, \dots, P_n$ de degré maximal. Tout diviseur commun à $P_1, \dots, P_n$ est alors un diviseur de D.

Propriété 30.

Tous les pgcd de $P_1, \dots, P_n$ sont associés. On note $P_1 \wedge \cdots \wedge P_n$ l'unique pgcd unitaire de $P_1, \dots, P_n$.

Propriété 31 (Bézout).

Soient $P_1, \dots, P_n$ n polynômes. Il existe n polynômes $U_1, \dots, U_n$ tels que

$$U_1P_1 + \cdots + U_nP_n = P_1 \wedge \cdots \wedge P_n.$$

Définition 18.

n polynômes $P_1, \dots, P_n$ sont dits premiers entre eux dans leur ensemble si

$$P_1 \wedge \cdots \wedge P_n = 1.$$

Théroème 32 (Bézout).

n polynômes $P_1, \dots, P_n$ sont premiers entre eux dans leur ensemble ssi il existe n polynômes $U_1, \dots, U_n$ tels que

$$U_1P_1 + \cdots + U_nP_n = 1.$$

2.2 Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$, factorisation

Définition 19.

On considère un polynôme P de $\mathbb{K}[X]$. On dit que P est irréductible si, et seulement si, P est non constant et ne se compose pas comme le produit de deux polynômes non constants ; dit autrement, si, et seulement si, P est non constant et que ses seuls diviseurs sont les polynômes associés à 1 et les polynômes associés à P lui-même.

`Remarque.`

Pour unifier cela avec l'arithmétique des entiers : c'est un élément non nul et non inversible (non unité) qui ne se compose pas comme produit de deux tels éléments.

`Exemple 2.2.`

1. **Attention au corps de base !** X^2+1 n'est pas irréductible sur $\mathbb{C}$ (il est divisible par $X-i$) mais est irréductible sur $\mathbb{R}$: en effet, si X^2+1 avait un diviseur non constant et non associé à X^2+1, ce diviseur serait de degré 1, et donc s'annulerait sur $\mathbb{R}$. Donc X^2+1 s'annulerait sur $\mathbb{R}$, ce qui est faux !
2. Aucun polynôme réel de degré impair $\geqslant 3$ n'est irréductible. Soit en effet P un tel polynôme, d le degré de P, λ son coefficient dominant. On écrit toujours P la fonction polynôme associée.

Alors $P(x) \underset{x\to\pm\infty}{\sim} \lambda x^d$, de signe opposé en $+\infty$ et en $-\infty$. P étant continue, elle s'annule donc en un réel α par le théorème des valeurs intermédiaires. P étant divisible par $X-\alpha$, qui n'est ni constant, ni associé à P, donc P n'est pas irréductible.

Propriété 33.

1. Les polynômes de degré 1 sont irréductibles.

2. Si P est un polynôme de degré $\geqslant 2$ qui s'annule sur $\mathbb{K}$, alors P est réductible.

`Remarque.`

Attention le point 2. n'est pas une équivalence ! En effet, $(X^2+1)^2$ ne s'annule pas sur $\mathbb{R}$, mais n'est pas irréductible sur $\mathbb{R}$.

► ***Démonstration.***

1. Soit P de degré 1, Q un diviseur de P. Alors $0 \leqslant \deg(Q) \leqslant \deg(P) = 1$:

(a) si $\deg(Q) = 0$, $Q \in \mathbb{K}^*$,

(b) si $\deg(Q) = 1$, alors P et Q sont associés.

Donc P est irréductible.

2. Soit P de degré 2, dans $\mathbb{K}[X]$, s'annulant sur $\mathbb{K}$. Alors on dispose de α dans $\mathbb{K}$ tel que $P(\alpha) = 0$, donc P est divisible par $X-\alpha$. Mais $X-\alpha$ n'est ni constant, ni associé à P, donc P n'est pas irréductible sur $\mathbb{K}$.

QED ◄

Qui sont les polynômes irréductibles de $\mathbb{C}[X]$? de $\mathbb{R}[X]$? On aura d'abord besoin du

Théroème 34 (D'Alembert-Gauss).

Soit P dans $\mathbb{C}[X]$, non constant. Alors P s'annule sur $\mathbb{C}$.

Corollaire 35.

Les polynômes irréductibles unitaires de $\mathbb{C}[X]$ sont de la forme $X-\alpha$ où $\alpha \in \mathbb{C}$.

► ***Démonstration.***

- Déjà, les polynômes de degré 1 sont irréductibles.

- Soit P dans $\mathbb{C}[X]$, de degré supérieur ou égal à 2. Alors, par le théorème de D'Alembert-Gauss, P s'annule. Mais comme P est de degré supérieur ou égal à 2, P n'est pas irréductible.

QED ◄

Théroème 36 (Décomposition en produit d'irréductibles sur $\mathbb{C}$).
Soit $P \in \mathbb{C}[X]$. Supposons P non nul. Alors P s'écrit

$$P(X) = \Lambda \prod_{i=1}^{r} (X - z_i)^{m_i}.$$

où

- $\Lambda \in \mathbb{C} \setminus \{0\}$,
- $r \in \mathbb{N}$ (Le cas $r = 0$ est inclus),
- $z_1, \ldots, z_r \in \mathbb{C}$ sont distincts,
- $m_1, \ldots, m_r \in \mathbb{N} \setminus \{0\}$,

Cette décomposition est unique à permutation près des facteurs. De plus,

- Λ est le coefficient dominant de P,
- $\deg(P) = \sum_{i=1}^{r} m_i$.

► ***Démonstration.***
On ne donne pas vraiment la preuve, mais l'idée de la preuve :

$\boxed{\exists}$ On démontre l'existence par récurrence sur $\deg(P)$.

— si $\deg(P) = 0$, $P = \Lambda$,

— si $\deg(P) \geqslant 1$, par le théorème de D'Alembert-Gauss, P s'annule sur $\mathbb{C}$, i.e. on dispose de $\alpha \in \mathbb{C}$ tel que $P(\alpha) = 0$. Donc $P(X) = (X - \alpha)Q(X)$ et $\deg(Q) = \deg(P) - 1$. On applique alors la proposition sur Q.

$\boxed{\exists!}$ Si $\Lambda \prod_{i=1}^{r} (X - \alpha_i)^{m_i} = K \prod_{i=1}^{s} (X - \beta_i)^{p_i}$, alors on montre successivement que

— $\Lambda = K$,

— les degrés sont les mêmes,

— $\forall i \in [\![1, r]\!]$, α_i est racine du polynôme de droite, donc égale un β_j, avec la même multiplicité.

QED ◄

On déduit de ceci la décomposition en produit d'irréductibles sur $\mathbb{R}$:

Théroème 37 (Décomposition en produit d'irréductibles sur $\mathbb{R}$.).
Soit $P \in \mathbb{R}[X]$. Supposons P non nul. Alors P s'écrit

$$P(X) = \Lambda \left(\prod_{i=1}^{r} (X - x_i)^{m_i} \right) . \left(\prod_{k=1}^{s} (X^2 + b_k X + c_k)^{n_k} \right)$$

où

- $\Lambda \in \mathbb{R} \setminus \{0\}$,
- $r \in \mathbb{N}$ (Le cas $r = 0$ est inclus),
- $x_1, \dots, x_r \in \mathbb{R}$ sont distincts,
- $m_1, \dots, m_r \in \mathbb{N} \setminus \{0\}$,
- $s \in \mathbb{N}$ (Le cas $s = 0$ est inclus),
- $(b_1, c_1), \dots, (b_s, c_s) \in \mathbb{R}^2$ sont distincts et vérifient : $\forall k \in [\![1, s]\!],\ b_k^2 - 4c_k < 0$,
- $n_1, \dots, n_s \in \mathbb{N} \setminus \{0\}$.

