Chapitre 18

Polynôme

Hugo Salou MP2I

Dernière mise à jour le 14 juin 2022

TABLE DES MATIÈRES

Dans ce chapitre, $\mathbb{K}$ désigne un corps

Première partie

Définition

Définition: — Un polynôme à coefficients dans $\mathbb{K}$ est une suite presque nulle de $\mathbb{K}^{\mathbb{N}}$

— Le polynôme nul, noté 0 est la suite nulle.

— Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme non nul.
$\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$ est non-vide et majoré. Le degré de P est $\max\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$, et on le note $\deg(P)$ et $a_{\deg(P)}$ est le coefficient dominant de P, il est noté $\mathrm{dom}(P)$.

— Le degré du polynôme nul est $-\infty$

Proposition – Définition: Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$. Alors, $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$ est un polynôme appelé somme de P et Q.

■

Proposition – Définition: Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$. On pose

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

La suite $(c_n)_{n\in\mathbb{N}}$ est presque nulle. Ce polynôme est appelé produit de P et Q et noté PQ.

■

Remarque (Notation):
Soit $P = (a_n)_{n\in\mathbb{N}}$, un polynôme à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$. Le polynôme $(\lambda a_n)_{n\in\mathbb{N}}$ est noté λP

Remarque (Notation):
On pose $X = (0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, \ldots) = (\delta_{1,n})_{n\in\mathbb{N}}$

Théorème: Soit $P = (a_n)_{n\in\mathbb{N}}$ un polynôme non nul à coefficients dans $\mathbb{K}$. Alors

$$P = \sum_{k=0}^{n} a_k X^k \quad \text{où } n = \deg(P) \text{ et } X^0 = (1, 0, \ldots)$$

■

Remarque (Notation):
On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ dont l'indéterminée $(0, 1, 0, \ldots)$ est notée X.

Proposition: $\big(\mathbb{K}[X], +, \times, \cdot\big)$ est une $\mathbb{K}$-algèbre commutative i.e.

1. $\big(\mathbb{K}[X], +, \times\big)$ est un anneau commutatif

2. $\left(\mathbb{K}[X], +, \cdot\right)$ est un $\mathbb{K}$-espace vectoriel
3. $\forall \lambda \in \mathbb{K}, \forall (P, Q) \in \left(\mathbb{K}[X]\right)^2, \lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q)$

■

Remarque:
$(\mathscr{M}_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre non commutative (si $n > 1$)

Proposition: $i : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K}[X] \\ \lambda & \longmapsto & \lambda X^0 \end{array}$ est un morphisme d'algèbre injectif, i.e.

$$\forall \lambda, \mu \in \mathbb{K}, \begin{cases} i(\lambda + \mu) = i(\lambda) + i(\mu) \\ i(\lambda \cdot \mu) = i(\lambda) \times i(\mu) \end{cases}$$

et i est injective.

Remarque (Notation):
On identifie $\lambda \in \mathbb{K}$ avec $\lambda X^0 \in \mathbb{K}[X]$. Ainsi, on peut écrire $X^0 = 1$, on peut écrire $2 + X + 3X^2$ au lieu de $2X^0 + X + 3X^2$

Proposition: Soient $P, Q \in \mathbb{K}[X]$

— $\deg(P + Q) \leqslant \max\left(\deg(P), deg(Q)\right)$
— Si $\deg(P) \neq \deg(Q)$, alors
  — $\deg(P + Q) = \max\left(\deg(P), \deg(Q)\right)$
  — $\operatorname{dom}(P + Q) = \begin{cases} \operatorname{dom}(P) & \text{si } \deg(P) > \deg(Q) \\ \operatorname{dom}(Q) & \text{si } \deg(P) < \deg(Q) \end{cases}$
— Si $\deg(P) = \deg(Q)$ et $\operatorname{dom}(P) + \operatorname{dom}(Q) \neq 0$,
  alors $\begin{cases} \deg(P + Q) = \deg(P) = \deg(Q) \\ \operatorname{dom}(P + Q) = \operatorname{dom}(P) + \operatorname{dom}(Q) \end{cases}$
— Si $\deg(P) = \deg(Q)$ et $\deg(P) + \deg(Q) = 0$, alors $\deg(P + Q) < \deg(P)$

