

Polynômes

I Généralités	2
Construction formelle (HP, MAIS...)	
Définition informelle	
Loi de composition	
Aparté sur la parité	
II Degré d'un polynôme et $\mathbb{K}_n[X]$	8
III Évaluation d'un polynôme en...	11
IV Divisibilité et division euclidienne	12
V Racines et critère de nullité	13
VI Multiplicité d'une racine	15
Définition et amélioration du critère de nullité	
Relation coefficients-racines pour un polynôme scindé	
VII Dérivation chez les polynômes	18
Polynôme dérivé	
Un peu de « primitivation »	
Polynômes dérivés successifs	
Deux belles formules!	
Retour sur la multiplicité : critère différentiel	
Racine d'un polynôme à coefficients réels	
VIII Factorisation	22
Polynômes irréductibles	
Théorème de d'Alembert-Gauss	
Factorisation dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$	



Dans ce chapitre, on utilisera la lettre $\mathbb{K}$ pour désigner l'ensemble des nombres réels ou l'ensemble des nombres complexes. Ainsi $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. Un élément de $\mathbb{K}$ sera appelé « un scalaire ».

I. Généralités

La notion de polynôme vous est déjà familière via les fonctions polynomiales $x \mapsto a_0 + a_1x + \dots + a_nx^n$ définie sur $\mathbb{R}$. La plupart des propriétés de ces *fonctions* polynomiales sont « formelles », c'est-à-dire ne dépendent que des *coefficients*.

D'où l'idée d'introduire une nouvelle notion, celle de « polynôme (formel) », en se basant uniquement sur la *suite des coefficients*, qui est une suite *nulle à partir d'un certain rang* : on dit que la suite est *presque nulle*.

Construction formelle (HP, MAIS...)

On rappelle que l'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites à coefficients dans $\mathbb{K}$, muni des lois $+$ et $\cdot$ définies par :

$$u + v = (u_n + v_n)_{n \in \mathbb{N}} \quad \lambda \cdot u = (\lambda u_n)_{n \in \mathbb{N}}$$

est un $\mathbb{K}$ -espace vectoriel.

1

Proposition. L'ensemble des suites presque nulles, noté ici $\widehat{\mathbb{K}^{\mathbb{N}}}$, est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$.

Preuve.

- La suite nulle est évidemment une suite presque nulle.
- Soit $A = (a_k)_{k \in \mathbb{N}}$ et $B = (b_k)_{k \in \mathbb{N}}$ deux suites de $\widehat{\mathbb{K}^{\mathbb{N}}}$. Soit $\lambda, \mu \in \mathbb{K}$.
Comme A et B sont deux suites presque nulles, il existe p et q tels que $\forall k > p, a_k = 0$ et $\forall k > q, b_k = 0$.
La suite $\lambda \cdot A + \mu \cdot B$ est la suite de terme général $\lambda a_k + \mu b_k$. Donc pour tout $k > \max(p, q)$, ce terme est nul.
Donc $\lambda \cdot A + \mu \cdot B$ est une suite presque nulle.

2

Définition (loi $\times$ pour l'ensemble $\widehat{\mathbb{K}^{\mathbb{N}}}$ des suites presque nulles).

Considérons $A = (a_k)_{k \in \mathbb{N}}$ et $B = (b_k)_{k \in \mathbb{N}}$ deux suites presque nulles.

On définit $A \times B$, noté encore AB , comme étant la suite $(c_k)_{k \in \mathbb{N}}$ de terme général

$$c_k = \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j$$

Cette suite $AB = (c_k)_{k \in \mathbb{N}}$ est une suite presque nulle.

- **Preuve.** Comme A et B sont deux suites presque nulles, il existe p et q tels que

$$\forall k > p, a_k = 0 \quad \text{et} \quad \forall k > q, b_k = 0$$

Montrons que pour tout $k > p + q$, on a $c_k = 0$.

Considérons un couple (i, j) tel que $i + j = k$. On a nécessairement $i > p$ ou $j > q$ (sans quoi on aurait $i + j \leq p + q < k$).

Ainsi, tous les termes de la somme $c_k = \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j$ sont nuls, donc $c_k = 0$.

- **Propriétés.** Le produit ainsi défini sur $\widehat{\mathbb{K}^{\mathbb{N}}}$ est

- associatif, autrement dit $(AB)C = A(BC)$
- commutatif, autrement dit $AB = BA$
- distributif sur la loi $+$, autrement dit $A(B + C) = AB + AC$
- compatible avec la loi $\cdot$, autrement dit $\lambda \cdot (AB) = (\lambda \cdot A)B = A(\lambda \cdot B)$
- muni d'un élément neutre, à savoir **la suite U définie par** $(1, 0, 0, \dots)$, c'est-à-dire la suite de terme général $(\delta_{k,0})_{k \in \mathbb{N}}$. Autrement dit, on a $AU = UA = A$.



- **Puissance d'une suite presque nulle.**

Soit $A \in \widehat{\mathbb{K}^{\mathbb{N}}}$. On définit par récurrence les puissances successives de A en posant : $\begin{cases} A^0 = U \\ \forall n \in \mathbb{N}, A^{n+1} = AA^n \end{cases}$

Que vaut U^2 ?

- **Remarque.** On peut reformuler la loi $\cdot$ avec la loi $\times$:

$$\forall \lambda \in \mathbb{K}, \quad \lambda \cdot U = (\lambda, 0, \dots, 0) \times U$$

En effet, $(\lambda, 0, 0, \dots) \times U = (\lambda \cdot U) \times U = \lambda \cdot (U \times U) = \lambda \cdot U$

Autrement dit, étant donné un scalaire $\lambda \in \mathbb{K}$, on peut sans ambiguïté le « plonger » dans $\widehat{\mathbb{K}^{\mathbb{N}}}$, c'est-à-dire le voir comme la suite presque nulle $(\lambda, 0, 0, \dots)$. Cette dernière phrase signifie que l'application

$\mathbb{K} \rightarrow \widehat{\mathbb{K}^{\mathbb{N}}}$ est linéaire injective.

$$\lambda \mapsto \lambda \cdot U$$

L'apparition de la suite $X = (0, 1, 0, 0, \dots)$

- **Action de décalage!**

Soit $A \in \widehat{\mathbb{K}^{\mathbb{N}}}$. Que vaut XA ? où $X = (0, 1, 0, 0, \dots)$ est la suite de terme général $(\delta_{k,1})_{k \in \mathbb{N}}$.

Réponse. C'est la suite de terme général c_k où

$$c_k = \sum_{i=0}^k \delta_{i,1} a_{k-i} = \begin{cases} 0 & \text{si } k=0 \\ a_{k-1} & \text{sinon} \end{cases}$$

Ainsi, $XA = (0, a_0, a_1, a_2, \dots)$.

- **Puissance de X .**

Que vaut X^0 ?

Que vaut X^2 ?

Réponse. En écrivant $X^2 = X \times X$ et en prenant $A = X$ dans le point précédent, on obtient $X^2 = (0, 0, 1, 0, 0, \dots)$.

Par récurrence, on montre que : $\forall p \in \mathbb{N}, \quad X^p = (0, \dots, 0, 1, 0, \dots)_p$

- **Lien entre $\widehat{\mathbb{K}^{\mathbb{N}}}$ et les X^k . Une suite presque nulle est une combinaison linéaire de puissances de X .**

Preuve. Soit $A \in \widehat{\mathbb{K}^{\mathbb{N}}}$. Alors il existe $n \in \mathbb{N}$ tel que $A = (a_0, a_1, \dots, a_n, 0, 0, \dots)$.

On ne dit rien sur la nullité des a_k : ils peuvent être nuls ou pas.

Par définition des lois $+$ et $\cdot$, on a alors :

$$\begin{aligned} A &= a_0 \cdot (1, 0, 0, \dots) \\ &+ \\ &\quad a_1 \cdot (0, 1, 0, \dots) \\ &+ \\ &\quad a_2 \cdot (0, 0, 1, \dots) \\ &+ \\ &\quad \vdots \\ &+ \\ &\quad a_n \cdot (0, \dots, 0, 1, 0, \dots) \end{aligned}$$

En utilisant la suite X , cela se réécrit :

$$A = a_0 \cdot X^0 + a_1 \cdot X^1 + a_2 \cdot X^2 + \dots + a_n \cdot X^n$$

De plus, on a vu que $X^0 = U$ et que $\lambda \cdot U$ peut s'identifier à λ .

Ainsi, $a_0 \cdot X^0$ s'identifie à a_0 et on peut donc omettre le X^0 dans l'écriture.

On peut aussi omettre le $\cdot$ partout pour alléger :

$$A = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$$

Et voilà un polynôme formel d'indéterminée X .

Définition informelle

3

Définition.

- Un polynôme P à coefficients dans $\mathbb{K}$ est une expression de la forme $\sum_{k=0}^n a_k X^k$, c'est-à-dire

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 X^0$$

où $a_0, a_1, \dots, a_n \in \mathbb{K}$ et $n \in \mathbb{N}$.

- Les scalaires $a_0, \dots, a_n$ sont appelés les coefficients du polynôme.
Le scalaire a_k s'appelle le coefficient en X^k de P . En PCSI 3, il sera parfois noté $\text{coeff}_{X^k}(P)$
- L'ensemble de ces polynômes est noté $\mathbb{K}[X]$ (on lit « K crochet X »).
La « lettre » X s'appelle l'*indéterminée*.

- **Reformulation.** Par définition, se donner un polynôme revient à se donner la suite (nulle à partir d'un certain rang) de ses coefficients.
- **Exemple.**
Le polynôme $7X^2 + 1$ peut s'écrire $7X^2 + 0X + 1$ ou $0X^3 + 7X^2 + 0X + 1$ ou $0X^4 + 0X^3 + 7X^2 + 0X + 1$.
Ce polynôme est codé par la suite presque nulle $(1, 0, 7, 0, 0, \dots)$.
- **Coefficient constant.** Le coefficient constant de P est a_0 .
- **Le polynôme nul.** Il y a un polynôme très particulier, c'est le polynôme nul, celui dont tous les coefficients sont nuls ! Il est noté $0_{\mathbb{K}[X]}$.
- **Polynôme constant.** On peut considérer un scalaire $a \in \mathbb{K}$ comme le polynôme aX^0 (que l'on notera simplement a). Un tel polynôme est appelé un polynôme constant.
- **Notation.**
Un polynôme se notera P ou bien $P(X)$ (cela dépendra des jours de la semaine).
Mais attention, en analyse, une fonction s'appelle toujours f (jamais $f(x)$).
- **Inclusion.** Comme $\mathbb{R} \subset \mathbb{C}$, un polynôme à coefficients réels peut être vu comme un polynôme à coefficients complexes. On a donc $\mathbb{R}[X] \subset \mathbb{C}[X]$.

