Polynômes

I. L'aspect formel des polynômes

1) Définitions, opérations

Définition. Dans un premier temps, un polynôme à coefficients dans $\mathbb{K}$ est une suite d'éléments comportant un nombre fini (éventuellement nul) de termes non nuls. Dans un premier temps, un polynôme s'écrit donc $P = (a_0, a_1, \ldots)$ où la suite $(a_k)_{k\in\mathbb{N}}$ est à support fini (le support de la suite $(a_k)_{k\in\mathbb{N}}$ étant l'ensemble des entiers k tels que $a_k \neq 0$.

On note alors X le polynôme $(0, 1, 0, 0\ldots)$ et une fois défini les opérations usuelles sur les polynômes, on adopte une nouvelle notation : $P = \sum_{k=0}^{+\infty} a_k X^k$ (la somme étant en fait finie) ou $P = \sum_{k=0}^{n} a_k X^k$ (n ne désignant le degré de P que si $a_n \neq 0$).

Les opérations dans $\mathbb{K}[X]$ sont définies par (les suites considérées ci-dessous étant à support fini) :

- Si $A = \sum_{n=0}^{+\infty} a_n X^n$ et $B = \sum b_n X^n$, alors $A + B = \sum_{n=0}^{+\infty} (a_n + b_n) X^n$,
- Si $A = \sum_{n=0}^{+\infty} a_n X^n$, alors $\lambda A = \sum_{n=0}^{+\infty} (\lambda a_n) X^n$,
- Si $A = \sum_{n=0}^{+\infty} a_n X^n$ et $B = \sum b_n X^n$, alors $A \times B = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n$,
- Si $A = \sum_{n=0}^{+\infty} a_n X^n$ et $B = \sum b_n X^n$, alors $B \circ A = \sum_{n=0}^{+\infty} b_n A^n$.

Théorème.
• $(\mathbb{K}[X], +, .)$ est un $\mathbb{K}$-espace vectoriel de dimension infinie. La base canonique de $\mathbb{K}[X]$ est $(X^n)_{n\in\mathbb{N}}$.
• $(\mathbb{K}[X], +, \times)$ est un anneau commutatif et intègre (dans $\mathbb{K}[X]$, un produit de facteurs est nul si et seulement si l'un de ses facteurs est nul (se démontre grâce aux degrés des polynômes)). Les inversibles de cet anneau sont les constantes non nulles.
• $(\mathbb{K}[X], +, ., \times)$ est une $\mathbb{K}$-algèbre de dimension infinie.

2) Dérivation (formelle)

Définition. Si $P = \sum_{n=0}^{+\infty} a_n X^n$, alors $P' = \sum_{n=1}^{+\infty} n a_n X^{n-1} = \sum_{n=0}^{+\infty} (n+1) a_{n+1} X^n$.

Plus généralement, $P^{(k)} = \sum_{n=k}^{+\infty} n(n-1)\ldots(n-k+1) X^{n-k} = \sum_{n=0}^{+\infty} (n+k)(n+k-1)\ldots(n+1) a_{n+k} X^n = \sum_{n=0}^{+\infty} \frac{(n+k)!}{n!} a_{n+k} X^n$.

Théorème. Cette dérivation formelle obéit à toutes les formules usuelles connues en analyse.

En particulier, $(P_1 \times \ldots \times P_k)' = \sum_{i=1}^{k} P_i' \prod_{j\neq i} P_j$ et $(P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$ (Leibniz).

3) Degré, coefficient dominant

Définition. Si P est un polynôme non nul, $\deg(P) = \mathrm{Max}\{k \in \mathbb{N} / \ a_k \neq 0\}$. D'autre part, par convention, $\deg(0) = -\infty$. Si P n'est pas nul, $\mathrm{dom}(P) = a_n$ où $n = \deg(P)$. Un polynôme unitaire (ou normalisé) est un polynôme de coefficient dominant égal à 1.

Théorème.
- $\deg(P \times Q) = \deg(P) + \deg(Q)$.
- $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.
- $\deg(\lambda P) = \begin{cases} \deg(P) \text{ si } \lambda \neq 0 \\ -\infty \text{ si } \lambda = 0 \end{cases}$. Dans tous les cas, $\deg(\lambda P) \leqslant \deg(P)$.
- Si $\deg(P) \neq \deg(Q)$ ou si $\deg(P) = \deg(Q) \neq -\infty$ et $\mathrm{dom}(P) \neq -\mathrm{dom}(Q)$, $\deg(P + Q) = \mathrm{Max}\{\deg(P), \deg(Q)\}$. Dans tous les cas, $\deg(P + Q) \leqslant \mathrm{Max}\{\deg(P), \deg(Q)\}$.