Cette décomposition est unique à permutation près des facteurs. De plus,

- Λ est le coefficient dominant de P,
- $\deg(P) = \sum_{i=1}^{r} m_i + 2 \sum_{k=1}^{s} n_k$.

► ***Démonstration.***
Là, il y a deux choses à démontrer :

- la décomposition : là c'est simple. On prend la décomposition de P sur $\mathbb{C}$ et on rassemble $(X - \alpha_i)^{m_i} (X - \overline{\alpha_i})^{m_i}$, où α_i est une racine complexe non réele de P. Ainsi, on transforme

$$(X-\alpha_i)^{m_i}(X-\overline{\alpha_i})^{m_i} = (X - 2\mathfrak{Re}(\alpha_i)X + |\alpha_i|^2)^{m_i},$$

où

$$(-2\mathfrak{Re}(\alpha_i))^2 - 4|\alpha_i|^2 = 4(\mathfrak{Re}(\alpha_i)^2 - |\alpha_i|) < 0,$$

car $\alpha_i \notin \mathbb{R}$.

- il faut ensuite dire que les polynômes de degré 2 de discriminant strictement négatifs sont irréductibles ! Là aussi c'est simple, il suffit de se dire que si $X^2 + bX + c$ n'est pas irréductible, alors il admet un diviseur **de degré** 1, donc s'annulerait. Absurde !

QED ◀

`Remarque.`

On ne connaît pas bien les polynômes irréductibles de $\mathbb{Q}[X]$. Par exemple, on peut montrer (pas évident !) que si p est un nombre premier, $X^{p-1}+\cdots+X+1$ est irréductible sur $\mathbb{Q}$ (ce polynôme est appelé p-ième polynôme cyclotomique).

Propriété 38 (Décomposition en irréductibles sur $\mathbb{C}$ de X^n-1).

Soit $N \in \mathbb{N}^*$. Alors

$$X^n - 1 = \prod_{\omega\in\mathbb{U}_n}(X-\omega) = \prod_{k=0}^{n-1}(X - e^{\frac{2ik\pi}{n}}).$$

`Exemple 2.3.`

- $X^4-1 = (X-1)(X+1)(X-i)(X+1)$ sur $\mathbb{C}$,
- $X^4-1 = (X-1)(X+1)(X^2+1)$ sur $\mathbb{R}$.

Exo 2.1

1. Faire la décomposition en produit d'irréductibles sur $\mathbb{C}$, puis sur $\mathbb{R}$, de X^4+1.

2. (exo classique) Faire la décomposition en produit d'irréductibles sur $\mathbb{R}$ de X^n-1.

Deux conséquences importantes viennent de cette décomposition en produit d'irréductibles : le lien entre arithmétique des polynômes et racines, ainsi que ce que l'on appelle les relations coefficients-racines.

Propriété 39 (Conséquences arithmétiques : cas complexe).
Soient P et Q dans $\mathbb{C}[X]$.

1. P divise Q si et seulement si pour tout réel α, la multiplicité de α dans P est inférieure ou égale à la multiplicité de α dans Q.
2. Si $\alpha_1, \ldots, \alpha_r$ sont les racines distinctes de P ou de Q, si

$$P(X) = \prod_{i=1}^{r}(X-\alpha_i)^{m_i} \text{ et } Q(X) = \prod_{i=1}^{r}(X-\alpha_i)^{n_i},$$

avec certains exposants éventuellement nuls, alors

$$P \wedge Q = \prod_{i=1}^{r}(X-\alpha_i)^{\min(m_i,n_i)} \text{ et } P \vee Q = \prod_{i=1}^{r}(X-\alpha_i)^{\max(m_i,n_i)}.$$

3. P et Q sont premiers entre eux si et seulement s'ils n'ont pas de racine en commun.

`Remarque.`

Comment la proposition précédente s'adapte-t-elle sur $\mathbb{R}$?

- si P et Q sont scindés, les trois propositions précédentes sont toujours vraies.
- sinon, il faut mettre en jeu la puissance associée à chaque polynôme irréductible de degré 2 : la proposition précédente devient moins utilisable.

Moralité : pour faire de l'arithmétique, mieux vaut toujours passer dans $\mathbb{C}[X]$.

`Exemple 2.4.`

1. Si $P = (X-1)(X-2)^2$ et $Q = (X-1)^3(X-\pi)$, $P \not| Q$, $P \wedge Q = X-1$ et $P \vee Q = (X-1)^3(X-2)^2(X-\pi)$.
2. **TRÈS IMPORTANT**, à retenir (mais pas écrit comme complètement au programme, donc à

réécrire). Soit $P \in \mathbb{C}[X]$. Déjà P est scindé. On a alors les équivalences suivantes

$$\begin{aligned} & P \text{ est scindé à racines simples} \\ \Leftrightarrow & \forall \alpha \text{ racine de } P,\ P'(\alpha) \neq 0 \\ \Leftrightarrow & P \text{ et } P' \text{ n'ont pas de racines en commun} \\ \Leftrightarrow & P \wedge P' = 1. \end{aligned}$$

Pourquoi est-ce important ? Car, grâce à l'algorithme d'Euclide notamment, on n'a pas besoin de connaître les racines de P pour calculer $P \wedge P'$.

3. La proposition ne fonctionne pas sur $\mathbb{R}$: il faudrait aussi prendre en compte les facteurs irréductibles de degré 2.

`Exemple 2.5.`

Développer

$$K(X-\alpha_1)(X-\alpha_2)$$

puis

$$K(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$$

puis enfin

$$K(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$$

Que remarquez-vous sur les coefficients ?

Propriété 40 (Relations de Viète ou coefficients-racines).
Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme scindé non constant, $\alpha_1, \dots, \alpha_n$ ses racines (éventuellement comptées avec multiplicités). On définit, pour k dans $[\![1, n]\!]$,

$$\sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} \alpha_{i_1} \dots \alpha_{i_k}.$$

Alors pour tout k dans $[\![1, n]\!]$,

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

`Remarque.`

1. Les racines sont, ici, comptées avec multiplicité, c'est-à-dire que si $P = (X-1)^3(X-\pi)^2$,

$$\alpha_1 = 1,\ \alpha_2 = 1,\ \alpha_3 = 1,\ \alpha_4 = \pi,\ \alpha_5 = \pi$$

2. Deux formules sont à connaître en priorité : la somme et le produit. Si $P = \sum_{k=0}^{n} a_k X^k$ un polynôme scindé, $\alpha_1, \dots, \alpha_n$ ses racines, alors

$$\alpha_1 \times \dots \times \alpha_n = (-1)^n \frac{a_0}{a_n}$$

et

$$\alpha_1 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n}.$$

`Exemple 2.6.`

Explicitons les formules dans le cas d'un polynôme de degré 3.

`Exemple 2.7` *Exercice important*.