Par construction de $\mathbb{K}[X]$, on a :

4

Faits.

- **Identification des coefficients.**
Deux polynômes sont égaux si et seulement s'ils ont les mêmes coefficients.
- **Le polynôme nul.** Le polynôme nul est le polynôme dont tous ses coefficients sont nuls !
Autrement dit :

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = 0_{\mathbb{K}[X]} \iff \forall k \in \llbracket 0, n \rrbracket, \quad a_k = 0$$



Définition (opérations algébriques).

Soit $P, Q \in \mathbb{K}[X]$ deux polynômes que l'on écrit $P = \sum_{k=0}^p a_k X^k$ et $Q = \sum_{k=0}^q b_k X^k$

Il est pratique de poser $\begin{cases} a_k = 0 & \text{pour } k > p \\ b_k = 0 & \text{pour } k > q \end{cases}$

- La multiplication de P par $\lambda \in \mathbb{K}$, notée $\lambda \cdot P$, est le polynôme $\sum_{k=0}^p \lambda a_k X^k$.

C'est le polynôme dont le coefficient en X^k est :

$$\text{coeff}_{X^k}(\lambda \cdot P) = \lambda \text{coeff}_{X^k}(P)$$

- En prenant n supérieur à p et q (par exemple, en prenant $n = \max(p, q)$), les deux polynômes s'écrivent :

$$P = \sum_{k=0}^n a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^n b_k X^k$$

La somme $P + Q$ est le polynôme $\sum_{k=0}^n (a_k + b_k) X^k$.

C'est le polynôme dont le coefficient en X^k est :

$$\text{coeff}_{X^k}(P + Q) = \text{coeff}_{X^k}(P) + \text{coeff}_{X^k}(Q)$$

- Le produit $P \times Q$ est le polynôme $\sum_{k=0}^{p+q} c_k X^k$ où $c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{j=0}^k a_{k-j} b_j = \sum_{i+j=k} a_i b_j$

C'est le polynôme dont le coefficient en X^k est :

$$\text{coeff}_{X^k}(PQ) = \sum_{i+j=k} \text{coeff}_{X^i}(P) \text{coeff}_{X^j}(Q)$$

- **Structure.** Muni des lois $+$ et $\cdot$, l'ensemble $\mathbb{K}[X]$ est un $\mathbb{K}$ -espace vectoriel.
- **Liberté.** Pour tout $n \in \mathbb{N}$, la famille $(X^0, X^1, \dots, X^n)$ est une famille libre.
- **Produit de monômes.** La loi $\times$ est faite pour que $X^p \times X^q = X^{p+q}$. La vie est belle, n'est-ce pas?!
- **Règles de calcul.**

— L'addition des polynômes est commutative et associative :

$$\forall P, Q \in \mathbb{K}[X], \quad P + Q = Q + P \quad \text{et} \quad \forall P, Q, R \in \mathbb{K}[X], \quad (P + Q) + R = P + (Q + R)$$

— La multiplication des polynômes est commutative et associative :

$$\forall P, Q \in \mathbb{K}[X], \quad PQ = QP \quad \text{et} \quad \forall P, Q, R \in \mathbb{K}[X], \quad (PQ)R = P(QR)$$

— La multiplication est distributive sur l'addition :

$$\forall P, Q, R \in \mathbb{K}[X], \quad P(Q + R) = PQ + PR$$

- **Newton et Bernoulli.**

Ces propriétés impliquent que l'on peut calculer avec des polynômes comme usuellement. On a

$$\forall m \in \mathbb{N}, \quad \forall P, Q \in \mathbb{K}[X], \quad (P + Q)^m = \sum_{k=0}^m \binom{m}{k} P^k Q^{m-k} \quad \text{et} \quad P^m - Q^m = (P - Q) \sum_{k=0}^{m-1} P^k Q^{m-1-k}$$



• **Un polynôme particulier.**

Soit $n \in \mathbb{N}$. Le polynôme $(X+1)^n$ intervient très souvent en maths. C'est $(X+1)^n = \sum_{k=0}^n \binom{n}{k} X^k$:

$$(X+1)^n = X^n + nX^{n-1} + \frac{n(n-1)}{2}X^{n-2} + \binom{n}{3}X^{n-3} + \dots + \binom{n}{3}X^3 + \frac{n(n-1)}{2}X^2 + nX + 1$$

Pour tout $k \in \llbracket 0, n \rrbracket$, le coefficient en X^k du polynôme $(X+1)^n$ est $\binom{n}{k}$;
c'est même valable pour tout $k \in \mathbb{N}$ (WHY?).

6 Quiz. Soit $n \in \mathbb{N}^*$. Donner rapidement le coefficient en X^n des polynômes suivants (même question avec le coefficient en X^0 , qui s'appelle le coefficient constant ; puis avec X^k où $k \in \mathbb{N}$) :

$$P_1 = (X+1)^n + (X-1)^n, \quad P_2 = (X+1)^n - (X-1)^n,$$

$$P_3 = (X+1)^n + (1-X)^n, \quad P_4 = (X+1)^n - (1-X)^n.$$

Loi de composition

7

Définition. Soit $P, Q \in \mathbb{K}[X]$ deux polynômes. On écrit $P = \sum_{k=0}^n a_k X^k$.

Le polynôme composé $P \circ Q$ est défini par $P \circ Q = \sum_{k=0}^n a_k Q^k$.

• **Composition avec le polynôme $Q = -X$.**

Soit P un polynôme. On croiera souvent l'objet $P(-X)$.

C'est un polynôme ! Plus précisément, c'est le polynôme composé $P \circ Q$ avec $Q = -X$.

Et l'on a, sans surprise :

$$\text{si } P = \sum_{k=0}^n a_k X^k \text{ alors } P(-X) = \sum_{k=0}^n (-1)^k a_k X^k.$$

• **Composition avec le polynôme $Q = X$.**

On a évidemment $P \circ X = P$.

On a aussi $X \circ P = P$.

• **Attention.** En général, $P \circ Q \neq Q \circ P$.

Prenons $P = aX + b$ et $Q = X^2$. On a

$$P \circ Q = P(X^2) = aX^2 + b \quad \text{et} \quad Q \circ P = Q(aX + b) = (aX + b)^2 = a^2 X^2 + 2abX + b^2$$

Il est alors facile de construire un contre-exemple, par exemple prendre

• **Attention.** En général, $P \circ (Q + R) \neq P \circ Q + P \circ R$.

Prenons $P = X^2$. On a alors

$$P \circ (Q + R) = (Q + R)^2 \quad \text{et} \quad P \circ Q + P \circ R = Q^2 + R^2$$

Il est alors facile de construire un contre-exemple, par exemple prendre

• **Propriétés.** La composition est associative :

$$\forall P, Q, R \in \mathbb{K}[X], \quad (P \circ Q) \circ R = P \circ (Q \circ R)$$

La composition est distributive à droite sur l'addition et la multiplication :

$$\forall P, Q, R \in \mathbb{K}[X], \quad (P + Q) \circ R = P \circ R + Q \circ R$$

$$\forall P, Q, R \in \mathbb{K}[X], \quad (P \times Q) \circ R = (P \circ R) \times (Q \circ R)$$

Question. À votre avis, que représente $(PQ)(X^2)$?



Aparté sur la parité

On définit l'ensemble des polynômes pairs comme étant :

$$\mathcal{P} = \{P \in \mathbb{K}[X] \mid P(-X) = P(X)\}$$

et l'ensemble des polynômes impairs :

$$\mathcal{I} = \{P \in \mathbb{K}[X] \mid P(-X) = -P(X)\}$$

8

Proposition.

Tout polynôme s'écrit de manière unique comme la somme d'un polynôme pair et d'un polynôme impair.

9

Proposition (caractérisation de la parité).

— Soit $P \in \mathbb{K}[X]$ que l'on écrit sous la forme $\sum_{k=0}^n a_k X^k$.

On a l'équivalence

$$P \text{ pair} \iff \forall k \text{ impair}, a_k = 0$$

— Résultat analogue pour P impair.

— On a les égalités :

$$\mathcal{P} = \{P \in \mathbb{K}[X] \mid \exists Q \in \mathbb{K}[X], P = Q(X^2)\}$$

et

$$\mathcal{I} = \{P \in \mathbb{K}[X] \mid \exists Q \in \mathbb{K}[X], P = XQ(X^2)\}$$

10

Question. Les polynômes de Tchebychev.

On considère la suite $(T_n)_{n \in \mathbb{N}}$ de polynômes de $\mathbb{R}[X]$ définie par

$$\begin{cases} T_0 = 1 \\ T_1 = X \\ \forall n \in \mathbb{N}, T_{n+2} = 2XT_{n+1} - T_n \end{cases}$$

Calculer T_2 et T_3 .

Émettre une conjecture sur la parité de T_n . La prouver.



II. Degré d'un polynôme et $\mathbb{K}_n[X]$

11

Définition.

- Soit $P \in \mathbb{K}[X]$ un polynôme **non nul** que l'on écrit $\sum_{k=0}^n a_k X^k$.

— L'entier suivant est bien défini

$$d = \max \{k \in \llbracket 0, n \rrbracket \mid a_k \neq 0\}$$

C'est le degré de P , noté $\deg P$.

- Le coefficient a_d est appelé le coefficient dominant de P ;
le monôme $a_d X^d$ est le *monôme dominant* de P .
- On dit que P est **unitaire** lorsque son coefficient dominant vaut 1.

- Par convention, le degré du polynôme nul est $-\infty$ (le polynôme nul n'a ni monôme dominant, ni coefficient dominant).

- **À retenir.** Le degré de P vaut $\begin{cases} -\infty & \text{si } P \text{ est le polynôme nul} \\ \text{un entier } \mathbb{N} & \text{sinon} \end{cases}$

- **Pour calculer avec des degrés** (à utiliser avec modération).

