N. Laillet
nlaillet.math@gmail.com

Chapitre 16
Polynômes

1 Anneau des polynômes à une indéterminée

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

1.1 Construction

Cette partie diffère beaucoup du cours que vous avez eu en classe. Elle est très incomplète...

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.

Proposition 2
Deux polynômes sont égaux si et seulement si leurs coefficients sont tous égaux.

Définition 3 (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 $P \times Q = (c_n)_{n\in\mathbb{N}}$ et

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

(produit de Cauchy).

Proposition 4
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 $(\delta_{0,n})_{n\in\mathbb{N}}$.

N. Laillet
nlaillet.math@gmail.com

Définition 5

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

Proposition 6

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

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. ■

Proposition 7

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 $a_j \neq 0$ et $P = \sum_{k=0}$

Remarque 8

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

Définition 9

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.

N. Laillet
nlaillet.math@gmail.com

(iii) Si $a_d = 1$, on dit que P est unitaire.

Remarque 10

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

Définition 11

L'indéterminée X étant fixée, on appelle $\mathbb{K}[X]$ 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 degré n.

Remarque 12

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

Proposition 13

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

(i) $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$.

(ii) $\deg(P \times Q) = \deg(P) + \deg(Q)$.

PREUVE

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

Proposition 14

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

PREUVE

Définition 15

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

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

N. Laillet
nlaillet.math@gmail.com

Proposition 16

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 17

Soient A et B deux polynômes à coefficients dans $\mathbb{K}$. On dit que A divise B et on écrit $A|B$ s'il existe $P \in \mathbb{K}[X]$ tel que $B = AP$.

Proposition 18

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

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

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

(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 19

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

Proposition 20

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

Proposition 21

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.

Théorème 22

Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$. Alors il existe deux polynômes Q et R tels que

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

N. Laillet
nlaillet.math@gmail.com

1.3 Fonctions polynomiales et racines

Définition 23

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 α, est l'élément de $\mathbb{K}$

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

Remarque 24

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).

Proposition 25

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 $R = R(\alpha) = P(\alpha)$. ■

Corollaire 26

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

Définition 27

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

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.

■

Définition 28 (Et prop)

Soit P dans $\mathbb{K}[X]$, 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.

Proposition 29

Soit P dans $\mathbb{K}[X]$, 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)⇔(ii) On remarque que

$$\begin{aligned}(\text{ii}) &\Leftrightarrow \max(\{k \in \mathbb{N},\ (X-\alpha)^k | P\} = m \\ &\Leftrightarrow (X-\alpha)^m | P \text{ et } \forall k > m,\ (X-\alpha)^k \not| P \\ &\Leftrightarrow (X-\alpha)^m | P \text{ et } (X-\alpha)^{m+1} \not| P.\end{aligned}$$

(i)⇒(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)⇒(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).

■

Cette proposition peut nous faire penser à la caractérisation de la valuation ! On a d'ailleurs la proposition suivante :

Proposition 30

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

Proposition 31

Soit P dans $\mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_n$ n éléments de $\mathbb{K}$, de multipicités respectives $m_1, \dots, m_n$. Alors $(X-\alpha_1)^{m_1} \dots (X-\alpha_n)^{m_n}$ divise P.

Démonstration

Démontre par récurrence que pour tout n dans $\mathbb{N}$:

$\forall (\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$, éléments de $\mathbb{K}$, de multipicités respectives $m_1, \dots, m_n$, $(X-\alpha_1)^{m_1} \dots (X-\alpha_n)^{m_n}$ divise P. $(\mathcal{Q}_n)$

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 $\mathbb{K}^{n+1}$ de multiplicités respectives $(m_1, dots, m_{n+1})$. ■

Théorème 32

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

Remarque 33

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

Corollaire 34

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

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

Exemple 35

(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

N. Laillet
nlaillet.math@gmail.com

Définition 36

Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme. On appelle polynôme dérivé de P le polynôme nommé P' et défini par

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

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

Proposition 37

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.

PREUVE : ok

Proposition 38

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.

Théorème 39 (Formule de Taylor pour les polynômes)

Soit P un polynôme de degré n sur $\mathbb{K}$, α dans $\mathbb{K}$. Alors

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

PREUVE : partir de $\alpha = 0$ (en écrivant bêtement ce qu'est la dérivée), et faire des translations pour se ramener au cas $\alpha = 0$.

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

Proposition 40

Soit P un polynôme de $\mathbb{K}[X]$, α dans $\mathbb{K}$, $m \in \mathbb{N}$. α est une racine de P de multiplicité m si, et seulement si

$$\left(\forall k \leqslant m,\ P^{(k)}(\alpha) = 0\right) \text{ et } P^{(m+1)}(\alpha) \neq 0.$$

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

Proposition 41

Soit P un polynôme de $\mathbb{R}[X]$, $\alpha \in \mathbb{C}$. Alors α est racine de P de multiplicité m si, et seulement si $\overline{\alpha}$ est racine de P de multiplicité m.

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 42

Soient A et B deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. L'ensemble $\text{div}(A, B) = \{D \in \mathbb{K}[X], D|A \text{ et } D|B\}$ est une partie majorée de $\mathbb{N}$, elle possède donc un élément maximal d. Tout polynôme de $\text{div}(A, B)$ de degré d est appelé PGCD de A et B.

PREUVE évidente

Proposition 43 (Proposition 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, et il existe U et V tels que $D = AU + BV$.

Définition 44

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

PREUVE de la proposition de Bézout :

N. Laillet
nlaillet.math@gmail.com

1. preuve théorique via l'ensemble des combinaisons linéaires
2. preuve pratique via l'algorithme d'euclide.