■

Proposition: Soient $P, Q \in \mathbb{K}[X]$. Alors

$$\deg(PQ) = \deg(P) + \deg(Q)$$

■

Deuxième partie

Évaluation

Définition: Soit A une $\mathbb{K}$-algèbre et $P \in \mathbb{K}[X]$. On pose $P = \sum_{k=0}^{n} e_k X^k$. Soit $a \in A$.
On pose

$$\begin{aligned} P(a) &= \sum_{k=0}^{n} e_k a^k \\ &= e_0 1_A + e_1 a + e_2 a^2 + \cdots + e_n a^n \in A \end{aligned}$$

On dit qu'on a <u>évalué</u> P en a, ou <u>spécialisé</u> X avec la valeur de a, ou <u>remplacé</u> X par a, <u>substitué</u> a à X.

Définition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
On dit que a est une <u>racine de P</u> si $P(a) = 0_{\mathbb{K}}$.

Définition: Soit $P \in \mathbb{K}[X] \in \mathscr{M}_n(\mathbb{K})$. On dit que c'est un <u>polynôme de matrices</u>.

Définition: Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k=0}^{n} a_k X^k$.

Alors $P(Q) = \sum_{k=0}^{n} a_k Q^k \quad \in \mathbb{K}[X]$
C'est la <u>composée</u> de P et Q.

Remarque (⚠ Attention):
Ne pas confondre $\underbrace{P(X+1)}_{\text{composée}}$ et $\underbrace{P\,(X+1)}_{\text{produit}}$.
On a $\underbrace{P\,(X+1)}_{\text{produit}} = (X+1)\,P = P(X)\,(X+1) = P \times (X+1)$

Proposition: Soient $P, Q \in \mathbb{K}[X]$ avec $\begin{cases} Q \neq 0 \\ P \neq 0 \end{cases}$. On a

$$\deg\big(P(Q)\big) = \deg(P) \times \deg(Q)$$

□

Théorème: Soit A une $\mathbb{K}$-algèbre. L'application

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow A^A \\ P &\longmapsto f_P : \begin{array}{ccc} A & \longrightarrow & A \\ a & \longmapsto & P(a) \end{array} \end{aligned}$$

vérifie

1. $\forall P, Q \in \mathbb{K}[X], \varphi(P+Q) = \varphi(P) + \varphi(Q)$
2. $\forall P, Q \in \mathbb{K}[X], \varphi(PQ) = \varphi(P) \times \varphi(Q)$
3. $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X], \varphi(\lambda P) = \lambda\varphi(P)$

□

Définition: Soit $P \in \mathbb{K}[X]$,

$$P = \sum_{k=0}^{n} a_k X^k$$

Le polynôme dérivé de P est

$$P' = \sum_{k=0}^{n} k a_k X^{k-1} = \sum_{k=1}^{n} k a_k X^{k-1}$$

où

$$\forall k \in [\![1, n]\!], k a_k = \underbrace{a_k + \cdots + a_k}_{k \text{ fois}}$$

$$0_{\mathbb{N}} a_k = 0_{\mathbb{K}}$$

Remarque:

Si $P \in \mathbb{R}[X]$, $f_p : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P(x) \end{array}$

$f_{P'} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P'(x) \end{array}$ alors $f_{P'} = f'_P$

Proposition:

$$\forall P \in \mathbb{K}[X], \deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg(P) > 0 \\ -\infty & \text{sinon} \end{cases}$$

Proposition: Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

1. $(P+Q)' = P' + Q'$
2. $(PQ)' = P'Q + PQ'$
3. $(\lambda P)' = \lambda P'$

■

Définition: Pour $k \in \mathbb{N}$, on définit la dérivée k-ième d'un polynôme $P \in \mathbb{K}[X]$ par

— si $k = 0$, $P^{(k)} = P$
— si $k = 1$, $P^{(1)} = P'$
— si $k > 1$, $P^{(k)} = \left(P^{(k-1)}\right)'$

Proposition:

$$\forall k, j \in \mathbb{N}^2, \left(X^k\right)^{(j)} = \begin{cases} 0 & \text{si } j > k \\ k(k-1)\cdots(k-j+1)X^{k-j} = \dfrac{k!}{(k-j)!}X^k & \text{si } j \leqslant k \end{cases}$$