Rappelons les conventions usuelles de calcul dans $\mathbb{N} \cup \{-\infty\}$:

$$(-\infty) + (-\infty) = -\infty \quad \text{et} \quad \forall n \in \mathbb{N}, n + (-\infty) = -\infty \quad \text{et} \quad \forall n \in \mathbb{N}, -\infty \leq n$$

12

Proposition (opérations algébriques et degré). Soit $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$.

Multiplication par un scalaire. On a $\deg(\lambda \cdot P) = \begin{cases} \deg P & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0 \end{cases}$

Somme.

- On a $\deg(P + Q) \leq \max(\deg P, \deg Q)$.
- De plus, $\deg P \neq \deg Q \implies \deg(P + Q) = \max(\deg P, \deg Q)$.

La réciproque est fausse.

Combinaison linéaire. On a $\deg(\lambda P + \mu Q) \leq \max(\deg P, \deg Q)$.

Produit. On a $\deg(PQ) = \deg P + \deg Q$.

Composition. Si Q est non constant ($\deg Q \geq 1$), on a $\deg(P \circ Q) = \deg P \times \deg Q$.

- **Des exemples et contre-exemples.**

- Que vaut le degré de $P(X^3)$?
- Les polynômes $P = -X^4 + X^3 + X$ et $Q = X^4 - X^3 + 1$ ont pour somme $P + Q = X + 1$.
On a :

$$\deg(P + Q) = 1 < \max(\deg P, \deg Q) = 4$$

- Prenons $P = X^3 + 1$ et $Q = X^4 - X^3 + 1$. Le polynôme $P + Q = X^4 + 2$ est de degré 4.
Comme $\deg P \neq \deg Q$, on vérifie bien la formule :

$$\deg(P + Q) = 4 = \max(\deg P, \deg Q)$$

- Les polynômes $P = 2X^4 - X^3 + X + 1$ et $Q = X^4 + X^3 + 1$ ont pour somme $P + Q = 3X^4 + X + 2$.
Bien que les polynômes aient le même degré, on a **ici** :

$$\deg(P + Q) = 4 = \max(\deg P, \deg Q)$$



Le sous-espace vectoriel $\mathbb{K}_n[X]$

13

The définition ! Soit $n \in \mathbb{N}$.

On définit $\mathbb{K}_n[X]$ comme étant l'ensemble des polynômes de degré **au plus** n .

14

Proposition. Soit $n \in \mathbb{N}$.

L'ensemble $\mathbb{K}_n[X]$ est un $\mathbb{K}$ -espace vectoriel.

C'est le sous-espace vectoriel de $\mathbb{K}[X]$ engendré par la famille $(X^0, X^1, \dots, X^n)$.

Mieux, la famille $(X^0, X^1, \dots, X^n)$ est une base de $\mathbb{K}_n[X]$; c'est la-base-canonique de $\mathbb{K}_n[X]$.

- **À retenir.** Le polynôme nul est dans $\mathbb{K}_n[X]$, et $\mathbb{K}_n[X]$ est stable par combinaison linéaire.
- **Remarque.** L'ensemble $\mathbb{K}_n[X]$ n'est pas stable pour le produit (sauf pour $n = 0$).
- **Cas particulier** $n = 0$. $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants : il contient le polynôme nul et les constantes non nulles.

15
sol → 26

Question. Soit $F = \{P \in \mathbb{K}_3[X] \mid P(1 - X) = P(X)\}$.

Montrer que F est le noyau d'un certain endomorphisme.

Et déterminer une base de F .

16

Question. Les polynômes de Tchebychev.

On considère la suite $(T_n)_{n \in \mathbb{N}}$ de polynômes de $\mathbb{R}[X]$ définie par
$$\begin{cases} T_0 = 1 \\ T_1 = X \\ \forall n \in \mathbb{N}, T_{n+2} = 2XT_{n+1} - T_n \end{cases}$$

Pour tout $n \in \mathbb{N}$, conjecturer le degré et le coefficient dominant de T_n .

Une telle conjecture peut être prouvée par récurrence sur n . Énoncer clairement une assertion $\mathcal{H}_n$.

17 Vrai ou Faux?

(i) Soit $a, b, c \in \mathbb{K}$. A-t-on

$$a(X-2)^8 + b(X-3)^9 + c(X-4)^7 = 0_{\mathbb{K}[X]} \implies \begin{cases} a = 0 \\ b = 0 \\ c = 0 \end{cases}$$

(ii) Soit $a, b, c \in \mathbb{K}$. A-t-on

$$a(X-2) + b(X-3) + c(X-4) = 0_{\mathbb{K}[X]} \implies \begin{cases} a = 0 \\ b = 0 \\ c = 0 \end{cases}$$

(iii) Soit $a, b \in \mathbb{K}$. A-t-on

$$a(X-2) + b(X-3) = 0_{\mathbb{K}[X]} \implies \begin{cases} a = 0 \\ b = 0 \end{cases}$$

18
preuve

Proposition. Pour $P_1, \dots, P_s \in \mathbb{K}[X]$, on a

$$\begin{cases} P_1, \dots, P_s \text{ NON NULS} \\ \deg(P_1) < \dots < \deg(P_s) \end{cases} \implies \text{la famille } (P_1, \dots, P_s) \text{ est libre}$$

« Une famille de polynômes non nuls échelonnée en degré est libre ».

- Certains ouvrages omettent le « non nuls » en prenant comme définition d'une famille échelonnée en degré, une famille $(P_1, \dots, P_s)$ telle que $0 \leq \deg(P_1) < \dots < \deg(P_s)$, ce qui assure qu'aucun des P_i n'est nul.

19
sol → 27

Question. On définit les trois polynômes suivants :

$$L_1 = (X-2)(X-3), \quad L_2 = (X-1)(X-3), \quad L_3 = (X-1)(X-2)$$

Montrer que la famille (L_1, L_2, L_3) est une famille libre de $\mathbb{R}[X]$.

Produit de polynômes

20
preuve

Proposition (intégrité de $\mathbb{K}[X]$). Soit $P, Q \in \mathbb{K}[X]$. On a l'équivalence

$$PQ = 0_{\mathbb{K}[X]} \iff P = 0_{\mathbb{K}[X]} \text{ ou } Q = 0_{\mathbb{K}[X]}$$

« Un produit de polynômes est nul si et seulement si l'un des polynômes est nul. »

21

Proposition (simplification par un polynôme non nul). Soit $P, Q, A \in \mathbb{K}[X]$.

On a

$$\begin{cases} AP = AQ \\ A \neq 0_{\mathbb{K}[X]} \end{cases} \implies P = Q$$



III. Évaluation d'un polynôme en...

- **Avertissement.** Quand on voit un « grand X » dans ce chapitre, il s'agit d'une indéterminée, d'un élément abstrait, formel. Ce grand X n'est pas un « nombre ».

Il n'y aura donc jamais de quantificateur $\forall$ devant ce X .

Bien que X ne désigne pas un nombre, on peut le « remplacer » par un nombre $z \in \mathbb{K}$.

22

Définition. Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ et $z \in \mathbb{K}$.

On définit l'évaluation de P en z comme étant le scalaire $P(z) = \sum_{k=0}^n a_k z^k$.

- **À retenir.** Pour $z = 0$, on a $P(0) = a_0$. Ainsi « L'évaluation en 0 d'un polynôme fournit son coefficient constant ».

23

Proposition (évaluation en un scalaire). Soit $P, Q \in \mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$.

Pour tout scalaire $z \in \mathbb{K}$, on a :

$$(\lambda \cdot P)(z) = \lambda P(z) \quad (P + Q)(z) = P(z) + Q(z) \quad (PQ)(z) = P(z)Q(z)$$

- **Reformulation.** L'application $\text{éval}_z : \mathbb{K}[X] \rightarrow \mathbb{K}$ est une forme linéaire.

$$P \mapsto P(z)$$

Bonus : éval_z est une forme linéaire *non nulle*.

24

sol → 27

Question. On considère $H = \{P \in \mathbb{K}[X] \mid P(3) = 0\}$ et $D = \mathbb{K}_0[X]$.

Montrer que $\mathbb{K}[X] = H \oplus D$.

25

sol → 28

Question. On définit les trois polynômes suivants :

$$L_1 = (X - 2)(X - 3), \quad L_2 = (X - 1)(X - 3), \quad L_3 = (X - 1)(X - 2)$$

Montrer que la famille (L_1, L_2, L_3) est une famille libre de $\mathbb{R}_2[X]$.

26

Proposition (évaluation en une matrice carrée/un endomorphisme). Soit $P, Q \in \mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$.
 Pour toute matrice $M \in \mathcal{M}_n(\mathbb{K})$ carrée, on a :

$$(\lambda \cdot P)(M) = \lambda P(M) \quad (P + Q)(M) = P(M) + Q(M) \quad (PQ)(M) = P(M)Q(M)$$

Pour tout endomorphisme $f \in \mathcal{L}(E)$, on a :

$$(\lambda \cdot P)(f) = \lambda P(f) \quad (P + Q)(f) = P(f) + Q(f) \quad (PQ)(f) = P(f) \circ Q(f)$$

- **Reformulation.** Les deux premiers points se reformulent en disant que les applications

$$\begin{array}{ccc} \text{éval}_M : \mathbb{K}[X] & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ P & \longmapsto & P(M) \end{array} \quad \text{et} \quad \begin{array}{ccc} \text{éval}_f : \mathbb{K}[X] & \longrightarrow & \mathcal{L}(E) \\ P & \longmapsto & P(f) \end{array}$$

sont des applications linéaires.

27

Question. Soit $f \in \mathcal{L}(E)$.

On suppose que

— l'on peut trouver ¹ $\lambda \in \mathbb{K}$ et $x \in E \setminus \{0_E\}$ tel que $f(x) = \lambda x$. En Spé, vous direz que « λ est une valeur propre de f ».

— f vérifie $f^2 - 5f + 6\text{id}_E = 0_{\mathcal{L}(E)}$: le polynôme $P = X^2 - 5X + 6$ est un polynôme annulateur de l'endomorphisme f .

Montrer que $\lambda^2 - 5\lambda + 6 = 0$: le scalaire λ est racine du polynôme P .

