CHAPITRE 18

POLYNÔMES FORMELS

1. Construction formelle

Naïvement, un polynôme est une expression de la forme $a_nX^n + \cdots + a_1X + a_0$, où $a_0, \ldots, a_n$ sont des scalaires. Il nous faut donc définir l'indéterminée X (qui ensuite pourra être remplacée par un réel ou une matrice), la somme de deux polynômes et le produit de deux polynômes. En réalité, un polynôme est entièrement déterminé par la suite de ses coefficients $a_0, \ldots, a_n$, d'où l'idée de définir un polynôme formellement par ses coefficients.

Définition 1.1

On appelle *polynôme à coefficients dans* $\mathbb{K}$ toute suite $(a_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ telle qu'il existe un ensemble **fini** $I \subset \mathbb{N}$ tel que pour tout $k \notin I$, $a_k = 0$. (On parle aussi de suite presque nulle).

Les scalaires a_k, $k \in \mathbb{N}$ sont alors appelés coefficients du polynôme.

Définition 1.2

Soient (a_k) et (b_k) deux polynômes. Leur *somme* est le polynôme $(a_k + b_k)$.

Définition 1.3

Soient (a_k) et (b_k) deux polynômes. Leur *produit* est le polynôme (c_k) où

$$\forall k \in \mathbb{N},\ c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Exemple 1.4

(1) Tout scalaire x peut être identifié (et le sera) au polynôme (a_k) défini par $a_0 = x$ et pour tout $k \geq 1$, $a_k = 0$. La somme et le produit de deux scalaires correspond à la somme et au produit des polynômes associés.

(2) On note X le polynôme défini par la suite (b_k) où $b_1 = 1$ et pour tout $k \neq 1$, $b_k = 0$. Calculons X^2 : on note $(c_k) = X^2$ et donc $c_0 = b_0 \times b_0 = 0$, $c_1 = b_1 \times b_0 + b_0 \times b_1 = 0$, $c_2 = b_2b_0 + b_1^2 + b_0b_2 = 1$ et pour tout $k \geq 3$, $c_k = \sum_{i=0}^{k} b_i b_{k-i} = 2b_1b_{k-1} = 0$.

Notation 1.5

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. Le polynôme X est appelé *l'indéterminée*.

Proposition 1.6

$\forall n \in \mathbb{N},\ X^n = (a_k)$ où $\forall k \neq n,\ a_k = 0$ et $a_n = 1$.

Proposition 1.7

Soit $P \in \mathbb{K}[X]$ non nul. Il existe un unique entier n et un unique $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$ tels que $P = \sum_{k=1}^{n} a_k X^k$ et $a_n \neq 0$.

Proposition 1.8

Soient P, Q, R trois polynômes.

(1) $(P+Q)+R = P+(Q+R)$;
(2) $P+Q = Q+P$;
(3) $P(QR) = (PQ)R$;
(4) $PQ = QP$;
(5) $(P+Q)R = PR+QR$.

2. Degré d'un polynôme

Définition 2.1

Le *degré* d'un polynôme $P = (a_k)$ non nul est l'entier $\deg(P) = \max\{k \in \mathbb{N} \mid a_k \neq 0\}$, et son *coefficient dominant* est alors $\mathrm{dom}(P) = a_n$. Le monôme $a_n X^n$ est alors appelé *terme dominant* de P. On dit qu'un polynôme est *unitaire* si $\mathrm{dom}(P) = 1$. Par convention, le degré du polynôme nul est $-\infty$.

Proposition 2.2

Soient P et Q deux polynômes non nuls.

(1) $\deg(P+Q) \leq \max(\deg(P), \deg(Q)$ avec égalité si et seulement si $(\deg P \neq \deg Q))$ ou $(\deg(P) = \deg(Q)$ et $\mathrm{dom}(P) + \mathrm{dom}(Q) \neq 0)$.
(2) $\deg(PQ) = \deg(P)\deg(Q)$ et $\mathrm{dom}(PQ) = \mathrm{dom}(P)\,\mathrm{dom}(Q)$.

3. L'espace vectoriel des polynômes

Notation 3.1

Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré inférieur ou égal à n.

Proposition 3.2

$\mathbb{K}[X]$ est un espace vectoriel, et pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.

Proposition 3.3

Soit $n \in \mathbb{N}^*$. La famille $(1, X, \dots, X^n)$ est une base de $\mathbb{K}_n[X]$, appelée *base canonique*, et donc $\dim(\mathbb{K}_n[X]) = n+1$.