■

Proposition: Soient $P, Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$

1. $\forall k \in \mathbb{N}, (P+Q)^{(k)} = P^{(k)} + Q^{(k)}$
2. $\forall k \in \mathbb{N}, (PQ)^{(k)} = \displaystyle\sum_{i=0}^{k} \binom{k}{i} P^{(i)} Q^{(k-i)}$
3. $\forall k \in \mathbb{N}, (\lambda P)^{(k)} = \lambda P^{(k)}$

■

Troisième partie

Arithmétique dans $\mathbb{K}[X]$

Définition: Soient $A, B \in \mathbb{K}[X]$. On dit que A divise B (dans $\mathbb{K}[X]$) s'il existe $C \in \mathbb{K}[X]$ tel que
$$AC = B$$
On dit dans ce cas que A est un diviseur de B ou que B est un multiple de A. On le note alors $A \mid B$
On dit que A et B sont associés s'il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $A = \lambda B$. Il s'agit d'une relation d'équivalence.

Proposition: Soient $A, B \in \mathbb{K}[X]$.
$$\left.\begin{matrix} A \mid B \\ B \mid A \end{matrix}\right\} \iff A \text{ et } B \text{ sont associés}$$
■

Lemme: $\mathbb{K}[X]$ est un anneau intègre.
■

Lemme:
$$\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$$
■

Proposition: $\mid$ est une relation réflexive et transitive. □

Proposition: Soient $A, B, C \in \mathbb{K}[X]$ tels que $A \mid B$ et $A \mid C$. Alors
$$\forall (P, Q) \in \mathbb{K}[X]^2, A \mid BQ + CP$$
□

Proposition – Définition: Soit $A \in \mathbb{K}[X], B \in \mathbb{K}[X] \setminus \{0\}$.
$$\exists ! (P, Q) \in \mathbb{K}[X]^2, \begin{cases} A = PQ + R \\ \deg(R) < \deg(B) \end{cases}$$
On dit que Q est le quotient et R le reste de la division (euclidienne) de A par B.
■

Théorème: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
$$P(a) = 0 \iff X - a \mid P$$
■

Corollaire: Soit $P \in \mathbb{K}[X]$ non nul de degré n. Alors, P a au plus n racines distinctes dans $\mathbb{K}$

■

Définition: Soient A et B deux polynômes dont l'un au moins est non nul, $D \in \mathbb{K}[X]$. On dit que D est un PGCD de A et B si D est un diviseur commun de A et B et de degré maximal.

Proposition: Avec les hypothèse précédents, deux PGCD quelconques de A et B sont nécessairement associés

■

Remarque:
Dans la preuve précédente, on a aussi montré les deux propositions suivantes.

Théorème (Théorème de Bézout)**:** Soient $A, B \in \mathbb{K}[X]$ tels que $A \neq 0$ ou $B \neq 0$ Soit D un PGCD de A et B. Alors

$$\exists (U, V) \in \mathbb{K}[X]^2, AU + BV = D$$

■

Proposition: Avec les hypothèses précédents,

$$\forall \Delta \in \mathbb{K}[X],$$
$$\left.\begin{array}{l} \Delta \mid A \\ \Delta \mid B \end{array}\right\} \iff \Delta \mid D$$

■

Définition: On dit qu'un polynôme est <u>unitaire</u> si sont coefficient dominant vaut 1.

Proposition – Définition: Soient A et B deux polynômes dont l'un au moins est non nul. Parmi tous les PGCD de A et B, un seul est unitaire. On le note $A \wedge B$.

■

Proposition: Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Soit R le reste de la division de A par B. Alors,

$$A \wedge B = B \wedge R$$

■

Théorème (Théorème de Gauß)**:** Soient A, B, C trois polynômes non nuls tels que
$\begin{cases} A \mid BC \\ A \wedge B = 1 \end{cases}$
Alors, $A \mid C$

■

Corollaire: Avec les notations précédentses,

$$\left.\begin{array}{l} A \mid B \\ B \mid C \\ A \wedge B = 1 \end{array}\right\} \implies AB \mid C$$

Proposition: Soient A et B deux polynômes non nuls et D un PGCD de A et B. Soit $x \in \mathbb{K}$.

$$A(x) = B(x) = 0 \iff D(X) = 0$$

■

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

On dit que P n'est pas irréductible si il existe $(Q, R) \in \mathbb{K}[X]^2$ non constants tels que $P = QR$ **ou** si P est constant.