Retrouvons les formules pour la somme et le produit des racines de l'unité. Soit $n \geqslant 2$. Alors

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega)$$

On écrit $X^n - 1 = \sum_{k=0}^{n} a_k X^k$. En particulier, $a_0 = -1$ et $a_{n-1} = 0$, $a_n = 1$.
Alors, par les relations coefficients-racines,

$$\sum_{\omega \in \mathbb{U}_n} \omega = -\frac{a_{n-1}}{a_n} = \frac{0}{1} = 0$$

De même,

$$\prod_{\omega \in \mathbb{U}_n} \omega = (-1)^n \frac{a_0}{a_n} = (-1)^{n+1}.$$

3 Formule d'interpolation de Lagrange

Exo 3.2

On veut trouver au moins un polynôme P de $\mathbb{C}[X]$ qui prend aux points 1, 2 et 3 les valeurs 26, 24 et 25 respectivement, et décrire tous les polynômes de la sorte s'il en existe.

1. (*Voie naïve*) Chercher P sous la forme $P = a + bX + cX^2$.

2. (*Principe de substitution*) Chercher P sous la forme $P = a' + b'(X-1) + c'(X-1)(X-2)$.

3. (*Principe de superposition*) Chercher P sous la forme $P = a''L_1 + b''L_2 + c''L_3$; où L_1, L_2, L_3 sont les polynômes de degrés égaux à 2 qui prennent la valeur 0 sur $\{1, 2, 3\}$ sauf en $1, 2, 3$ respectivement où ils prennent respectivement la valeur 1.

Idée.

- on sait que par deux points, il ne passe qu'une droite : si $\deg(P) \leqslant 1$, si on fixe $P(a)$ et $P(b)$, alors P est déterminé de manière unique.
- si (a, b, c) sont 3 éléments de $\mathbb{K}$ distincts, si α, β et γ sont dans $\mathbb{K}$, on peut montrer qu'il existe un unique P de degré $\leqslant 2$ tel que $P(a) = \alpha$, $P(b) = \beta$ et $P(c) = \gamma$.

Question. Peut-on généraliser ? Si l'on prend $(x_0, \dots, x_n)$ $n+1$ points distincts, $(y_0, \dots, y_n)$ $n+1$ valeurs (pas forcément distinctes), peut-on trouver P de degré inférieur ou égal à n tel que pour tout i, $P(x_i) = y_i$?
La réponse est oui ! L'idée principale est de chercher à d'abord trouver un polynôme qui s'annule en tous les (x_i) sauf un.

Exo 3.3

Trouver une expression d'un polynôme s'annulant en $x_1, \dots, x_n$ mais pas en x_0.

Définition 20.
Soit $n \in \mathbb{N}$, $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$, deux à deux distincts.
La base d'interpolation de Lagrange associée à $(x_0, \dots, x_n)$ est la famille de polynômes $(L_0, \dots, L_n)$ définie par

$$\forall i \in [\![0, n]\!],\ L_i(X) = \prod_{\substack{0 \leqslant k \leqslant n \\ k \neq i}} \frac{X - x_k}{x_i - x_k}.$$

Exo 3.4

Donner la base d'interpolation de Lagrange associée à -1, 1, 3.

Propriété 41.

Soit $n \in \mathbb{N}$, $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$, deux à deux distincts, $(L_0, \dots, L_n)$ la base d'interpolation de Lagrange associée à $(x_0, \dots, x_n)$.

1. $\forall (i,j) \in [\![0, n]\!]^2,\ L_i(x_j) = \delta_{ij} = \begin{cases} 0 & \text{si } x_j \neq x_i \\ 1 & \text{si } x_j = x_i \end{cases}$.

2. $\deg(L_i) = n$ (« nombre de points d'interpolation, moins un »).

`Représentation.`

$$\begin{bmatrix} L_0(x_0) & L_1(x_0) & L_2(x_0) & \cdots & L_n(x_0) \\ L_0(x_1) & L_1(x_1) & L_2(x_1) & \cdots & L_n(x_1) \\ L_0(x_2) & L_1(x_2) & L_2(x_2) & & \\ \vdots & \vdots & & \ddots & \\ L_0(x_n) & L_1(x_n) & & & L_n(x_n) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1 \end{bmatrix}$$

.

► ***Démonstration.***

1. Soit $(i,j) \in [\![0, n]\!]^2$. $L_i(x_j) = \prod_{\substack{0 \leqslant k \leqslant n \\ k \neq i}} \frac{x_j - x_k}{x_i - x_k}$.

- si $i = j$, $L_i(x_i) = \prod_{\substack{0 \leqslant k \leqslant n \\ k \neq i}} \frac{x_i - x_k}{x_i - x_k} = \prod_{\substack{0 \leqslant k \leqslant n \\ k \neq i}} 1 = 1$,
- sinon, on dispose de k dans $[\![0, n]\!]$, différent de i, tel que $k = j$. Alors $x_j - x_k = 0$, donc $L_i(x_j) = 0$.

2. RAS !

QED ◄

Propriété 42.

Soient $x_0, \dots, x_n$ $n+1$ éléments de $\mathbb{K}$ deux à deux distincts, $y_0, \dots, y_n$ $n+1$ éléments de $\mathbb{K}$. Alors il existe un unique polynôme P de $\mathbb{K}_n[X]$ tel que

$$\forall k \in [\![0, n]\!],\ P(x_k) = y_k.$$

On a la formule $P(X) = \sum_{i=0}^{n} y_i L_i(X)$, où $(L_0, \ldots, L_n)$ est la base d'interpolation de Lagrange associée à $(x_0, \ldots, x_n)$.

Un tel polynôme P est appelé polynôme interpolateur de Lagrange associé aux points $(x_0, \ldots, x_n)$ et aux valeurs $(y_0, \ldots, y_n)$.

► ***Démonstration.***

Existence. Soit $(L_0, \ldots, L_n)$ la base d'interpolation de Lagrange associée à $(x_0, \ldots, x_n)$. Posons $P(X) = \sum_{i=0}^{n} y_i L_i(X)$. Soit j dans $[\![1, n]\!]$. Alors

$$P(x_j) = \sum_{i=0}^{n} y_i L_i(x_j) = \sum_{i=0}^{n} y_i \delta_{ij} = y_j.$$

Unicité. Soit Q un autre polynôme de degré inférieur ou égal à n vérifiant : $\forall i \in [\![1, n]\!]$, $Q(x_i) = y_i$. Alors pour tout i dans $[\![1, n]\!]$,

$$(P - Q)(x_i) = P(x_i) - Q(x_i) = y_i - y_i = 0.$$

Donc $P - Q$ s'annule $n + 1$ fois et est dans $\mathbb{K}_n[X]$, donc $P - Q$ est nul. Donc $Q = P$, d'où l'unicité. ***QED*** ◄

Corollaire 43 (Un corollaire important).

Soit P dans $\mathbb{K}_n[X]$, $(x_0, \ldots, x_n) \in \mathbb{K}^{n+1}$ deux à deux distincts, $(L_0, \ldots, L_n)$ la base d'interpolation de Lagrange associée. Alors

$$P = \sum_{i=0}^{n} P(x_i) L_i.$$

`Exemple 3.1.`

Soit P un polynôme de $\mathbb{C}[X]$ tel que $P(\mathbb{R}) \subset \mathbb{R}$. Montrer que $P \in \mathbb{R}[X]$. Même question avec $\mathbb{Q}$.

Propriété 44.