Définition 3.4

Soient $(P_i)_{i\in I}$ une famille de polynômes. On dit qu'elle est *de degrés échelonnés* si pour tout $i \neq j$, $\deg(P_i) \neq \deg(P_j)$.

Proposition 3.5

Toute famille de polynômes non nuls de degrés échelonnés est libre.

4. Fonctions polynomiales

Dans ce paragraphe, E désignera $\mathbb{R}$, ou $\mathbb{C}$, ou $M_n(\mathbb{K})$, ou $\mathbb{R}^I$, ou $\mathbb{C}^{\mathbb{N}}$, ou $\mathbb{K}[X]$, de manière générale, tout ensemble dans lequel on peut additionner et multiplier comme dans $M_n(\mathbb{K})$ par exemple.

Définition 4.1

Soit $P = \sum_k a_k X^k \in \mathbb{K}[X]$ et $x \in E$. L'élément $\sum_k a_k x^k$ de E est noté $P(x)$ et on dit que l'on a substitué x à X. On obtient de cette façon la fonction polynomiale $f_P : x \in E \mapsto P(x) \in E$.

Proposition 4.2

Soient P et Q deux polynômes et $x \in E$. Alors $(P+Q)(x) = P(x) + Q(x)$ et $(PQ)(x) = P(x)Q(x)$.

Proposition 4.3

L'application $P \in \mathbb{K}[X] \mapsto f_P \in \mathbb{K}^{\mathbb{K}}$ est injective.

Définition 4.4

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. Son *polynôme dérivé*, noté P' est défini par

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

On définit les polynômes dérivés successifs de P par récurrence : $P^{(k+1)} = \left(P^{(k)}\right)'$.

Proposition 4.5

Soit $P \in \mathbb{R}[X]$ et $f : \mathbb{R} \to \mathbb{R}$ la fonction polynomiale associée. Alors f est dérivable et f' est la fonction polynomiale associée à P'.

Proposition 4.6

Soient $P, Q \in \mathbb{K}[X]$. On a $(P+Q)' = P' + Q'$ et $(PQ)' = P'Q + PQ'$.

Proposition 4.7: Formule de Taylor

Soit $P \in \mathbb{K}[X]$ non nul de degré n, et $a \in \mathbb{K}$. Alors

$$P = P(a) + \sum_{k=1}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Définition 4.8

Soient $P, Q \in \mathbb{K}[X]$. On définit le polynôme composé $P(Q)$ en substituant Q à X.

5. Arithmétique des polynômes

5.1. Divisibilité.

Définition 5.1

Soient $A, B \in \mathbb{K}[X]$. On dit que A *divise* B, situation notée $A|B$, s'il existe $Q \in \mathbb{K}[X]$ tel que $B = AQ$.

Exemple 5.2

Le polynôme $X - i$ divise $X^2 + 1$ dans $\mathbb{C}[X]$ car $X^2 + 1 = (X-i)(X+i)$.

Définition 5.3

Soit $A \in \mathbb{K}[X]$. On dit que A *n'est pas irréductible* (dans $\mathbb{K}[X]$) s'il existe $B, Q \in \mathbb{K}[X]$ non constants tels que $A = BQ$. Si ce n'est pas le cas, on dit que A est *irréductible*.

Exemple 5.4

Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$.

Proposition 5.5

Tout polynôme non constant peut s'écrire de façon unique à une constante multiplicative près comme produit de polynômes irréductibles.

5.2. Division euclidienne.

Proposition 5.6

Soient A, $B \in \mathbb{K}[X]$ tels que $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]$ tels que

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B). \end{cases}$$

Corollaire 5.7

Soient $A, B \in \mathbb{K}[X]$. Alors $B|A$ si et seulement si le reste dans la division de A par B est nul.

5.3. PGCD et PPCM.

Définition 5.8

Soient A et B deux polynômes dont l'un au moins est non nul. Soit D un autre polynôme. On dit que D est un *PGCD* de A et B si R est un diviseur de A et B de degré maximal.

Remarque 5.9

Avec les notations précédentes, tous les PGCD de A et B sont associés.

Notation 5.10

On note $A \wedge B$ le seul PGCD de A et B unitaire.

Proposition 5.11: Euclide

Soient A et B deux polynômes avec $B \neq 0$. On pose R le reste de la division euclidienne de A par B. Alors $A \wedge B = B \wedge R$.