1. Ce n'est pas toujours vrai ! Cela signifie qu'il existe une droite vectorielle stable par f .



IV. Divisibilité et division euclidienne

28

Définition. Soit $A, B \in \mathbb{K}[X]$.

On dit que B divise A , et on note $B \mid A$, lorsqu'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.

- **Remarque.** Si $B \neq 0_{\mathbb{K}[X]}$, un tel polynôme Q est nécessairement unique. WHY?
- **Divisibilité sur $\mathbb{K}[X]$ versus ordre naturel $\leq$ sur $\mathbb{N}$.**

La relation de divisibilité sur $\mathbb{K}[X] \setminus \{0\}$ est liée à l'ordre naturel sur $\mathbb{N}$ par la relation :

$$\forall A, B \in \mathbb{K}[X] \setminus \{0\}, \quad B \mid A \implies \deg B \leq \deg A$$

Ce résultat est faux dans $\mathbb{K}[X]$ puisque, par exemple, $X^2 \mid 0$, mais $2 \leq -\infty$.

En revanche, on a (WHY?) $\begin{cases} B \mid A \\ A \neq 0 \end{cases} \implies \deg B \leq \deg A$.

- **Exemple.** Soit $n \in \mathbb{N}$.
Le polynôme $X - 3$ divise $X^n - 3^n$. WHY?
Le polynôme $X^3 - 1$ divise $X^{3n} - 1$. WHY?

29

Proposition. Soit $A, B \in \mathbb{K}[X]$.

Si $A \mid B$ et $B \mid A$, alors il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

30

Proposition (Division euclidienne dans $\mathbb{K}[X]$). Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$.

Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $\begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases}$

- **Outil.** Pour montrer que R est le reste de la division euclidienne de A par B , il est équivalent de montrer que $\deg R < \deg B$ et $B \mid A - R$.
- **Exemple.** Écrire la division euclidienne de $2X^5 - 3X^4 + 3X^3 + 5X + 1$ par $X^2 + 2$.

31

Question. Soit $P \in \mathbb{K}[X]$ et $a, b \in \mathbb{K}$ deux scalaires *distincts*.

Exprimer le reste de la division de P par $(X - a)(X - b)$ en fonction de $P(a)$ et $P(b)$.

32

Question. Soit $f \in \mathcal{L}(E)$ tel que $f^2 - 5f + 6\text{id}_E = 0_{\mathcal{L}(E)}$.

Pour tout $m \in \mathbb{N}$, exprimer f^m comme un polynôme en f de degré ≤ 1 .

On pourra considérer la division euclidienne de X^m par $X^2 - 5X + 6$.



V. Racines et critère de nullité

33

Définition. Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

On dit que α est une racine de P lorsque l'évaluation de P en α est nulle, *id est* lorsque $P(\alpha) = 0$.

• **Exemples.**

- Le scalaire 1 est racine de $P = \sum_{k=0}^{2023} (-1)^k X^k$.
- Les racines de $X^2 + 1$ sont i et $-i$. Les racines de $X^2 + X + 1$ sont j, j^2 .
- Les racines de $X^3 - 1$ sont
- 3, -5 et $\frac{1}{2}$ sont des racines, par exemple, du polynôme

34

Proposition.

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On a l'équivalence α racine de $P \iff X - \alpha$ divise P

35

Question. Démontrer le résultat suivant :

Soit $P \in \mathbb{K}[X]$ et $\alpha, \beta \in \mathbb{K}$ des racines distinctes de P .

Alors $(X - \alpha)(X - \beta)$ divise P .

36

preuve

Proposition (divisibilité et racines). Soit $P \in \mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ des scalaires distincts.

On a l'équivalence

$$\alpha_1, \dots, \alpha_r \text{ racines de } P \iff (X - \alpha_1) \cdots (X - \alpha_r) \text{ divise } P$$

- **Remarque.** Il va sans dire que l'on retrouve ce qui précède. La proposition précédente concerne le cas $r = 1$ et la question concerne le cas $r = 2$.

37

Proposition (racines $n^{\text{èmes}}$ de l'unité).

Soit $n \in \mathbb{N}^*$. On a les deux égalités remarquables suivantes

$$\bullet \quad X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) \quad \text{que l'on peut encore écrire} \quad X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{i \frac{2k\pi}{n}} \right)$$

$$\bullet \quad X^{n-1} + X^{n-2} + \cdots + X + 1 = \prod_{\omega \in \mathbb{U}_n \setminus \{1\}} (X - \omega)$$

- **Avertissement.** Ce résultat est fondamental. C'est peut-être la seule chose à retenir du chapitre sur les nombres complexes.

Il faut savoir retrouver les arguments de la preuve, surtout pour la deuxième égalité.



38

Théorème (critère de nullité). ♡i) Soit $n \in \mathbb{N}$.Si $P \in \mathbb{K}_n[X]$ admet $n + 1$ racines *distinctes*, alors $P = 0$.Un polynôme de degré au plus n ayant $n + 1$ racines distinctes est nul.ii) Un polynôme *non nul* ne peut pas avoir plus de racines que son degré.

iii) Le seul polynôme ayant une infinité de racines est le polynôme nul.

• **Encore une reformulation.**Si un polynôme admet strictement plus de racines que son degré (pris dans $\mathbb{N} \cup \{-\infty\}$), alors il est nul.• **Question rapide!** La fonction sinus est-elle une fonction polynomiale?

39

Corollaire du critère de nullité.— Deux polynômes de $\mathbb{K}_n[X]$ qui coïncident en $n + 1$ points distincts sont égaux.— Deux polynômes qui coïncident sur une partie infinie de $\mathbb{K}$ sont égaux.• **Retour au lycée!**Soit $n \in \mathbb{N}$. Soit $a_0, \dots, a_n \in \mathbb{R}$ et $b_0, \dots, b_n \in \mathbb{R}$.

Si on a

$$\forall t \in \mathbb{R}, \quad a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0 = b_n t^n + b_{n-1} t^{n-1} + \dots + b_1 t + b_0$$

alors

$$\begin{cases} a_n &= b_n \\ a_{n-1} &= b_{n-1} \\ &\vdots \\ a_0 &= b_0 \end{cases}$$

En effet, en posant $P = \sum_{k=0}^n a_k X^k$ et $Q = \sum_{k=0}^n b_k X^k$, l'hypothèse s'écrit $\forall t \in \mathbb{R}, P(t) = Q(t)$

Ce qui implique ...

40

Petit quizz!i) Trouver deux polynômes *différents* P et Q tels que $\forall t \in \{\pi, \sqrt{2}\}, P(t) = Q(t)$ ii) Trouver un polynôme P , différent de X^2 , vérifiant

$$P(2) = 4 \quad \text{et} \quad P(3) = 9 \quad \text{et} \quad P(4) = 16$$

iii) Soit $P \in \mathbb{K}_2[X]$ vérifiant

$$P(2) = 4 \quad \text{et} \quad P(3) = 9 \quad \text{et} \quad P(4) = 16$$

Que peut-on dire de P ? Preuve?

41

Question. Prouver l'énoncé suivant :

On a l'égalité d'ensembles :

$$\{P \in \mathbb{K}[X] \mid P(X) = P(X+1)\} = \mathbb{K}_0[X]$$

En français : « un polynôme 1-périodique est constant, et réciproquement ».



VI. Multiplicité d'une racine

Définition et amélioration du critère de nullité

Question avant de commencer.

- Donner un polynôme de $\mathbb{R}[X]$ de degré 4 qui admet exactement 3 racines réelles, disons 7, 8, 9.
- Donner un polynôme de $\mathbb{R}[X]$ de degré 4 qui admet exactement 2 racines réelles, disons 7 et 8.
- Donner un polynôme de $\mathbb{R}[X]$ de degré 4 qui admet exactement 2 racines réelles, chacune de multiplicité 1.

42

Définition (ordre de multiplicité d'une racine).

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, $m \in \mathbb{N}^*$.

— On dit que α est racine-de-multiplicité-**au moins**- m du polynôme P lorsque

$$(X - \alpha)^m \text{ divise } P \quad \text{c'est-à-dire lorsque} \quad P \text{ s'écrit } (X - \alpha)^m Q$$

— On dit que α est racine-de-multiplicité-**exactement**- m du polynôme P lorsque

$$\left\{ \begin{array}{l} (X - \alpha)^m \text{ divise } P \\ (X - \alpha)^{m+1} \text{ ne divise pas } P \end{array} \right. \quad \text{c'est-à-dire lorsque} \quad \left\{ \begin{array}{l} P \text{ s'écrit } (X - \alpha)^m Q \\ \text{avec } Q(\alpha) \neq 0 \end{array} \right.$$

Remarque.

Dans la définition, on a fixé P , α et m et on a défini la locution « α est racine de multiplicité m de P ».

On a donc défini la locution « être racine de multiplicité m » (qui nécessite de fixer m), mais on n'a **pas** défini la notion de « multiplicité ».

Question que l'on peut alors se poser : peut-on définir « la multiplicité de α en tant que racine de P » ?

Autre définition à connaître.

Soit $P \in \mathbb{K}[X]$ non nul, et $\alpha \in \mathbb{K}$ une racine de P .

La multiplicité (ou l'ordre de multiplicité) de α en tant que racine de P est

$$\mu = \max \left\{ k \in \mathbb{N}^* \text{ tel que } (X - \alpha)^k \mid P \right\}$$

Encore plus général. jeu des 7 différences.

Soit $P \in \mathbb{K}[X]$ non nul et $\alpha \in \mathbb{K}$.

La multiplicité (ou l'ordre de multiplicité) de α en tant que racine de P est

$$\mu = \max \left\{ k \in \mathbb{N} \text{ tel que } (X - \alpha)^k \mid P \right\}$$

- **Exemple.** Soit $P = X^4 + 3X^3 - 3X^2 - 7X + 6$. On a (WHY?) $P = (X - 1)^2(X^2 + 5X + 6)$.

Ainsi, 1 est racine de multiplicité *au moins* 2. Pourquoi 1 est racine de multiplicité exactement 2 ?

Décompte des racines.

Lorsque l'on dénombre les racines d'un polynôme non nul, on peut :

- ou bien parler du nombre de racines distinctes
- ou bien parler du nombre de racines-comptées-avec-multiplicité.