Soient $(x_0, \dots, x_n)$ des éléments de $\mathbb{K}$ deux à deux distincts, $(y_0, \dots, y_n) \in \mathbb{K}^{n+1}$. Soit P le polynôme interpolateur de Lagrange associé aux points $(x_0, \dots, x_n)$ et aux valeurs $(y_0, \dots, y_n)$. Alors

$$\{Q \in \mathbb{K}[X] \mid \forall i \in [\![0, n]\!],\ Q(x_i) = y_i\} = \{P + R \times \prod_{i=0}^{n}(X - x_i)\ :\ R \in \mathbb{K}[X]\}.$$

`Remarque.`

Ceci doit vous faire penser à la forme des solutions d'un système linéaire.

► ***Démonstration.***

Soit Q dans $\mathbb{K}[X]$. Alors on a les équivalences

$$\begin{aligned}
\forall i \in [\![0, n]\!],\ Q(x_i) = y_i &\Leftrightarrow \forall i \in [\![0, n]\!],\ Q(x_i) = P(x_i) \\
&\Leftrightarrow \forall i \in [\![0, n]\!],\ (Q - P)(x_i) = 0 \\
&\Leftrightarrow (X - x_0) \times \cdots \times (X - x_n) \text{ divise } Q - P \\
&\Leftrightarrow \exists R \in \mathbb{K}[X],\ Q - P = R \times (X - x_0) \times \cdots \times (X - x_n) \\
&\Leftrightarrow \exists R \in \mathbb{K}[X],\ Q = P + R \times (X - x_0) \times \cdots \times (X - x_n)
\end{aligned}$$

D'où l'égalité des ensembles. ***QED*** ◄

4 Fractions rationnelles

4.1 Construction

Nous allons faire le point sur une construction d'un corps de fractions à partir d'un anneau (HP, mais avoir une idée de la manière dont les choses sont construites).

Définition 21 : *et prop.*

Soit A un anneau intègre. On définit sur $A^* \times A$ deux lois d'addition et de multiplication

(i) Une addition : $(n\ ,\ d) + (n'\ ,\ d') = (d'n + dn'\ ,\ dd')$.

(ii) Une multiplication : $(n\ ,\ d) \times (n'\ ,\ d') = (nn'\ ,\ dd')$.

On définit aussi une relation d'équivalence sur $A \times A^*$ par $(n\ ,\ d) \sim (n'\ ,\ d') \Leftrightarrow dn' = d'n$.

La relation $\sim$ est une relation d'équivalence compatible avec $+$ et $\times$. De plus, l'ensemble $(A \times A^*)/\sim$ des classes d'équivalence, dont les éléments sont notés $\frac{n}{d}$, muni des deux lois induites $+$ et $\times$, est un corps appelé corps des fractions de A. C'est le plus petit corps contenant A.

Exemple 4.1.
$\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. On rappelle que $\frac{n}{d}$ est le multiplicateur pour passer de d à n.

Définition 22.

1. On définit alors l'ensemble $\mathbb{K}(X)$ comme le corps des fractions de $\mathbb{K}[X]$, appelé corps des fractions rationnelles en une indéterminée.
2. Une fraction rationnelle F est donc représenté par au moins un couple $(N\ ,\ D)$ de polynômes où D est non nul. On note $R = \frac{N}{D}$ et on note que le couple $(N\ ,\ D)$ n'est pas unique !
3. Si $(P_1, P_2) \in \mathbb{K}[X]^2$, si $(Q_1, Q_2) \in (\mathbb{K}[X] \setminus \{0\})^2$, $\frac{P_1}{Q_1} = \frac{P_2}{Q_2}$ si et seulement si $P_1Q_2 = P_2Q_1$.
4. $(\mathbb{K}(X), +, \times)$ est donc un corps.
5. Si $R = \frac{P}{Q}$ et $Q|P$, alors $R \in \mathbb{K}[X]$.
6. Si $R_1 = \frac{P_1}{Q_1}$ et $R_2 = \frac{P_2}{Q_2}$,
$$R_1 + R_2 = \frac{P_1Q_2 + P_2Q_1}{Q_1Q_2} \text{ et } R_1 \times R_2 = \frac{P_1P_2}{Q_1Q_2}.$$
7. Si $R = \frac{P}{Q}$ et $P \neq 0$, alors l'inverse de R est noté $\frac{1}{R}$.

8. Si $R = \dfrac{P}{Q}$, avec $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_k X^k$, si $S \in \mathbb{K}(X)$ est non constante, on définit

$$R \circ S = \frac{\sum_{k=0}^{n} a_k S^k}{\sum_{k=0}^{p} b_k S^k}.$$

`Remarque.`

Il faut penser que les fractions rationnelles se manipulent comme on le souhaiterait !

1. $\dfrac{X+1}{X^2-2X+1} = \dfrac{X}{X^2-2X+1} + \dfrac{1}{X^2-2X+1} = \dfrac{X+1}{(X-1)^2} = \dfrac{1}{X-1} + \dfrac{2}{(X-1)^2}$

2. $\dfrac{2X^2-2}{3(X^2-2X+1)} = \dfrac{2(X-1)(X+1)}{3(X-1)^2} = \dfrac{2(X+1)}{3(X-1)}$.

Définition 23.

Soit $R \in \mathbb{K}(X)$. Un représentant irréductible de R est un couple $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$ tels que

- $R = \dfrac{P}{Q}$,
- $P \wedge Q = 1$,
- Q est unitaire.

Propriété 45.

Toute fraction rationnelle admet un unique représentant irréductible.

▶ ***Démonstration.***

$\boxed{\exists}$ Soit (P, Q) un représentant de R.

Alors on dispose de $(A, B) \in \mathbb{K}[X]^2$ tels que $P = A \times (P \wedge Q)$ et $Q = B \times (P \wedge Q)$. Alors $AQ = BP$, donc $R = \dfrac{A}{B}$, avec $A \wedge B = 1$. Maintenant, si λ est le coefficient dominant de B,

$$R = \frac{\frac{1}{\lambda}A}{\frac{1}{\lambda}B},$$

et $\dfrac{1}{\lambda}B$ est bien unitaire.

$\boxed{\exists!}$ Supposons que $R = \dfrac{P}{Q} = \dfrac{A}{B}$ avec (P, Q) premiers entre eux, (A, B) premiers entre eux, Q et B unitaires. Alors $PB = QA$. Donc

— B divise QA, $B \wedge A = 1$ donc, par le théorème de Gauss, $B|Q$,

— $Q|PB$, $Q \wedge P = 1$, donc, par le théorème de Gauss, $Q|B$,

donc B et Q sont associés. Comme ils sont unitaires, ils sont égaus. Donc $B = Q$, comme $PB = QA$, $P = A$.

QED ◄

Définition 24.
Soit $R = \dfrac{P}{Q}$ une fraction rationnelle. La quantité $\deg(P) - \deg(Q)$ est indépendante du représentant choisi. On l'appelle degré de la fraction rationnelle.

► ***Démonstration.***
Si $R = \dfrac{P}{Q} = \dfrac{A}{B}$, $PB = QA$ donc $\deg(P) + \deg(B) = \deg(Q) + \deg(A)$, donc

$$\deg(P) - \deg(Q) = \deg(A) - \deg(B)$$

QED ◄

`Remarque.`
Attention ! Une fraction de degré nul n'est pas forcément constante !

On a les formules que l'on veut avoir pour le degré :

Propriété 46.
Soit $(R, S) \in \mathbb{K}(X)^2$.

1. $\deg(R + S) \leqslant \max(\deg(R), \deg(S))$, avec égalité si $\deg(R) \neq \deg(S)$,

2. $\deg(R \times S) = \deg(R) + \deg(S)$,

3. si $R \neq 0$, $\deg \dfrac{1}{R} = -\deg(R)$,

4. si S est non constante, $\deg(R \circ S) = \deg(R) \times \deg(S)$.