Théorème 5.12: Bézout

Soient A et B deux polynômes non tous les deux nuls et $D = A \wedge B$. Alors il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = D$.

Corollaire 5.13

Soient A et B deux polynômes dont l'un au moins est non nul, et D un autre polynôme. Alors D divise à la fois A et B si et seulement si D divise $A \wedge B$.

Définition 5.14

On dit que deux polynômes sont *premiers entre eux* si $A \wedge B = 1$.

Théorème 5.15: Gauss

Soient A, B, C trois polynômes tels que $A \wedge B = 1$ et $A|BC$. Alors $A|C$.

Corollaire 5.16

Soient A, B, C trois polynômes tels que $A|C$, $B|C$ et $A \wedge B = 1$. Alors $AB|C$.

Définition 5.17

Soient A, B, M trois polynômes. On dit que R est un *PPCM* de A et B si R est un multiple de A et B de degré minimal. On note $A \vee B$ le seul PPCM unitaire de A et B.

Proposition 5.18

Soient A et B deux polynômes dont l'un au moins est non nul. Alors $(A \wedge B)(A \vee B)$ et AB sont associés.

6. Racines d'un polynôme

Définition 6.1

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une *racine* de P si $P(a) = 0$.

Proposition 6.2

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

$$P(a) = 0 \iff X - a | P.$$

Corollaire 6.3

Soit $P \in \mathbb{K}[X]$ non nul, de degré n. Alors P a au maximum n racines.

Corollaire 6.4

L'application $P \in \mathbb{K}[X] \mapsto f_P \in \mathbb{K}^{\mathbb{K}}$ est injective.

Définition 6.5

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une racine de P de multiplicité m si $(X-a)^m | P$ et $(X-a)^{p+1} \nmid P$. Lorsque $m = 1$, on dit que a est une racine *simple* de P.

Exemple 6.6

i et $-i$ sont racines de multiplicité 2 de $P = X^4 - 2X^2 + 1$ car $P = (X^2+1)^2 = (X-i)^2(X+i)^2$.

Proposition 6.7

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

$$a \text{ est une racine de } P \text{ de multiplicité } m \iff \begin{cases} \forall k \in [\![0, m-1]\!], P^{(k)}(a) = 0 \\ P^m(a) \neq 0. \end{cases}$$

6.1. Théorème fondamental de l'algèbre.

Théorème 6.8: D'Alembert-Gauss

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

Corollaire 6.9

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

Corollaire 6.10

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et les polynômes de degré 2 sans racine réelle.

Exemple 6.11

Le polynôme X^4+1 n'est pas irréductible dans $\mathbb{R}[X]$ alors qu'il n'a aucune racine réelle. En effet,

$$X^4+1 = X^4+2X^2+1-2X^2 = (X^2+1)^2-2X^2 = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$

Définition 6.12

Soit $P \in \mathbb{K}[X]$. On dit que P est *scindé* si P est un produit de polynômes de degré 1.

Remarque 6.13

— Tout polynôme de $\mathbb{C}[X]$ est scindé.
— Un polynôme à coefficients réels est scindé sur $\mathbb{R}[X]$ si et seulement toutes ses racines sont réelles.

6.2. Relations entre coefficients et racines.

Proposition 6.14

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ unitaire, non constant de degré n, $x_1, \dots, x_n$ ses racines (comptées plusieurs fois). Alors

$$\forall k \in [\![0, n-1]\!],\ a_k = (-1)^{n-k} \sum_{0 \leq i_1 < i_2 < \dots < i_{n-k} \leq n} x_{i_1} x_{i_2} \cdots x_{i_{n-k}}.$$

En particulier, $a_0 = (-1)^n \prod_{i=1}^{n} x_i$ et $a_{n-1} = -\sum_{i=1}^{n} x_i$.

Exemple 6.15

Soit $P = aX^2+bX+c \in \mathbb{C}[X]$, $a \neq 0$, et x_1, x_2 les deux racines de P, éventuellement confondues. On a $x_1+x_2 = \dfrac{-b}{a}$ et $x_1 x_2 = \dfrac{c}{a}$.

Exemple 6.16

Soit $P = X^3+a_2X^2+a_1X+a_0 \in \mathbb{C}[X]$ et x_1, x_2, x_3 ses racines (éventuellement confondues). Alors $x_1+x_2+x_3 = -a_2$ et $x_1x_2x_3 = -a_0$. On a aussi $x_1x_2 + x_2x_3 + x_1x_3 = a_1$.