Par exemple, le polynôme $(X - 9)(X - 8)^2(X - 7)^3$ possède

- trois racines distinctes : 9, 8, 7
- six racines-comptées-avec-multiplicité : 9, 8, 8, 7, 7, 7.



43

Proposition.

Soit $P \in \mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ des scalaires **distincts** et $m_1, \dots, m_r \in \mathbb{N}$.

On a l'équivalence :

$$\left\{ \begin{array}{l} \alpha_1 \text{ racine de multiplicité au moins } m_1 \text{ de } P \\ \vdots \\ \alpha_r \text{ racine de multiplicité au moins } m_r \text{ de } P \end{array} \right. \iff (X - \alpha_1)^{m_1} \dots (X - \alpha_r)^{m_r} \text{ divise } P$$

44

Proposition (amélioration du critère de nullité).

i) Soit $n \in \mathbb{N}$.

Si $P \in \mathbb{K}_n[X]$ admet $n + 1$ racines-comptées-avec-multiplicité, alors $P = 0$.

ii) Un polynôme *non nul* ne peut pas avoir plus de racines-comptées-avec-multiplicité que son degré.

45

Proposition.

Soit $P \in \mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ des scalaires distincts et $m_1, \dots, m_r \in \mathbb{N}$.

On a :

$$\left\{ \begin{array}{l} \forall i \in \llbracket 1, r \rrbracket, \alpha_i \text{ racine de multiplicité au moins } m_i \text{ de } P \\ \deg P = m_1 + \dots + m_r \end{array} \right. \implies \exists \lambda \in \mathbb{K}, P = \lambda (X - \alpha_1)^{m_1} \dots (X - \alpha_r)^{m_r}$$

- **Remarque.** Que dit cet énoncé pour le polynôme nul?

Pour la preuve, mieux vaut enlever le polynôme nul de la circulation!



Relation coefficients-racines pour un polynôme scindé

46

Définition (polynôme scindé).

Soit $P \in \mathbb{K}[X]$ un polynôme non nul.

On dit que P est scindé sur $\mathbb{K}$ lorsqu'il existe $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}$, $\beta_1, \dots, \beta_n \in \mathbb{K}$ tels que
$$P = \lambda \prod_{i=1}^n (X - \beta_i)$$

- **Remarque.** On peut faire « naviguer » le λ dans un des facteurs (par exemple le premier).

Un polynôme scindé est donc $\begin{cases} \text{un polynôme constant } \textit{non nul} & \text{(c'est-à-dire de degré 0 exactement)} \\ \text{ou bien} \\ \text{un polynôme s'écrivant comme produit de polynômes de degré 1} \end{cases}$

- **Vocabulaire.** Un polynôme de degré $n \in \mathbb{N}$ qui admet n racines distinctes est scindé sur $\mathbb{K}$.
On dit qu'un tel polynôme est *scindé à racines simples*.
- **Mieux.** Un polynôme de degré $n \in \mathbb{N}$ qui admet n racines-comptées-avec-multiplicité dans $\mathbb{K}$ est scindé sur $\mathbb{K}$.
- **Exemple.**

Le polynôme $X^2 + 1$ appartient à $\mathbb{R}[X]$. Est-il scindé sur $\mathbb{R}$?

Le polynôme $X^2 + 1$ appartient à $\mathbb{C}[X]$. Est-il scindé sur $\mathbb{C}$?

Le polynôme $X^3 - 1$ est-il scindé sur $\mathbb{R}$? sur $\mathbb{C}$?

47

Proposition (relation coefficients-racines).

Soit $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ un polynôme de degré n (donc $a_n \neq 0$).

On suppose que P est scindé, c'est-à-dire que P s'écrit

$$P = \lambda (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

On a alors

$$\lambda = a_n \quad \text{et} \quad \sum_{i=1}^n \alpha_i = \frac{-a_{n-1}}{a_n} \quad \text{et} \quad \prod_{i=1}^n \alpha_i = (-1)^n \frac{a_0}{a_n}$$

- **À retenir.** Pour un polynôme scindé **unitaire** de degré n :
— la somme des racines est égal à « l'opposé de son coefficient en X^{n-1} ».
— le produit des racines est égal à « $(-1)^n \times$ son-coefficient-constant ».

- **Le résultat du lycée.**

Soit $P = aX^2 + bX + c$ est un polynôme de degré 2 (donc $a \neq 0$).

Si P est scindé, disons $P = \lambda(X - x_1)(X - x_2)$, alors on a les relations :

$$\lambda = a \quad \text{et} \quad x_1 + x_2 = \frac{-b}{a} \quad \text{et} \quad x_1 x_2 = \frac{c}{a}$$

- **Application.** Soit $n \geq 1$.

Que vaut la somme des racines $n^{\text{ème}}$ de l'unité? Et le produit?



VII. Dérivation chez les polynômes

Polynôme dérivé

48

Définition. Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$. On définit le polynôme dérivé de P , noté P' , comme étant

$$P' = \sum_{k=1}^n k a_k X^{k-1}$$

- **Vocabulaire.** Dans ce cours, on n'écrira jamais la phrase « P est dérivable ». En effet, il n'y a pas de notion de dérivabilité pour un polynôme formel. En revanche, il y a la notion de polynôme dérivé. On pourra donc dire directement « le polynôme dérivé de P est ... ».
- **Quizz.** Que vaut le polynôme dérivé de $P = \sum_{k=0}^{15} X^{k+1}$?
- **Polynôme dérivé d'un monôme.** Pour tout $d \in \mathbb{N}$, on a par définition :

$$(X^d)' = \begin{cases} dX^{d-1} & \text{si } d \geq 1 \\ 0_{\mathbb{K}[X]} & \text{sinon} \end{cases}$$

49

preuve

Proposition (polynôme dérivé d'une somme, d'un produit). Soit $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$.

Alors

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q' \quad \text{et} \quad (PQ)' = P'Q + PQ'$$

- **Reformulation.** L'égalité de gauche dit que l'application $\mathbb{K}[X] \longrightarrow \mathbb{K}[X]$ est linéaire.
 $P \longmapsto P'$

50

Proposition (degré du polynôme dérivé). Soit $P \in \mathbb{K}[X]$.

Alors

$$\deg P' = \begin{cases} \deg P - 1 & \text{si } \deg P \geq 1 \\ -\infty & \text{sinon} \end{cases}$$

- **Inégalité dans $\mathbb{N} \cup \{-\infty\}$.**
Dans tous les cas, on a $\deg P' \leq \deg P - 1$
- **Une équivalence.** On a (WHY?) $\deg P' = -\infty \iff \deg P \leq 0$



Un peu de « primitivation »

51 Question.

Montrer que tout polynôme P est le polynôme dérivé d'un polynôme Q . (« tout polynôme P est primitivable »)
Plus précisément, soit $P \in \mathbb{K}_n[X]$. Montrer que l'on peut trouver $Q \in \mathbb{K}_{n+1}[X]$ tel que $Q' = P$.

52 Proposition. Soit $P \in \mathbb{K}[X]$.

0) On a

$$P' = 0_{\mathbb{K}[X]} \iff P \in \mathbb{K}_0[X]$$

En français : Si un polynôme admet pour polynôme dérivé le polynôme nul, alors il est constant.

1) On a

$$P' \in \mathbb{K}_0[X] \iff P \in \mathbb{K}_1[X]$$

2) Soit $n \in \mathbb{N}$. On a

$$P' \in \mathbb{K}_n[X] \iff P \in \mathbb{K}_{n+1}[X]$$

Polynômes dérivés successifs

53 Définition (polynômes dérivés successifs). Soit $P \in \mathbb{K}[X]$.

Pour $r \in \mathbb{N}$, on définit le polynôme dérivé d'ordre r , noté $P^{(r)}$, par la formule de récurrence suivante :

$$\begin{cases} P^{(0)} = P \\ \forall r \in \mathbb{N}, P^{(r+1)} = (P^{(r)})' \end{cases}$$

• Linéarité. Soit $r \in \mathbb{N}$.

L'application $\mathbb{K}[X] \rightarrow \mathbb{K}[X]$ est linéaire. On a donc $(\lambda P + \mu Q)^{(r)} = \lambda P^{(r)} + \mu Q^{(r)}$.
 $P \mapsto P^{(r)}$

• Polynômes dérivés successifs d'un monôme. Soit $n \in \mathbb{N}$.

Pour tout $r \in \mathbb{N}$, le polynôme dérivé d'ordre r de X^n est

$$\begin{cases} \frac{n!}{(n-r)!} X^{n-r} & \text{si } r \leq n \\ 0_{\mathbb{K}[X]} & \text{sinon} \end{cases} \quad \text{ou encore} \quad \begin{cases} n(n-1) \cdots (n-r+1) X^{n-r} & \text{si } r \leq n \\ 0_{\mathbb{K}[X]} & \text{sinon} \end{cases}$$

54 Proposition (degré des polynômes dérivés successifs). Soit $P \in \mathbb{K}[X]$.

On a

$$\forall r \in \mathbb{N}, \quad \deg P^{(r)} = \begin{cases} \deg P - r & \text{si } \deg P \geq r \\ -\infty & \text{sinon} \end{cases}$$

• Inégalité dans $\mathbb{N} \cup \{-\infty\}$.

Dans tous les cas, on a $\deg P^{(r)} \leq \deg P - r$.

• Une équivalence.

On a (WHY?) $\deg P^{(r)} = -\infty \iff \deg P \leq r-1$ ou encore $P^{(r)} = 0_{\mathbb{K}[X]} \iff P \in \mathbb{K}_{r-1}[X]$.



Deux belles formules!

55

Proposition (formule de Leibniz).

Soit $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

On a

$$(PQ)^{(1)} = \dots\dots\dots$$

On a

$$(PQ)^{(2)} = \dots\dots\dots$$

On a

$$(PQ)^{(n)} = \dots\dots\dots$$

56

preuve

Proposition (base de Taylor en α).

Soit $n \in \mathbb{N}$ et $\alpha \in \mathbb{K}$.

La famille $((X - \alpha)^k)_{k \in \llbracket 0, n \rrbracket}$ est une base de $\mathbb{K}_n[X]$.