Définition 25.
Soit $R = \dfrac{P}{Q}$ une fraction rationnelle. Alors la quantité $\dfrac{P'Q - PQ'}{Q^2}$ ne dépend pas du

couple représentant de R choisi. On l'appelle dérivée de R et on note

$$R' = \frac{P'Q - PQ'}{Q^2}.$$

Propriété 47.
La dérivation vérifie les mêmes règles algébriques que la dérivation des fonctions.

Définition 26.
Soit $R = \dfrac{P}{Q}$ une fraction de $\mathbb{K}(X)$ sous forme irréductible.

1. Un zéro de R est une racine de P.

2. Un pôle de R est une racine de Q.

Si λ est un pôle, la multiplicité de λ dans R est la multiplicité de λ en tant que racine de Q.

`Exemple 4.2.`
Si $R = \dfrac{X^2+2X+1}{(X-2)^2(X+1)(X^2+1)} = \dfrac{X+1}{(X-2)^2(X^2+1)}$,

- sur $\mathbb{R}$: -1 est un zéro de $\mathbb{R}$, 2 est le seul pôle de $\mathbb{R}$,
- sur $\mathbb{C}$: -1 est un zéro de $\mathbb{R}$, 2, i et $-i$ sont les pôles de $\mathbb{R}$.

La notion de pôle et de zéro dépend du corps de base.

Définition 27.
Soit $R \in \mathbb{K}(X)$, $R = \dfrac{P}{Q}$, sous forme irréductible, $\lambda \in \mathbb{K}$. Si λ n'est pas un pôle de R, on peut définir l'évaluation de R en λ par

$$R(\lambda) = \frac{P(\lambda)}{Q(\lambda)}.$$

4.2 Décomposition en éléments simples sur $\mathbb{C}$ et sur $\mathbb{R}$

Le but de cette section est pratique, il est d'écrire sous une forme bien particulière les fractions rationnelles : c'est la décomposition en éléments simples.
Pourquoi faire des décompositions en éléments simples ?

(i) aspect pratique : calcul d'intégrales.

(ii) aspect + théorique : théorème de Gauss-Lucas (exo de la fin)

Propriété 48.

Qu'on donne $P, Q \in \mathbb{K}[X]$. Supposons que $Q \neq 0$ et $P \wedge Q = 1$. Ainsi, il existe un unique couple $(E, P_1) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que

$$\frac{P}{Q} = E + \frac{P_1}{Q} \qquad \text{ET} \qquad \deg(P_1) < \deg(Q).$$

Propriété 49.

Qu'on donne $R \in \mathbb{K}(X)$. Ainsi, il existe un unique couple $(E, S) \in \mathbb{K}(X) \times \mathbb{K}(X)$ tel que

$$R = E + S \qquad \text{ET} \qquad E \in \mathbb{K}[X] \qquad \text{ET} \qquad \deg(S) < 0.$$

On appelle E partie entière de R.

► ***Démonstration.***

Écrivons $R = \dfrac{P}{Q}$ sous forme irréductible.

$\boxed{\exists}$ Effectuons la division euclidienne de P par Q : $P = AQ + B$, avec $\deg(B) < \deg(Q)$. ALors

$$\frac{P}{Q} = \frac{AQ + B}{Q} = A + \frac{B}{Q},$$

$A \in \mathbb{K}[X]$ et $\deg(B) - \deg(Q) < 0$.

$\boxed{\exists!}$ Supposons $R = E + S = F + T$, où $(E, F) \in \mathbb{K}[X]$ et $(S, T) \in \mathbb{K}(X)$ avec $\deg(S) < 0$ et $\deg(T) < 0$. Alors $E - F = T - S$. et $\deg(T - S) < 0$. Or, si $E \neq F$ alors $\deg(E - F) \geqslant 0$. Donc $E = F$, et $T = S$.

QED ◄

`Exemple 4.3.`

Déterminer la partie entière de $\dfrac{X^3 + X^2 + 3X + 1}{(X-1)(X-2)}$.

Propriété 50 (Décomposition en éléments simples sur $\mathbb{C}$).

Soit R dans $\mathbb{C}(X)$, $R = \dfrac{P}{Q}$ avec $P \wedge Q = 1$. Soient $z_1, \ldots, z_r$ les racines distinctes de Q et $m_1, \ldots, m_r$ leurs multiplicités respectives. Il existe E dans $\mathbb{C}[X]$, de degré

$\deg(R)$ si $\deg(R) > 0$ (nul sinon), et des complexes $(w_{k\ell})_{\substack{1\leqslant k\leqslant r\\1\leqslant \ell\leqslant m_k}}$ tel que

$$R(X) = E(X) + \sum_{k=1}^{r}\left(\sum_{\ell=1}^{m_k}\frac{w_{k\ell}}{(X-z_k)^{\ell}}\right).$$

Exemple 4.4.

Déterminons la forme de la DES de $\dfrac{4X^2+3X-1}{(X-1)^2X^3}$.

Propriété 51 (Décomposition en éléments simples sur $\mathbb{R}$).

Soit R dans $\mathbb{R}(X)$, $R = \dfrac{P}{Q}$, irréductible, telle que la décomposition de Q en produit d'irréductibles soit

$$Q(X) = \Lambda\left(\prod_{i=1}^{r}(X-x_i)^{m_i}\right)\left(\prod_{k=1}^{s}(X^2+b_kX+c_k)^{n_k}\right).$$

(avec $b_k^2 - 4c_k < 0$). Alors il existe E dans $\mathbb{R}[X]$, de degré $\deg(R)$ si $\deg(R) > 0$ (nul sinon), et des réels $(\alpha_{ij})_{\substack{1\leqslant i\leqslant r\\1\leqslant j\leqslant m_i}}$, $\left((\beta_{k\ell},\gamma_{k\ell})\right)_{\substack{1\leqslant k\leqslant s\\1\leqslant \ell\leqslant n_k}}$, tels que

$$R(X) = E(X) + \sum_{i=1}^{r}\left(\sum_{j=1}^{m_i}\frac{\alpha_{ij}}{(X-x_i)^{j}}\right) + \sum_{k=1}^{s}\left(\sum_{\ell=1}^{n_k}\frac{\beta_{k\ell}X+\gamma_{k\ell}}{(X^2+b_kX+c_k)^{\ell}}\right).$$

Exemple 4.5.

Exemples avec $\dfrac{3X+2}{X^2(X^2+1)}$, $\dfrac{(X-3)^4}{(X^2+X+1)^3}$.

► ***Démonstration.***

Nous n'allons pas donner l'existence en détail, mais juste donner quelques aspects intéressants de la preuve :

- la **partie entière** s'obtient à l'aide de la **division euclidienne** de P par Q.
- Si $R = \dfrac{P}{Q_1Q_2}$ avec Q_1 et Q_2 premiers entre, eux, par le théorème de Bézout, on peut écrire $Q_1U_1 + Q_2U_2 = 1$, donc

$$\frac{P}{Q_1Q_2} = \frac{Q_1PU_1 + Q_2PU_2}{Q_1Q_2} = \frac{PU_1}{Q_2} + \frac{PU_2}{Q_1},$$

donc on peut « séparer » les termes premiers entre eux,

- si on s'intéresse à un terme du type

$$\frac{P}{(X-\alpha)^m},$$

avec $\deg(P) < m$, une formule de Taylor nous permet d'écrire cette fraction comme

$$\frac{\sum_{k=0}^{m} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k}{(X-\alpha)^m} = \sum_{k=0}^{m} \frac{\frac{P^{(k)}(\alpha)}{k!}}{(X-\alpha)^{m-k}}$$

QED ◄

4.3 Méthodes de calcul

Méthode 1 [Les trois premières étapes].
Ce sont **toujours** les mêmes :

1. On calcule la partie entière via une division euclidienne,

2. on vérifie que la fraction est irréductible,

3. on écrit la décomposition théorique.