Théorème. Si $\mathbb{K}_n[X]$ est l'ensemble des polynômes de degré inférieur ou égal à n, $(\mathbb{K}_n[X], +, .)$ est un $\mathbb{K}$-espace vectoriel de dimension $n + 1$. La base canonique de $(\mathbb{K}_n[X], +, .)$ est $\left(X^k\right)_{0\leqslant k\leqslant n}$.

II. Arithmétique des polynômes

1) Division euclidienne

Théorème. Soient A et B deux éléments $\mathbb{K}[X]$ tels que $B \neq 0$. Il existe un couple (Q, R) élément de $(\mathbb{K}[X])^2$ et un seul tel que :

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

Q est le quotient de la division euclidienne de A et par B (ou aussi la partie entière de la fraction rationnelle $\frac{A}{B}$) et R est le reste de la division euclidienne de A et par B. Disposition pratique pour la division euclidienne de $2X^7 - X^4 + X^3 + X + 1$ par $X^2 - 3X + 1$:

$$\begin{array}{rl|l}
2X^7 - X^4 + X^3 + X + 1 & & X^2 - 3X + 1 \\
\hline
-(2X^7 - 6X^6 + 2X^5) & & 2X^5 + 6X^4 + 16X^3 + 41X^2 + 108X + 283 \\
\cline{1-1}
6X^6 - 2X^5 - X^4 + X^3 + X + 1 & & \\
-(6X^6 - 18X^5 + 6X^4) & & \\
\cline{1-1}
16X^5 - 7X^4 + X^3 + X + 1 & & \\
-(16X^5 - 48X^4 + 16X^3) & & \\
\cline{1-1}
41X^4 - 15X^3 + X + 1 & & \\
-(41X^4 - 123X^3 + 41X^2) & & \\
\cline{1-1}
108X^3 - 41X^2 + X + 1 & & \\
-(108X^3 - 324X^2 + 108X) & & \\
\cline{1-1}
283X^2 - 107X + 1 & & \\
-(283X^2 - 849X + 283) & & \\
\cline{1-1}
742X - 282 & &
\end{array}$$

2) Divisibilité

Définition. Soient A et B deux polynômes, $A \neq 0$. A divise B si et seulement si $\exists Q \in \mathbb{K}[X] / \ B = AQ$ ou encore A divise B si et seulement si le quotient de la division euclidienne de B par A est nul.

Théorème.
- La relation « A divise B » est réflexive et transitive.
- Si A et B sont deux polynômes non nuls, $A|B$ et $B|A$ si et seulement si $\exists \lambda \in \mathbb{K}^* / \ B = \lambda A$.
- Si C divise A et B, alors C divise $Q_1 \times A + Q_2 \times B$ pour tous polynômes Q_1 et Q_2.

3) PGCD. PPCM

Théorème et définition. Soient A et B deux polynômes non nuls. Il existe un et un seul polynôme unitaire D tel que
- D divise A et B,
- tout polynôme divisant A et B a un degré inférieur ou égal au degré de D.

D est le PGCD de A et B.

Théorème. Les diviseurs communs à deux polynômes non nuls A et B sont les diviseurs de leur PGCD.

Définition. Deux polynômes non nuls dont le PGCD est égal à 1 sont dits premiers entre eux.

Théorème et définition. Soient A et B deux polynômes non nuls. Il existe un et un seul polynôme unitaire M tel que
- M multiple de A et B,
- tout polynôme non nul multiple de A et B a un degré supérieur ou égal au degré de M.

M est le PPCM de A et B.

Théorème. Les multiples communs à deux polynômes non nuls A et B sont les multiples de leur PPCM.

4) Bézout et Gauss

Théorème de Bézout. Soient A et B deux polynômes non nuls. A et B sont premiers entre eux si et seulement si $\exists (U, V) \in \mathbb{K}[X]/; AU + BV = 1$.

Dans ce cas, une solution particulière (U_0, V_0) de l'équation de Bézout $AU + BV = 1$ peut être obtenue par l'algorithme d'Euclide.

Théorème de Gauss. Soient A, B et C trois polynômes, $A \neq 0$, $B \neq 0$. Si A divise BC et A est premier à B, alors A divise C.

5) Polynômes irréductibles, théorème de d'Alembert. Un bref rappel est effectué dans le résumé sur les fractions rationnelles.