Sinon, on dit que P est irréductible.

Théorème (Théorème de D'Alembert - Gauß)**:**

$$\forall P \in \mathbb{C}[X] \text{ non constant}, \exists a \in \mathbb{C}, P(a) = 0$$

□

Corollaire: Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactemenent les polynômes de degré 1.

■

Définition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, $\mu \in \mathbb{N}$.
On dit que a est une racine de P de multiplicité μ si

$$\begin{cases} (X-a)^\mu \mid P \\ (X-a)^{\mu+1} \nmid P \end{cases}$$

Si $\mu = 1$, on dit que a est une racine simple.
Si $\mu = 2$, on dit que a est une racine double.

Remarque:
a est une racine de multiplicité 0 si et seulement si $P(a) \neq 0$

Lemme: Soient $(A, B) \in \mathbb{R}[X]^2$ non nuls. On suppose que A divise B dans $\mathbb{C}[X]$
Alors, A divise B dans $\mathbb{R}[X]$

■

Proposition: Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$, $\mu \in \mathbb{N}$.
Si a est une racine de P de multiplicité μ alors $\overline{a}$ est une racine de P de multiplicité μ.

■

Corollaire: Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatifs.

■

Théorème: Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Tout polynôme de $\mathbb{K}$ se découpe en produit de facteurs irréductibles dans $\mathbb{K}[X]$ et cette décomposition est unique à multiplication par une constante non nulle près. □

Proposition: Soient $A, B \in \mathbb{C}[X]$ non nuls.

$$A \mid B \iff \begin{array}{l} \forall a \in \mathbb{C},\ \text{si } a \text{ est une racine de } A \text{ de multiplicité } \mu \in \mathbb{N}, \\ \text{alors } a \text{ est racine de } B \text{ avec une multiplicité } \geqslant \mu \end{array}$$

■

Proposition: Soit $P \in \mathbb{C}[X]$ de degré $n > 0$
Alors P a exactement n racines comptées avec multiplicité.

■

Quatrième partie

L'espace vectoriel $\mathbb{K}[X]$

Remarque (Rappel):
$(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel engendré par $(1, X, X^2, \ldots)$

Proposition: La famille $(X^n)_{n\in\mathbb{N}}$ est libre.

■

Corollaire:

$$\dim\big(\mathbb{K}[X]\big) = +\infty$$

□

Définition: Pour $n \in \mathbb{N}$, on note

$$\mathbb{K}_n[X] = \big\{P \in \mathbb{K}[X] \mid \deg(P) \leqslant n\big\}$$

Théorème: $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension $n+1$

■

Proposition: Soit $(P_i)_{i\in I}$ une famille de polynômes non nuls telle que

$$\forall i \neq j, \deg(P_i) \neq \deg(P_j)$$

Alors $(P_i)_{i\in I}$ est libre.

■

Théorème (Formule de Taylor)**:** Soit $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$.

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

■

Proposition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$\left.\begin{array}{r} a \text{ est une racine de } P \\ \text{de multiplicité } \mu \end{array}\right\} \iff \left\{\begin{array}{l} \forall k \leqslant \mu - 1, P^{(k)}(a) = 0 \\ P^{(\mu)}(a) \neq 0 \end{array}\right.$$

■

Corollaire: Avec les notations précédentes, si a est une racine de P de multiplicité μ, alors a est une racine de P' de multiplicité $\mu - 1$

□

Définition: On dit qu'un polynôme P est <u>scindé</u> sur $\mathbb{K}$ si P est un produit de polynômes de $\mathbb{K}[X]$ de degré 1, i.e. toutes les racines de P sont dans $\mathbb{K}$

Définition: Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ avec

$$\forall i \neq j, x_i \neq x_j$$

On pose

$$\forall i \in [\![1, n]\!], L_i = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$$

L_i est le <u>i-ème polynôme interpolateur de Lagrange</u> associé à $(x_1, \dots, x_n)$:

$$\forall j \in [\![1, n]\!], L_i(x_j) = \delta_{i,j}$$

Proposition: Avec les notations précédentes, $(L_1, \dots, L_n)$ est une base de $\mathbb{K}_{n-1}[X]$.

■