- D'après le caractère générateur de la base de Taylor, on en déduit que tout polynôme de $\mathbb{K}_n[X]$ s'écrit de manière unique comme combinaison linéaire des polynômes : $(X - \alpha)^0, (X - \alpha)^1, (X - \alpha)^2, \dots, (X - \alpha)^n$.
Mais au fait, quelles sont les coordonnées de P sur cette base?

57

Proposition (formule de Taylor).

Soit $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $\alpha \in \mathbb{K}$.

On a

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

.....

- **À retenir.** Il est bon d'apprendre la formule de Taylor sous la forme :

$$\text{Tout polynôme } P \text{ de } \mathbb{K}_n[X] \text{ s'écrit } \sum_{k=0}^n \lambda_k (X - \alpha)^k \text{ avec } \lambda_k = \frac{P^{(k)}(\alpha)}{k!}.$$

58

Question.

Soit $P \in \mathbb{K}_n[X]$. Soit $m \in \llbracket 0, n \rrbracket$.

À l'aide de la formule de Taylor, écrire la division euclidienne de P par $(X - \alpha)^m$.



Retour sur la multiplicité : critère différentiel

59

Proposition (caractérisation de la multiplicité avec les polynômes dérivés successifs).

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, $m \in \mathbb{N}$.

— Le scalaire α est racine de multiplicité au moins m si et seulement si

$$\forall k \in \llbracket 0, m-1 \rrbracket, \quad P^{(k)}(\alpha) = 0$$

Il y a m conditions d'annulation $P(\alpha) = 0$, $P'(\alpha) = 0$, ..., $P^{(m-1)}(\alpha) = 0$.

— Le scalaire α est racine de multiplicité exactement m si et seulement si

$$\begin{cases} \forall k \in \llbracket 0, m-1 \rrbracket, & P^{(k)}(\alpha) = 0 \\ P^{(m)}(\alpha) \neq 0 \end{cases}$$

Il y a m conditions d'annulation, et 1 condition de non-annulation.

• **Exemple.** Soit $P = X^4 + 2X^2 - 8X + 5$. Alors 1 est racine de P (WHY?) et son ordre de multiplicité est ...

• **Remarque importante pour la preuve.**

Soit $P \in \mathbb{K}[X]$, alors il existe $n \in \mathbb{N}$ tel que $P \in \mathbb{K}_n[X]$ (prendre pour n un majorant de son degré).

Soit $m \in \llbracket 0, n \rrbracket$.

Alors on peut écrire la formule de Taylor :

$$P = (X - \alpha)^m \times \sum_{k=m}^n \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^{k-m} + \sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$$

C'est la division euclidienne de P par $(X - \alpha)^m$.

On a

$$P = (X - \alpha)^m Q + R, \quad \text{avec } \deg R < m$$

avec

$$Q = \sum_{k=m}^n \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^{k-m} \quad \text{et} \quad R = \sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$$

Racine d'un polynôme à coefficients réels

60

preuve

Proposition. Soit $Q \in \mathbb{R}[X]$ et $\beta \in \mathbb{C}$, $m \in \mathbb{N}$.

$$\beta \text{ racine de } Q \iff \bar{\beta} \text{ racine de } Q$$

• **Remarque.** Cette équivalence est bien sûr vraie si $\beta \in \mathbb{R}$, mais n'est pas passionnante.

Elle souvent utilisée pour $\beta \in \mathbb{C} \setminus \mathbb{R}$.

61

Proposition. Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$, $m \in \mathbb{N}$.

Alors α est racine de P de multiplicité m si et seulement si $\bar{\alpha}$ est racine de P de multiplicité m .



VIII. Factorisation

Polynômes irréductibles

62

Définition.

Un polynôme $P \in \mathbb{K}[X]$ est *irréductible* lorsque $\begin{cases} P \text{ est non constant} \\ \forall A, B \in \mathbb{K}[X], \quad P = AB \implies \deg A = 0 \text{ ou } \deg B = 0 \end{cases}$

- **Analogie.** On remarquera l'analogie avec les nombres premiers.

Un entier $p \in \mathbb{N}$ est premier lorsque $\begin{cases} p \text{ est différent de } 1 \\ \forall a, b \in \mathbb{Z}, \quad p = ab \implies a = \pm 1 \text{ ou } b = \pm 1 \end{cases}$

- **Petits degrés.**

- Le polynôme nul n'est pas irréductible. WHY?
- Les polynômes de degré 0 ne sont pas irréductibles. WHY?
- Les polynômes de degré 1 sont irréductibles.

Soit P un polynôme de degré 1 (donc il est non constant).

Supposons qu'il existe $A, B \in \mathbb{K}[X]$ tel que $P = AB$.

On a donc $\deg P = \deg A + \deg B$ (c'est a priori une égalité de $\mathbb{N} \cup \{-\infty\}$, WHY?).

D'où $1 = \deg A + \deg B$.

Cette égalité est une égalité de $\mathbb{N}$, d'où $\deg A = 0$ ou $\deg B = 0$.

- Les polynômes de degré 2 : ça dépend! WHY?!
- Les polynômes de degré 3 sont non-irréductibles : c'est « facile » pour $\mathbb{K} = \mathbb{R}$, plus difficile pour $\mathbb{K} = \mathbb{C}$.
- En degré ≥ 4 , ils ne sont pas irréductibles, c'est un théorème.

- **Irréductibilité VERSUS racines.**

Grosso modo, un polynôme irréductible a fortement tendance à ne pas avoir de racines.

- Un polynôme irréductible de $\mathbb{K}[X]$ admettant une racine est de degré 1.

Soit $P \in \mathbb{K}[X]$ irréductible. Si P admet une racine α , alors P s'écrit $(X - \alpha)Q$. Par irréductibilité, on a $\deg Q = 0$. Ainsi $\deg P = 1$.

- Les polynômes irréductibles de degré ≥ 2 n'ont pas de racine.

La réciproque est fausse. Par exemple, dans $\mathbb{R}[X]$, le polynôme $X^4 + X^2 + 1$ n'a pas de racine dans $\mathbb{R}$ et pourtant il n'est pas irréductible puisque :

$$X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1)$$

63

preuve

Proposition (Décomposition en Facteurs Irréductibles = DFI).

Tout polynôme non constant s'écrit comme produit de polynômes irréductibles.

- **Quid des polynômes constants?**

Est-ce qu'un polynôme constant est produit de polynômes irréductibles?

Avec la convention classique sur le produit vide, on en déduit :

Tout polynôme non nul s'écrit, à $\mathbb{K}^$ près, comme produit de polynômes irréductibles.*

- **Analogie.** En arithmétique :

Tout entier de $\mathbb{Z}$ non nul s'écrit, à ± 1 près, comme produit de nombres premiers.

- **Important.** Quitte à mettre en facteur le coefficient dominant du polynôme considéré, les polynômes irréductibles intervenant dans le produit peuvent être pris unitaires. Ainsi :

Tout polynôme non nul s'écrit, à $\mathbb{K}^$ près, comme produit de polynômes irréductibles unitaires.*

- **Remarque.** Ce résultat ne dit encore rien sur la non-irréductibilité d'un polynôme de degré ≥ 3 .



Théorème de d'Alembert-Gauss

On **admet** le théorème fondamental suivant dû à Jean le Rond d'Alembert (1717-1783) et Gauss (1777-1855).

64

Théorème de d'Alembert-Gauss.

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.

- **Attention.** C'est faux si l'on remplace tous les $\mathbb{C}$ par des $\mathbb{R}$.

Penser à $X^2 + 1$ qui n'admet pas de racine dans $\mathbb{R}$.

En revanche, $X^2 + 1$, vu comme polynôme de $\mathbb{C}[X]$, admet bien au moins une (en fait 2) racine dans $\mathbb{C}$.

65

preuve

Proposition (les irréductibles de $\mathbb{K}[X]$).

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant < 0 .

- **Remarque.**

D'après la DFI, on sait que « tout polynôme non constant est produit de polynômes irréductibles ».

Ainsi, on peut déjà dire (cela sera précisé à la page suivante) que :

- Tout polynôme non constant de $\mathbb{C}[X]$ s'écrit comme produit de polynômes de degré 1.
ou encore

Tout polynôme non nul de $\mathbb{C}[X]$ s'écrit, à $\mathbb{C}^*$ près, comme produit de polynômes de degré 1.

- Tout polynôme non constant de $\mathbb{R}[X]$ s'écrit comme produit de polynômes de degré 1 ou 2 (et si vous voulez être précis, ajoutez la condition sur le discriminant).
ou encore

Tout polynôme non nul de $\mathbb{R}[X]$ s'écrit, à $\mathbb{R}^*$ près, comme produit de polynômes de degré 1 ou 2 (et si vous voulez être précis, ajoutez la condition sur le discriminant).

66

preuve

Proposition.

Tout polynôme non nul de $\mathbb{C}[X]$ est scindé (c'est-à-dire constant, ou produit de polynômes de degré 1).

- **Attention.** Ce résultat est faux sur $\mathbb{R}[X]$.

Par exemple, le polynôme $P = X^2 + 1$ n'est pas scindé sur $\mathbb{R}$.

Cependant, il est scindé sur $\mathbb{C}$ puisque $P = (X - i)(X + i)$.



67

Proposition (dans $\mathbb{C}[X]$).

— **En français.**

Tout polynôme non nul de $\mathbb{C}[X]$ s'écrit, à $\mathbb{C}^*$ près, comme produit de polynômes de degré 1.

— **En maths.**

Soit $P \in \mathbb{C}[X]$ non nul. Alors P s'écrit sous la forme

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

où $\lambda \in \mathbb{C}^*$ est le coefficient dominant de P ,

les α_i sont les racines complexes distinctes de P de multiplicité $m_i \in \mathbb{N}^*$.

68

Proposition (dans $\mathbb{R}[X]$).

— **En français.**

Tout polynôme non nul de $\mathbb{R}[X]$ s'écrit, à $\mathbb{R}^*$ près, comme produit de polynômes

de degré 1 ou bien de degré 2 à discriminant strictement négatif

— **En maths.**

Soit $P \in \mathbb{R}[X]$ non nul. Alors P s'écrit sous la forme

$$P = \lambda \prod_{i=1}^p (X - x_i)^{m_i} \times \prod_{i=1}^q (X^2 + b_i X + c_i)^{\mu_i} \quad \text{avec } b_i^2 - 4c_i < 0$$

où $\lambda \in \mathbb{R}^*$ est le coefficient dominant de P ,

les x_i sont les racines réelles distinctes de P de multiplicité $m_i \in \mathbb{N}^*$

les couples (b_i, c_i) sont distincts avec $b_i^2 - 4c_i < 0$ et les μ_i sont dans $\mathbb{N}^*$.