Maintenant, comment gérer les différents pôles ?

Propriété 52 (Pôles simples).
Soit $R \in \mathbb{K}(X)$ une fraction rationnelle, $R = \frac{P}{Q}$ (irréductible), α un pôle simple de R. Le coefficient a de $\frac{1}{X-\alpha}$ dans la D.E.S. de R est donné par l'une de ces deux formules :

- si $Q = (X-\alpha)\tilde{Q}$, $a = \frac{P(\alpha)}{\tilde{Q}(\alpha)}$.
- $a = \frac{P(\alpha)}{Q'(\alpha)}$.

► ***Démonstration.***
Il faut penser à la décomposition en éléments simples théorique : si on multiplie tout par $(X-\alpha)$, on obtient, à gauche $\frac{P}{\tilde{Q}}$ et, à droite, des quantités qui vont toutes s'annuler en

α sauf une.

Pour la deuxième formule, il suffit de remarquer que

$$Q' = \tilde{Q} + (X - \alpha)\tilde{Q}',$$

et donc $Q'(\alpha) = \tilde{Q}(\alpha)$. ***QED*** ◄

Méthode 2 [Pôle simple].

4. pour déterminer le coefficient de $\dfrac{1}{X-\alpha}$, on multiplie R et la DES théorique par $X - \alpha$ et on évalue en α.

Exemple. $\dfrac{1}{(X-1)(X-2)(X-3)} = \dfrac{a}{X-1} + \dfrac{b}{X-2} + \dfrac{c}{X-3}$

Pour déterminer le coefficient de $\dfrac{1}{X-1}$, on multiplie tout par $X - 1$

$$\frac{1}{(X-2)(X-3)} = a + \frac{b(X-1)}{X-2} + \frac{c(X-1)}{X-3}$$

et on évalue en 1 :

$$\frac{1}{(-1)(-2)} = a + 0 + 0,$$

i.e. $a = \dfrac{1}{2}$.

Exo 4.5

Parfois, la formule avec la dérivée peut servir ! Déterminer la DES de $\dfrac{1}{X^n - 1}$

Méthode 3.

5. Pôles multiples. Si α est un pôle de multiplicité m dans $\mathbb{R}$,

- le coefficient de $\dfrac{1}{(X-\alpha)^m}$ s'obtient comme les pôles simples : on multiplie tout par $(X - \alpha)^m$ et on évalue en α.

Exemple. Si $R = \dfrac{2X+1}{(X-1)^2(X+2)}$, on sait que

$$R = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+2}.$$

En multipliant par $(X-1)^2$,

$$\frac{2X+1}{X+2} = a(X-1) + b + \frac{c(X-1)^2}{X+2},$$

donc, en évaluant en 1, $\dfrac{3}{3} = b$.

- pour les autres coefficients, c'est plus délicat :
  - — la méthode systématique est de soustraire le terme en $\dfrac{1}{(X-\alpha)^m}$ à R, et de tout remettre au même dénominateur : on obtient une nouvelle fraction rationnelle dont α est un pôle de multiplicité $m-1$.

    Exemple. dans la fraction précédente,

    $$R = \frac{a}{X-1} + \frac{1}{(X-1)^2} + \frac{c}{X+2}.$$

    Donc

    $$\begin{aligned} R - \frac{1}{(X-1)^2} &= \frac{2X+1}{(X-1)^2(X+2)} - \frac{1}{(X-1)^2} \\ &= \frac{2X+1-(X+2)}{(X-1)^2(X+2)} \\ &= \frac{X-1}{(X-1)^2(X+2)} \\ &= \frac{1}{(X-1)(X+2)}. \end{aligned}$$

    En multipliant par $X-1$ et en évaluant en 1, on obtient $a = \dfrac{1}{3}$.
  - — une autre méthode peut être d'évaluer en certains points (si le coefficient dur à trouver est le dernier).

    Exemple. Revenons à l'exemple précédent, en supposant que l'on n'a pas trouvé a. On était arrêtés à

$$R = \frac{a}{X-1} + \frac{1}{(X-1)^2} + \frac{c}{X+2}.$$

On trouve très facilement c, en multipliant par $X+2$ et en évaluant en -2 : $c = -\frac{1}{3}$. Donc

$$R = \frac{a}{X-1} + \frac{1}{(X-1)^2} - \frac{1}{3(X+2)}.$$

Ensuite, on évalue en 0 :

$$\frac{1}{2} = -a + 1 - \frac{1}{6},$$

donc $a = 1 - \frac{1}{6} - \frac{1}{2} = \frac{1}{3}$.

— une dernière possibilité, très efficace pour des termes en $\frac{1}{X-\alpha}$, est de multiplier par X, d'évaluer en $x \in \mathbb{R}$ et de faire tendre x vers $+\infty$.
Toujours dans notre exemple, si on revient à

$$\frac{2X+1}{(X-1)^2(X+2)} = \frac{a}{X-1} + \frac{1}{(X-1)^2} - \frac{1}{3(X+2)},$$

alors pour tout x dans $\mathbb{R}$,

$$\frac{x(2x+1)}{(x-1)^2(x+2)} = \frac{xa}{x-1} + \frac{x}{(x-1)^2} - \frac{x}{3(x+2)},$$

soit, en faisant tendre x vers $+\infty$,

$$0 = a + 0 - \frac{1}{3}.$$

6. Cas des éléments irréductibles de degré 2 dans $\mathbb{R}$.

- si l'élément irréductible de degré 2 est à la puissance 1, on peut faire la DES sur $\mathbb{C}$ et mettre au même dénominateur.
Exemple. $\frac{2X+1}{X^2(X^2+1)} = \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X-i} + \frac{d}{X+i}$.

$c = \dfrac{2i+1}{i^2 \times 2i} = -1 + \dfrac{i}{2}$.
Comme la fraction est réelle, elle est égale à son conjugué donc, par unicité de la DES, $d = \overline{c} = -1 - \dfrac{i}{2}$. Alors l'élément simple de degré 2 est

$$\begin{aligned}\frac{c}{X-i} + \frac{d}{X+i} &= \frac{-1+\frac{i}{2}}{X-i} + \frac{-1-\frac{i}{2}}{X+i} \\ &= \frac{-2X-1}{X^2+1}\end{aligned}$$

Cette méthode ne fonctionne pas si l'élément simple a une puissance > 1 : ainsi

$$2\frac{X^2-1}{(X^2+1)^2} = \frac{1}{(X-i)^2} + \frac{1}{(X+i)^2}$$

En rassemblant les deux, on retombe sur la formule de départ, qui n'est pas une DES.

- si on doit faire la DES de $\dfrac{P}{(X^2+bX+c)^m}$, déjà, on n'a pas de chance. Ensuite, on peut s'en sortir à l'aide de divisions euclidiennes successives :

$$P(X) = (X^2+bX+c)Q(X) + \alpha X + \beta,$$

donc

$$\frac{P(X)}{(X^2+bX+c)^m} = \frac{Q(X)}{(X^2+bX+c)^{m-1}} + \frac{\alpha X+\beta}{(X^2+bX+c)^m}$$

Exemple. DES de $R(X) = \dfrac{X^4}{(X^2+1)^3}$.