III. L'aspect fonctionnel des polynômes

1) Formule de Taylor

Théorème. Pour tout polynôme P et tout nombre a, on a $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k$ (la somme est finie). En particulier, $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!}X^k$. Si P est non nul de degré $n \in \mathbb{N}$, $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$ et en particulier, $P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}X^k$.

Corollaire. Le reste de la division euclidienne de P par $(X-a)^p$, $p \in \mathbb{N}^*$, est $\sum_{k=0}^{p-1} \frac{P^{(k)}(a)}{k!}(X-a)^k$.

Corollaire. Si $P = \sum a_k X^k$, alors pour tout k, $a_k = \frac{P^{(k)}(0)}{k!}$ et aussi $P^{(k)}(0) = k!a_k$.

2) Racines d'un polynôme non nul

a) Définition. Soient P un polynôme et a un nombre. a est racine de P si et seulement si a est racine de P.

Théorème. a est racine de $P \neq 0$ si et seulement si P est divisible par $X - a$.

Corollaire. Un polynôme non nul de degré $n \in \mathbb{N}$ a un nombre de racines au plus égal à n.

Corollaire. • Un polynôme de degré inférieur ou égal à $n \in \mathbb{N}$ qui admet au moins $n+1$ racines deux à deux distinctes est nécessairement le polynôme nul.
• Un polynôme qui s'annule en une infinité de valeurs est nécessairement le polynôme nul.
• Deux polynômes qui coïncident en une infinité de valeurs sont égaux.

b) Ordre de multiplicité d'une racine d'un polynôme non nul.

Définition. Soient $P \in \mathbb{K}[X] \setminus \{0\}$, $a \in \mathbb{K}$ et $k \in \mathbb{N}^*$. a est racine de P d'ordre k si et seulement si P est divisible par $(X-a)^k$ et pas par $(X-a)^{k+1}$ ou encore a est racine de P d'ordre k si et seulement si il existe un polynôme Q tel que $P = Q \times (X-a)^k$ et $Q(a) \neq 0$.
a est racine d'ordre 0 de P si et seulement si a n'est pas racine de P.

Théorème (caractérisation de l'ordre de multiplicité). a est racine d'ordre $k \geqslant 1$ si et seulement si $P(a) = P'(a) = \ldots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.
a est racine d'ordre au moins $k \geqslant 1$ si et seulement si $P(a) = P'(a) = \ldots = P^{(k-1)}(a) = 0$.

Corollaire. • a est racine simple de P si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.
• P est à racines simples si et seulement si P et P' n'ont pas de racine commune dans $\mathbb{C}$ si et seulement si P et P' sont premiers entre eux.

Corollaire. Si a est racine d'ordre $p \geqslant 1$ de P, pour tout $k \in [\![0, p]\!]$, a est racine d'ordre $p-k$ de $P^{(k)}$

IV. Relations entre coefficients et racines d'un polynôme scindé

Soit $P = \sum_{k=0}^{n} a_k X^k = a_n (X-z_1)\ldots(X-a_n)$ où $n \geqslant 1$, $a_n \neq 0$ $\quad (*)$.
On pose $\sigma_1 = z_1 + \ldots + z_n$, $\sigma_n = z_1 \times \ldots \times z_n$ et plus généralement pour $1 \leqslant k \leqslant n$,

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} z_{i_1} \times z_{i_2} \times \ldots \times z_{i_k}$$
$$= \text{somme des produits } k \text{ à } k \text{ des } n \text{ racines (pas nécessairement deux à deux distinctes) de } P.$$

En développant l'expression factorisée de P et en identifiant, on obtient

$$\begin{aligned}
&\sigma_1 = -\frac{a_{n-1}}{a_n}\\
&\sigma_n = (-1)^n \frac{a_0}{a_n}\\
&\forall k \in [\![1, n]\!],\ \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.
\end{aligned}$$

- Si $P = aX^2 + bX + c = a(X - z_1)(X - z_2)$, $a \neq 0$, alors $z_1 + z_2 = -\dfrac{b}{a}$ et $z_1 z_2 = \dfrac{c}{a}$.
- Si $P = aX^3 + bX^2 + cX + d = a(X - z_1)(X - z_2)(X - z_3)$, $a \neq 0$, alors $z_1 + z_2 + z_3 = -\dfrac{b}{a}$ et $z_1 z_2 + z_1 z_3 + z_2 z_3 = \dfrac{c}{a}$ et $z_1 z_2 z_3 = -\dfrac{d}{a}$.