69

Exemples

- À l'œil nu, factoriser dans $\mathbb{R}[X]$ les polynômes suivants :

$$P_1 = 8X - 9 \quad T_2 = 2X^2 - 1 \quad T_3 = 4X^3 - 3X \quad P_4 = X^2 + X + 1 \quad P_5 = X^3 + 1$$

- Factoriser dans $\mathbb{R}[X]$ les polynômes

$$P = X^7 - X^6 - X^4 + X^3 \quad P = X^4 - 1 \quad P = X^4 + 1$$

70

preuve

Proposition.

Soit A et B deux polynômes non nuls de $\mathbb{C}[X]$.

Alors B divise A si, et seulement si, toute racine de B est racine de A , avec une multiplicité en tant que racine de A au moins égale à sa multiplicité en tant que racine de B .

En maths :

$$B \mid A \iff \forall z \in \mathbb{K}, \quad \text{mult}(z, B) \leq \text{mult}(z, A)$$



Polynômes

preuve et éléments de correction

15

- Posons $\varphi: \mathbb{K}_3[X] \longrightarrow \mathbb{K}_3[X]$.
 $P \mapsto P(1-X)$

Montrons que φ est un endomorphisme de $\mathbb{K}_3[X]$.

On a alors $F = \text{Ker}(\varphi - \text{id}_E)$.

- Déterminons pour commencer une famille génératrice de F .

Procédons par analyse-synthèse pour déterminer les « ? » dans $F = \text{Vect}(???)$.

Analyse/inclusion $\square$.

Soit $P \in \mathbb{K}_3[X]$ tel que $P(1-X) = P(X)$.

Le polynôme P s'écrit $aX^3 + bX^2 + cX + d$.

Comme il vérifie l'égalité $P(1-X) = P(X)$, on obtient

$$\underbrace{a(1-X)^3 + b(1-X)^2 + c(1-X) + d}_{-aX^3 + (3a+b)X^2 + (-3a-2b-c)X + (a+b+c+d)} = aX^3 + bX^2 + cX + d$$

Par identification des coefficients, on obtient

$$\begin{cases} -a = a \\ 3a + b = b \\ -3a - 2b - c = c \\ a + b + c + d = d \end{cases}$$

D'où

$$a = 0 \quad \text{et} \quad b + c = 0$$

Ainsi $P = bX^2 + (-b)X + d = b(X^2 - X) + d$.

Bilan de l'analyse : $P \in \text{Vect}(X^2 - X, 1)$.

Synthèse/inclusion $\supset$

Comme F est stable par combinaison linéaire, il suffit de vérifier que les deux polynômes $X^2 - X$ et $1 = X^0$ sont dans F .

On a $(1-X)^2 - (1-X) = \dots = X^2 - X$, donc $X^2 - X \in F$.

On a $(1-X)^0 = 1 = X^0$ donc $X^0 \in F$.

BILAN. On a l'égalité $F = \text{Vect}(X^2 - X, 1)$.

- Montrons que la famille $(X^2 - X, 1)$ est libre.

Soit $\lambda, \mu \in \mathbb{K}$ tel que $\lambda(X^2 - X) + \mu 1 = 0_{\mathbb{K}[X]}$.

Alors $\lambda X^2 - \lambda X + \mu 1 = 0$.

D'où (WHY?), $\lambda = 0$ et $\mu = 0$.

18

Pour alléger les notations, on pose $d_i = \deg P_i$.

Soit $\lambda_1, \dots, \lambda_s \in \mathbb{K}$. On suppose que $\sum_{k=1}^s \lambda_k P_k = 0_{\mathbb{K}[X]}$. On veut montrer que $\lambda_1 = \dots = \lambda_s = 0_{\mathbb{K}}$.

Contemplant l'égalité de polynômes $\lambda_1 P_1 + \lambda_2 P_2 + \dots + \lambda_s P_s = 0_{\mathbb{K}[X]}$ et examinons le coefficient en X^{d_1} de cette égalité. Idem avec $X^{d_2}, \dots, X^{d_s}$. On obtient les s égalités de scalaires suivantes :

$$\begin{cases} \lambda_1 \text{coeff}_{X^{d_1}}(P_1) + \lambda_2 \text{coeff}_{X^{d_1}}(P_2) + \dots + \lambda_s \text{coeff}_{X^{d_1}}(P_s) = 0_{\mathbb{K}} \\ \lambda_1 \text{coeff}_{X^{d_2}}(P_1) + \lambda_2 \text{coeff}_{X^{d_2}}(P_2) + \dots + \lambda_s \text{coeff}_{X^{d_2}}(P_s) = 0_{\mathbb{K}} \\ \vdots \\ \lambda_1 \text{coeff}_{X^{d_s}}(P_1) + \lambda_2 \text{coeff}_{X^{d_s}}(P_2) + \dots + \lambda_s \text{coeff}_{X^{d_s}}(P_s) = 0_{\mathbb{K}} \end{cases}$$



En fait (WHY?), on obtient le système *triangulaire* suivant

$$\left\{ \begin{array}{l} \lambda_1 \text{coeff}_{X^{d_1}}(P_1) + \lambda_2 \text{coeff}_{X^{d_1}}(P_2) + \lambda_3 \text{coeff}_{X^{d_1}}(P_3) + \cdots + \lambda_s \text{coeff}_{X^{d_1}}(P_s) = 0_{\mathbb{K}} \\ \lambda_2 \text{coeff}_{X^{d_2}}(P_2) + \lambda_3 \text{coeff}_{X^{d_2}}(P_3) + \cdots + \lambda_s \text{coeff}_{X^{d_2}}(P_s) = 0_{\mathbb{K}} \\ \lambda_3 \text{coeff}_{X^{d_3}}(P_3) + \cdots + \lambda_s \text{coeff}_{X^{d_3}}(P_s) = 0_{\mathbb{K}} \\ \vdots \\ \lambda_s \text{coeff}_{X^{d_s}}(P_s) = 0_{\mathbb{K}} \end{array} \right.$$

Comme $\text{coeff}_{X^{d_i}}(P_i) \neq 0$ (WHY?), on en déduit en remontant le système que $\lambda_s = 0$, puis $\lambda_{s-1} = 0$, etc. jusqu'à obtenir $\lambda_3 = 0$, $\lambda_2 = 0$, $\lambda_1 = 0$.

19

On va travailler avec les coefficients :

$$L_1 = X^2 - 5X + 6$$

$$L_2 = X^2 - 4X + 3$$

$$L_3 = X^2 - 3X + 2$$

Soit $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ tels que

$$\lambda_1 L_1 + \lambda_2 L_2 + \lambda_3 L_3 = 0_{\mathbb{R}[X]}$$

L'égalité précédente est une égalité de polynômes.

En identifiant les coefficients, on a ...

20

Preuve.

⇐ facile!

⇒ Par contraposée. On suppose $P \neq 0_{\mathbb{K}[X]}$ et $Q \neq 0_{\mathbb{K}[X]}$.

Les deux polynômes possèdent donc un degré **entier**.

Par produit, le polynôme PQ possède donc un degré **entier**.

Donc le polynôme PQ est non nul (sinon son degré serait égal à $-\infty$ et ne serait donc pas un entier).

24

Fixons $P \in E = \mathbb{K}[X]$.

On cherche à montrer que P se décompose de manière unique comme la somme d'un élément de H et d'un élément de D .

Raisonnons par analyse-synthèse.

• Analyse

Supposons qu'il existe $P_H \in H$ et $P_D \in D$ tels que $P \stackrel{\star}{=} P_H + P_D$.

Comme $P_H \in H$, on a $P_H(3) = 0$.

Comme $P_D \in D$, on a $P_D = aX^0 = a$.

En évaluant en 3 l'égalité $\star$, on trouve :

$$P(3) = \underbrace{P_H(3)}_{=0} + \underbrace{P_D(3)}_a$$

On a donc P_D en fonction de P : en effet, $P_D = P(3)$.

On a donc ensuite P_H en fonction de P : en effet, $P_H = P - P_D$, autrement dit $P_H = P - P(3)$.

• Synthèse

On pose $P_D = P(3)$ et $P_H = P - P(3)$.



Il y a 3 points à vérifier

$$\begin{cases} \text{i) } P_H \in H \\ \text{ii) } P_D \in D \\ \text{iii) } P = P_H + P_D \end{cases}$$

i) On doit montrer que $P_H(3) = 0$. Allons-y. On a $P_H(3) = P(3) - P(3) = 0$.

ii) On doit montrer que P_D s'écrit aX^0 , ce qui est le cas avec $a = P(3)$.

iii) On doit montrer que $P = P_H + P_D$. Allons-y. On a $P_H + P_D = (P - P(3)) + P(3) = P$.

Bilan. On a montré que $P \in E$ s'écrit de manière unique comme la somme d'un élément de H et d'un élément de D .

25

Montrons que la famille (L_1, L_2, L_3) est une famille libre de $\mathbb{R}_2[X]$.

Soit $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ tels que

$$\lambda_1 L_1 + \lambda_2 L_2 + \lambda_3 L_3 = 0_{\mathbb{R}[X]}$$

L'égalité précédente est une égalité de polynômes.

Évaluons en 1, puis en 2, puis en 3. On obtient

$$\begin{cases} \lambda_1 L_1(1) + \lambda_2 L_2(1) + \lambda_3 L_3(1) = 0 \\ \lambda_1 L_1(2) + \lambda_2 L_2(2) + \lambda_3 L_3(2) = 0 \\ \lambda_1 L_1(3) + \lambda_2 L_2(3) + \lambda_3 L_3(3) = 0 \end{cases}$$

d'où

$$\begin{cases} \lambda_1 \times 2 + \lambda_2 \times 0 + \lambda_3 \times 0 = 0 \\ \lambda_1 \times 0 + \lambda_2 \times (-1) + \lambda_3 \times 0 = 0 \\ \lambda_1 \times 0 + \lambda_2 \times 0 + \lambda_3 \times 2 = 0 \end{cases}$$

C'est-à-dire matriciellement :

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

La matrice est inversible. D'où $\lambda_1 = 0$, $\lambda_2 = 0$ et $\lambda_3 = 0$.