— $X^4 = (X^2+1)(X^2-1)+1$, donc

$$R(X) = \frac{X^2-1}{(X^2+1)^2} + \frac{1}{(X^2+1)^3}.$$

$X^2 - 1 = (X^2+1)1 - 2$ donc

$$R(X) = \frac{1}{X^2+1} - \frac{2}{(X^2+1)^2} + \frac{1}{(X^2+1)^3}.$$

7. penser aux trois « méthodes originales » que l'on a vues : évaluer en un point, multiplier par X et prendre la limite, ou le cas des fractions réelles (coefficients complexes conjugués)

4.4 Intégrales de fractions rationnelles

But : pouvoir calculer l'intégrale d'une fraction rationnelle.

Méthode 4.

1. Faire la DES de la fraction rationnelle (sur $\mathbb{R}$ ou sur $\mathbb{C}$)
2. On calcule l'intégrale de chaque élément simple :
   - si $\alpha \in \mathbb{R}$, $\displaystyle\int \frac{1}{x-\alpha}dx = \ln(|x-\alpha|)$,
   - si $m > 1$, $\displaystyle\int \frac{1}{(x-\alpha)^m} = \frac{1}{-m+1}(X-\alpha)^{-m+1}$,

   Exemple : calculer $\displaystyle\int_0^1 \frac{x}{(x+1)(x+2)^2}dx$.
   - $\displaystyle\int \frac{dx}{x^2-a^2} = \frac{1}{2a}\ln\left|\frac{x-a}{x+a}\right|$,
   - $\displaystyle\int \frac{1}{1+x^2}dx = \text{Arctan}(x)$,
   - $\displaystyle\int \frac{dx}{a^2+x^2} = \frac{1}{a}\text{Arctan}\frac{x}{a}$,
   - pour calculer $\displaystyle\int \frac{dx}{x^2+bx+c}$ avec $b^2-4c<0$, on passe par la forme canonique,
   - pour calculer $\displaystyle\int \frac{px+q}{x^2+bx+c}dx$ avec $b^2-4c<0$, on fait apparaître la dérivée du dénominateur.
   - pour calculer $\displaystyle\int \frac{px+q}{(x^2+bx+c)^m}dx$ avec $b^2-4c<0$, déjà on n'a pas de chance... On fait ensuite apparaître la dérivée du dénominateur et on se ramène à calculer $\displaystyle\int \frac{dx}{(x^2+bx+c)^m}$. Pour cette intégrale, changement de variables pour se ramener à $\displaystyle\frac{1}{(x^2+1)^m}$, et IPP + récurrence.

4.5 Intégrales de fractions en sin/cos/tan

On veut calculer une intégrale qui est une fraction rationnelle en $\sin/\cos/\tan$, par exemple

$$\int_0^{\frac{\pi}{4}} \frac{\sin^3(x)}{1+\cos^2(x)}dx.$$

L'idée est d'opérer un changement de variables qui va nous ramener à une fraction rationnelle. Il existe des règles « toutes faites », dites « règles de Bioche » mais elles ne sont pas au programme et encombrent la tête pour rien.

Méthode 5.

Si on veut calculer une primitive ou une intégrale d'une fraction rationnelle en $\sin / \cos / \tan$:

- si la fraction peut s'écrire sous la forme $R(\sin(\theta))\cos(\theta)$, alors on pose $t = \sin(\theta)$,
- si la fraction peut s'écrire sous la forme $R(\cos(\theta))\sin(\theta)$, alors on pose $t = \cos(\theta)$,
- si la fraction peut s'écrire sous la forme $R(\tan(\theta))(1+\tan^2(\theta))$, alors on pose $t = \tan(\theta)$,
- si rien ne marche, on pose $t = \tan(\theta/2)$. Alors $\sin(\theta) = \dfrac{2t}{1+t^2}$, $\cos(\theta) = \dfrac{1-t^2}{1+t^2}$ et $\tan(\theta) = \dfrac{2t}{1-t^2}$.

4.6 Un résultat théorique important : dérivée logarithmique

Exo 4.6

Pour tout $n \in \mathbb{N}^*$, pour tous $P_1, P_2, \dots, P_n \in \mathbb{K}[X] \setminus \{0\}$,

1. $(P_1P_2\cdots P_n)' = \cdots$
2. $\dfrac{(P_1P_2\cdots P_n)'}{P_1P_2\cdots P_n} = \cdots$

Propriété 53.

Soit $P(X) = \Lambda \prod_{i=1}^{r}(X-\alpha_i)^{m_i}$ avec $\Lambda \in \mathbb{K}^*$, $(\alpha_1, \dots, \alpha_r) \in \mathbb{K}^r$, deux à deux distincts, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$. Alors

1. $P'(X) = \Lambda \sum_{i=1}^{r} m_i(X-\alpha_i)^{m_i-1} \prod_{\substack{1\leqslant k\leqslant r\\ k\neq i}} (X-\alpha_k)^{m_k}$,

2. $\dfrac{P'}{P} = \displaystyle\sum_{i=1}^{r} \dfrac{m_i}{X - \alpha_i}$.

Voyons une jolie application de ce résultat :

Définition 28.

Soit $(z_1, \dots, z_n) \in \mathbb{C}^n$, $z \in \mathbb{C}$. On dit que z est dans l'enveloppe convexe de $(z_1, \dots, z_n)$ s'il existe $(\lambda_1, \dots, \lambda_n) \in [0, 1]^n$ tels que

$$z = \sum_{i=1}^{n} \lambda_i z_i \text{ et } \sum_{i=1}^{n} \lambda_i = 1.$$

`Remarque.`

Il faut voir cette définition comme signifiant que z est « à l'intérieur » du polygône formé par les points $(z_1, \dots, z_n)$, ou que z est une moyenne des points $(z_1, \dots, z_n)$.

Théroème 54 (Théorème de Gauss-Lucas – Hors-Programme complet !).

Soit $P \in \mathbb{C}[X]$. Alors les racines de P' sont dans l'enveloppe convexe des racines de P.

► ***Démonstration.***

Écrivons $P(X) = \Lambda \displaystyle\prod_{i=1}^{r} (X - \alpha_i)^{m_i}$. Soit z une racine de P'.

- si z est une racine de P, c'est ok !
- sinon, $P'(z) = 0$ donc $\dfrac{P'(z)}{P(z)} = 0$. Donc, par la décomposition en éléments simples de $\dfrac{P'}{P}$,

$$\frac{P'(z)}{P(z)} = \sum_{k=1}^{r} \frac{m_k}{z - \alpha_k},$$

donc, en multipliant chaque fraction de la somme par la quantité conjuguée,

$$\sum_{k=1}^{r} \frac{m_k(\overline{z} - \overline{\alpha_k})}{|z - \alpha_k|^2} = 0,$$

donc, en conjuguant,
$$\sum_{k=1}^{r} \frac{m_k(z-\alpha_k)}{|z-\alpha_k|^2} = 0,$$

Posons alors $\mu_k = \dfrac{m_k}{|z-\alpha_k|^2}$. Alors

$$\sum_{k=1}^{r} \mu_k(z-\alpha_k) = 0,$$

i.e.
$$\sum_{k=1}^{r} \mu_k z = \sum_{k=1}^{r} \mu_k \alpha_k$$

donc
$$z = \sum_{k=1}^{r} \frac{\mu_k}{\sum_{i=1}^{r} \mu_i} \alpha_k = \sum_{k=1}^{r} \lambda_k \alpha_k,$$

avec $\lambda_k = \dfrac{\mu_k}{\sum_{i=1}^{r} \mu_i} \in [0,1]$, et $\displaystyle\sum_{k=1}^{r} \lambda_k = 1$.