Exemple 45

Déterminer le PGCD de

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

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

Définition 46

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

Exemple 47

Exemples.

Théorème 48 (Bézout)

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

Théorème 49 (Gauss)

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

Définition 50

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

Proposition 51

Tout multiple commun à A et à B est multiple d'un PPCM de A et B.
Il existe donc un unique PPCM unitaire de A et B, noté $A\vee B$.

PREUVE : 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.

N. Laillet
nlaillet.math@gmail.com

Définition 52

Un pgcd de n polynômes $P_1, \dots, P_n$ 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.

Proposition 53

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

Proposition 54 (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 55

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

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

Théorème 56 (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

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

N. Laillet
nlaillet.math@gmail.com

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

Définition 57

Un polynôme P de $\mathbb{K}[X]$ est irréductible si P n'est pas constants et si ses seuls diviseurs sont soit constants non nuls, soit les polynômes associés à P.

Exemple 58

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.

Proposition 59

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 n'est pas irréductible.

Remarque 60

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 $\mathbb{K}$.

■

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

N. Laillet
nlaillet.math@gmail.com

Théorème 61 (D'Alembert-Gauss)

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

Corollaire 62

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.

■

Théorème 63 (Décomposition en produit d'irréductibles sur $\mathbb{C}$)

Soit $P \in \mathbb{C}[X]$, non nul. Alors il existe $\Lambda \in \mathbb{C}$, $r \in \mathbb{N}$, $(\alpha_1, \dots, \alpha_r) \in \mathbb{C}^r$, deux à deux distincts, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$, tels que

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

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

- K est le coefficient dominant de P,
- $\deg(P) = m_1 + \cdots + m_r$.

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.

■

N. Laillet
nlaillet.math@gmail.com

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

Théorème 64 (Décomposition en produit d'irréductibles sur $\mathbb{R}$.)

Soit $P \in \mathbb{R}[X]$, non nul. Alors il existe

- $\Lambda \in \mathbb{R}^*$,
- $r \in \mathbb{N}$, $(\alpha_1, \dots, \alpha_r) \in \mathbb{R}$, deux à deux distincts, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$,
- $s \in \mathbb{N}$, $\Big((b_1, c_1), \dots, (b_s, c_s)\Big) \in (\mathbb{R}^2)^s$, deux à deux distincts, vérifiant $\forall i \in [\![1, s]\!]$, $b_i^2 - 4c_i < 0$, $(n_1, \dots, n_s) \in (\mathbb{N}^*)^s$

tels que

$$P(X) = \Lambda \left(\prod_{i=1}^{r} (X - \alpha_i)^{m_i} \right) . \left(\prod_{j=1}^{s} (X^2 + b_j X + c_j)^{n_j} \right)$$

De plus, cette décomposition est unique à permutation près, Λ est le coefficient dominant de P et $\deg(P) = \sum_{i=1}^{r} m_i + 2 \sum_{j=1}^{s} n_j$.

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 !

■

Remarque 65

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).

N. Laillet
nlaillet.math@gmail.com

Proposition 66 (Décomposition en irréductibles sur $\mathbb{C}$ de X^n-1)

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

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

Exemple 67

1. $X^4 - 1 = (X-1)(X+1)(X-i)(X+1)$ sur $\mathbb{C}$,
   et $X^4 - 1 = (X-1)(X+1)(X^2+1)$ sur $\mathbb{R}$.
2. Faire la décomposition en produit d'irréductibles sur $\mathbb{C}$, puis sur $\mathbb{R}$, de X^4+1.
3. (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.

Proposition 68 (Conséquences arithmétiques)

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 $(\alpha_1, \dots, \alpha_r)$ est l'ensemble des racines 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 69

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 $\mathbb{C}[X]$.

N. Laillet
nlaillet.math@gmail.com

Exemple 70

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 71

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 ?

Proposition 72 (Relations de Viète ou coefficients-racines)

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme scindé, $\alpha_1, \dots, \alpha_n$ ses racines (éventuellement comptées avec multiplicité). 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 73

N. Laillet
nlaillet.math@gmail.com

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

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

et

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

Exemple 74

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

Exemple 75 (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

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 $P(c) = \gamma$.

N. Laillet
nlaillet.math@gmail.com

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.

Exercice 1. Trouver une expression d'un polynôme s'annulant en $x_1, \dots, x_n$ mais pas en x_0.

Définition 76

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

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

Exercice 77

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

Proposition 78

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. $\deg(L_i) = n$,
2. $\forall (i, j) \in [\![0, n]\!]^2,\ L_i(x_j) = \delta_{ij}$.

Démonstration

1. Évident,
2. 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 $L_i(x_j) = 0$.

■

N. Laillet
nlaillet.math@gmail.com

Proposition 79

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 $(L_0, \dots, L_n)$ est la base d'interpolation de Lagrange associée à $(x_0, \dots, x_n)$.
Un tel polynôme P est appelé polynôme interpolateur de Lagrange associé aux points $(x_0, \dots, x_n)$ et aux valeurs $(y_0, \dots, y_n)$.

Démonstration

Existence. Soit $(L_0, \dots, L_n)$ la base d'interpolation de Lagrange associée à $(x_0, \dots, x_n)$. 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. ■

Corollaire 80 (Un corollaire important)

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

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

Exemple 81

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 $\mathbb{Q}$.

N. Laillet
nlaillet.math@gmail.com

Proposition 82

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

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

Remarque 83

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. ■