Donc la famille est libre.

36

Par récurrence finie sur $k \in \llbracket 1, r \rrbracket$.

On pose $\mathcal{H}_k$ la propriété « $(X - \alpha_1) \cdots (X - \alpha_k)$ divise P ».

41

Deux preuves. Une utilisant les racines et le critère radical de nullité.

L'autre utilisant les coefficients, plus précisément le coefficient en X^{n-1} .

49

• Linéarité. Écrire $P = \sum_{k=0}^n a_k X^k$ et $Q = \sum_{k=0}^n b_k X^k$ (avec le même n). Puis se laisser porter!

• Le produit.

Étape 1. Commencer par le cas des monômes. Soit $p, q \in \mathbb{N}$.



Le membre gauche vaut :

$$(X^p X^q)' = (X^{p+q})' = \begin{cases} (p+q)X^{p+q-1} & \text{si } p+q \geq 1 \\ 0_{\mathbb{K}[X]} & \text{si } p+q = 0 \end{cases}$$

Le membre droit vaut :

$$(X^p)' X^q + X^p (X^q)' = \begin{cases} pX^{p-1} & \text{si } p \geq 1 \\ 0_{\mathbb{K}[X]} & \text{si } p = 0 \end{cases} \times X^q + X^p \times \begin{cases} qX^{q-1} & \text{si } q \geq 1 \\ 0_{\mathbb{K}[X]} & \text{si } q = 0 \end{cases}$$

On peut donc traiter 4 cas. Mais ce n'est pas judicieux.

Mieux vaut traiter les deux cas suivants.

- Cas $[p = 0 \text{ ou } q = 0]$

Comme p et q jouent des rôles symétriques, il suffit de traiter le cas $p = 0$.

Faire le calcul.

- Cas $[p \neq 0 \text{ et } q \neq 0]$

Simple constat.

Étape 2. Utiliser que

$$\left(\sum_i u_i\right)\left(\sum_j v_j\right) = \sum_i \sum_j u_i v_j$$

Notons $P = \sum_{i=0}^p a_i X^i$ et $Q = \sum_{j=0}^q b_j X^j$.

Par linéarité de la dérivation, on a

$$(PQ)' = \left(\sum_{i=0}^p \sum_{j=0}^q a_i b_j X^i X^j\right)' = \sum_{i=0}^p \sum_{j=0}^q a_i b_j (X^i X^j)'.$$

D'après l'étape 1 de la preuve, on a :

$$\begin{aligned} (PQ)' &= \sum_{k=0}^n \sum_{\ell=0}^m a_k b_\ell \left((X^k)' X^\ell + X^k (X^\ell)' \right) \\ &= \left(\sum_{k=0}^n a_k (X^k)' \right) \left(\sum_{\ell=0}^m b_\ell X^\ell \right) + \left(\sum_{k=0}^n a_k X^k \right) \left(\sum_{\ell=0}^m b_\ell (X^\ell)' \right) \\ &= \left(\sum_{k=0}^n a_k X^k \right)' \left(\sum_{\ell=0}^m b_\ell X^\ell \right) + \left(\sum_{k=0}^n a_k X^k \right) \left(\sum_{\ell=0}^m b_\ell X^\ell \right)' \\ &= P'Q + PQ'. \end{aligned}$$

56

— Elle est libre car échelonnée en degré

— Elle est génératrice, car

pour tout $j \in \llbracket 0, n \rrbracket$, on a $X^j \in \text{Vect}((X - \alpha)^k)_{k \in \llbracket 0, j \rrbracket}$.

En effet,

$$X^j = (X - \alpha + \alpha)^j = \sum_{k=0}^j \binom{j}{k} \alpha^k (X - \alpha)^{j-k}$$

On a donc $\mathbb{K}_n[X] \subset \text{Vect}((X - \alpha)^k)_{k \in \llbracket 0, n \rrbracket}$.



60

On prouve $\Rightarrow$.

Puis, pour $\Leftarrow$, on dit que l'on a prouvé $\forall \gamma \in \mathbb{C}, Q(\gamma) = 0 \Rightarrow Q(\bar{\gamma}) = 0$, et que l'on peut appliquer cela à $\gamma = \bar{\beta}$.

Remarque. L'énoncé est invariant par conjugaison (car la conjugaison est involutive). Autrement dit, en appliquant la conjugaison à l'équivalence

$$\beta \text{ racine de } Q \iff \bar{\beta} \text{ racine de } Q$$

on obtient (en utilisant que la conjugaison est involutive) :

$$\bar{\beta} \text{ racine de } Q \iff \beta \text{ racine de } Q$$

qui est donc la même équivalence que l'initiale.

63

Preuve par récurrence forte.

Pour tout $n \geq 1$, notons $\mathcal{H}_n$ la propriété « tout polynôme de degré n est un produit de polynômes irréductibles ».

Initialisation. Un polynôme de degré 1 est irréductible, donc a fortiori, produit de polynômes irréductibles

Donc $\mathcal{H}_1$ est vraie.

Hérédité. Soit $n \geq 1$.

On suppose $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_n$.

Montrons $\mathcal{H}_{n+1}$.

Soit P de degré $n+1$.

Distinguons deux cas.

- Si P est irréductible, il est en particulier un produit de polynômes irréductibles.
- Si P n'est pas irréductible, on peut trouver deux polynômes A et B de degré a et b appartenant à $\llbracket 1, n \rrbracket$ tels que $P = AB$.

D'après l'hypothèse de récurrence, $\mathcal{H}_a$ et $\mathcal{H}_b$ sont vraies.

Donc A et B sont produits de polynômes irréductibles.

On peut donc trouver des polynômes irréductibles $P_1, \dots, P_r$ et $Q_1, \dots, Q_s$ (pas nécessairement distincts) tels que

$$A = P_1 \cdots P_r \quad \text{et} \quad B = Q_1 \cdots Q_s$$

En effectuant le produit, on a alors $AB = P_1 \cdots P_r Q_1 \cdots Q_s$, ce qui démontre que P est un produit de polynômes irréductibles.

Dans les deux cas, P est un produit de polynômes irréductibles, ce qui démontre $\mathcal{H}_{n+1}$.

Preuve par absurde-minimalité.

Raisonnons par l'absurde et supposons qu'il existe des polynômes de degré ≥ 1 qui ne soit pas produit de polynômes irréductibles.

Notons E l'ensemble des degrés de ces polynômes.

$$E = \{d \in \mathbb{N}^* \mid \exists P \in \mathbb{K}[X] \text{ de degré } d \text{ non irréductible}\}$$

Alors E est une partie de $\mathbb{N}$ (en fait de $\mathbb{N}^*$) non vide (WHY?).

Donc E admet un plus petit élément. Posons $m = \min E$.

Considérons un polynôme P de degré m dans E . Alors P n'est pas irréductible.



Donc il existe $A, B \in \mathbb{K}[X]$ de degré a et b appartenant à $\llbracket 1, m-1 \rrbracket$ tel que $P = AB$.

Par minimalité de m , les entiers a et b ne sont pas dans E .

Donc A et B sont des polynômes irréductibles.

Mais alors leur produit, à savoir P , est également un produit de polynômes irréductibles.

D'où la contradiction.

65

Preuve. Procédons par double inclusion.

- On a déjà vu l'inclusion $\supset$.
- Prouvons $\subset$. Soit $P \in \mathbb{C}[X]$ irréductible.

Alors par définition, P est non constant. D'après le théorème de d'Alembert-Gauss, P admet au moins une racine.

Étant irréductible, P est donc de degré 1. WHY?

Preuve. Procédons par double inclusion.

- Montrons l'inclusion $\supset$. Il reste à montrer qu'un polynôme de degré 2 à discriminant strictement négatif est irréductible.

Soit P un tel polynôme. Procédons par l'absurde et supposons-le non irréductible.

Alors il existe A et B tels que $P = AB$ avec A et B non constants, donc nécessairement de degré ≥ 1 , et donc de degré 1 (car $\deg P = 2$).

Mais A , en tant que polynôme de degré 1, admet une racine, qui est aussi une racine de P contredisant le fait que son discriminant soit < 0 .

- Montrons l'inclusion $\subset$. Soit $P \in \mathbb{R}[X]$ irréductible. Alors par définition, P est non constant.

Ou bien P admet une racine réelle. Étant irréductible, P est donc de degré 1. WHY?

Ou bien P n'admet pas de racine réelle, mais d'après le théorème de d'Alembert-Gauss, il admet au moins une racine dans $\mathbb{C}$, qui n'est pas dans $\mathbb{R}$ (WHY?), que l'on note α . Comme P est à coefficients réels, $\bar{\alpha}$ est également racine de P et est distincte de α .

Ainsi, P s'écrit $(X - \alpha)(X - \bar{\alpha})Q$. WHY?

Comme P est irréductible, on a nécessairement $\deg Q = 0$, disons $Q = \lambda X^0$.

Ainsi, $P = \lambda(X - \alpha)(X - \bar{\alpha})$.

Donc P est de degré 2 à discriminant strictement négatif. WHY?

66

Soit P un polynôme non nul de $\mathbb{C}[X]$.

Ou bien, il est constant, donc P est scindé.

Ou bien, il est non constant, et alors est produit de polynômes irréductibles.

Comme les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1, on obtient que P est produit de polynômes de degré 1, donc P est scindé.

70

$\Rightarrow$

Sq $B \mid A$.

Soit $z \in \mathbb{K}$.

Notons $b = \text{mult}(z, B)$. Alors $(X - z)^b \mid B$.

Comme $B \mid A$, on a $(X - z)^a \mid A$.

D'où $\text{mult}(z, A) \geq b$.

$\Leftarrow$

Écrivons $B = \lambda \prod_{i=1}^r (X - \beta_i)^{m_i}$ avec r éventuellement nul.

D'après l'hypothèse avec $z = \beta_i$, on en déduit que β_i est racine de A de multiplicité au moins m_i .

On peut donc appliquer ?? et obtenir $\prod_{i=1}^r (X - \beta_i)^{m_i} \mid A$.

D'où $B \mid A$.