D'où le résultat ! ***QED*** ◄

Tâches de manipulation

1. Choisir un polynôme à coefficients complexes de degré inférieur à trois, en choisissant ses coefficients dans la base canonique. L'exprimer
   - Dans une base de Taylor par dérivations et évaluations suivant la méthode de Hörner.
   - Dans une base de Newton (HP : exlue de la référence commune).
   - Dans une base de Lagrange.

   Puis vérifier l'égalité des quatre expressions par des développements pour exprimer les trois dernières dans la base canonique de décomposition linéaire.
2. Choisir deux polynômes non constants à coefficients réels de degrés inférieurs à cinq.
   - Calculer leur PGCD unitaire suivant l'algorithme d'Euclide.
   - Calculer un couple de Bézout associé suivant l'algorithme d'Euclide étendu.
   - Les factoriser par leur PGCD unitaire.
   - Calculer leur PPCM unitaire à l'aide du lien entre PGCD et PPCM.
3. Choisir un polynôme non constant à coefficients réels de degré inférieur à cinq en choisissant ses coefficients canoniques.
   - Calculer son polynôme dérivé.
   - Calculer son PGCD unitaire avec son polynôme dérivé.
   - Décider si le polynôme de départ admet un facteur carré.

Retour sur les formules de Viète

Pour bien comprendre les formules de Viète, il faut **absolument** faire soi-même le travail de développement de $\lambda(X-\omega_1)(X-\omega_2)$ et $\lambda(X-\omega_1)(X-\omega_2)(X-\omega_3)$. La compréhension de ces formules ne **peut pas** s'apprendre en lisant ou en regardant des vidéos, il faut **écrire soi-même** pour comprendre.

Développons encore...

On écrit (mais il **faut** que vous refassiez cet effort de développer par vous même)

$$\begin{aligned}\lambda(X-\omega_1)(X-\omega_2) &= \lambda X^2 - \lambda(\omega_1+\omega_2)X + \lambda\omega_1\omega_2\\ \lambda(X-\omega_1)(X-\omega_2)(X-\omega_3) &= \lambda X^3 - \lambda(\omega_1+\omega_2+\omega_3)X^2\\ &\quad + \lambda(\omega_1\omega_2+\omega_1\omega_3+\omega_2\omega_3)X - \lambda\omega_1\omega_2\omega_3\end{aligned}$$

Et, pour vous, le développement pour 4 :

$$\begin{aligned}&\lambda(X-\omega_1)(X-\omega_2)(X-\omega_3)(X-\omega_4)\\ &= \lambda X^4 - \lambda(\omega_1+\omega_2+\omega_3+\omega_4)X^3\\ &\quad + \lambda(\omega_1\omega_2+\omega_1\omega_3+\omega_1\omega_4+\omega_2\omega_3+\omega_2\omega_4+\omega_3\omega_4)X^2\\ &\quad - \lambda(\omega_1\omega_2\omega_3+\omega_1\omega_2\omega_4+\omega_1\omega_3\omega_4+\omega_2\omega_3\omega_4)X + \lambda\omega_1\omega_2\omega_3\omega_4\end{aligned}$$

Reconnaissons les coefficients...

Regardez chacune des trois expressions :

- le coefficient de degré $n-1$ est, **dans tous les cas**, $-\lambda\times(\omega_1+\cdots+\omega_n)$, i.e. $-\lambda$ fois la somme des coefficients,
- le coefficient de degré $n-2$ est, **dans tous les cas**, $-\lambda$ fois la somme des produits de deux coefficients : $\omega_1\omega_2+\omega_2\omega_3+\ldots$. Comment écrire cette somme ? On peut l'écrire comme
$$\sum_{1\leqslant i<j\leqslant n}\omega_i\omega_j,$$
ou bien, **COMME LES VARIABLES DE SOMMATION SONT MUETTES,**
$$\sum_{1\leqslant j_1<j_2\leqslant n}\omega_{j_1}\omega_{j_2}.$$
(**REGARDEZ BIEN !** j_1 **et** j_2 **sont des NOMS de variables. C'est tout.**)
- le coefficient de degré $n-3$ (à regarder dans le dernier produit qu'on a développé) est égal à tous les produits de trois coefficients, c'est-à-dire à $\omega_1\omega_2\omega_3+\omega_1\omega_2\omega_4+\ldots$:

on peut écrire cette somme

$$\sum_{1\leqslant i<j<k\leqslant n} \omega_i\omega_j\omega_k$$

que l'on peut réécrire

$$\sum_{1\leqslant j_1<j_2<j_3\leqslant n} \omega_{j_1}\omega_{j_2}\omega_{j_3}$$

(**REGARDEZ BIEN ! j_1, j_2 et j_3 sont des NOMS de variables. C'est tout.**) On peut encore réécrire cette quantité comme

$$\sum_{1\leqslant j_1<j_2<j_3\leqslant n} \prod_{k=1}^{3} \omega_{j_k}$$

Retour sur σ_i

En faisant le chemin inverse, on peut comprendre σ_i :

$$\sigma_i = \sum_{1\leqslant j_1<\cdots<j_i\leqslant n} \prod_{k=1}^{i} \omega_{j_k}.$$

(**REGARDEZ BIEN ! $j_1, j_2, \ldots, j_i$ sont des NOMS de variables. C'est tout.**) On peut faire le chemin inverse, en regardant σ_1, σ_2, σ_3, σ_4 :

- $\sigma_1 = \sum_{1\leqslant j_1\leqslant n} \prod_{k=1}^{1} \omega_{j_k} = \sum_{1\leqslant j_1\leqslant n} \omega_{j_1} \boxed{=} \sum_{1\leqslant k\leqslant n} \omega_k$
- $\sigma_2 = \sum_{1\leqslant j_1<j_2\leqslant n} \prod_{k=1}^{2} \omega_{j_k} = \sum_{1\leqslant j_1<j_2\leqslant n} \omega_{j_1}\omega_{j_2} \boxed{=} \sum_{1\leqslant k<\ell\leqslant\leqslant n} \omega_k\omega_\ell = \omega_1\omega_2 + \omega_1\omega_3 + \cdots$
- $\sigma_3 = \sum_{1\leqslant j_1<j_2<j_3\leqslant n} \prod_{k=1}^{3} \omega_{j_k} = \sum_{1\leqslant j_1<j_2<j_3\leqslant n} \omega_{j_1}\omega_{j_2}\omega_{j_3} \boxed{=} \sum_{1\leqslant k<\ell<m\leqslant\leqslant n} \omega_k\omega_\ell\omega_m = \omega_1\omega_2\omega_3 + \omega_1\omega_2\omega_4 + \cdots$

Tous les « $\boxed{=}$ » sont vrais car les variables de sommation sont muettes.

Errata

Page ..

- exemple .., le degré de R est -4 et pas -3.
- exemple .., une coquille dans la factorisation, il y a du $X+1$ au lieu du $X+3$
- exemple .., il manque un terme en $\dfrac{h}{X+1}$.

DEBUT △