CHAPITRE 15

Polynômes

Sommaire

Dans tout le cours, $\mathbb{K}$ désigne l'un des ensembles $\mathbb{R}$ ou $\mathbb{C}$.

I Ensemble des polynômes

Définition 1 : Polynôme

Un polynôme est une expression de la forme $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ où les coefficients a_0, a_1, $\ldots$, a_n appartiennent à $\mathbb{K}$.
Dès lors que $a_n \neq 0$, n est appelé le **degré** du polynôme, a_n son **coefficient dominant**, et a_nX^n son **terme de plut haut degré**.
L'ensemble de tous les polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.
L'ensemble de tous les polynômes de degré inférieur ou égal à n est noté $\mathbb{K}_n[X]$.

Remarque :

- ▷ Le polynôme nul a tous ses coefficients égaux à 0, et par convention son degré est $-\infty$.
- ▷ Un polynôme dont le coefficient dominant est égal à 1 est appelé **polynôme unitaire**.
- ▷ On peut écrire tout polynôme de $\mathbb{K}[X]$ sous la forme $\sum_{k=0}^{+\infty} a_kX^k$ en comprenant que les coefficients a_k sont tous nuls à partir d'un certain rang (la somme est donc finie).

Définition 2 : Opérations sur les polynômes

Étant donnés deux polynômes $P = \sum_{k=0}^{+\infty} a_kX^k$ et $Q = \sum_{k=0}^{n} b_kX^k$, on définit :

- La **somme** des deux polynômes par : $P + Q = \sum_{k=0}^{+\infty} (a_k + b_k)X^k$
- Le **produit** des deux polynômes par : $P \times Q = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} a_ib_{k-i} \right) X^k$
- La **composée** des deux polynômes par : $P \circ Q = \displaystyle\sum_{k=0}^{+\infty} a_k \left(\sum_{i=0}^{n} b_iX^i \right)^k$

Théorème 1 : Degré d'une somme, d'un produit

Pour tous polynômes $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_k X^k$ de $\mathbb{K}[X]$,

- $\deg(P+Q) \leq \max(\deg P, \deg Q)$
- $\deg(P \times Q) = \deg P + \deg Q$ et le terme de plus haut degré de $P \times Q$ est $a_n b_p X^{n+p}$.
  En particulier, $\forall P, Q \in \mathbb{K}[X],\ P \times Q = 0 \Rightarrow P = 0$ ou $Q = 0$.

Définition 3 : Fonctions polynomiale associée

Étant donné un polynôme $P \in \mathbb{K}[X]$, on appelle fonction polynomiale associée la fonction de $\mathbb{K}$ dans $\mathbb{K}$ qui à x associe $P(x)$.

II Division euclidienne de polynômes

Définition 4 : Divisibilité dans $\mathbb{K}[X]$

Étant donnés trois polynômes P, Q et R de $\mathbb{K}[X]$, tels que $P = Q \times R$, on dit que Q est un **diviseur** de P et que P est un **multiple** de Q.

Théorème 2 : Division euclidienne de polynômes (admis)

$\forall A \in \mathbb{K}[X], \forall B \in \mathbb{K}[X] \setminus \{0\}, \exists Q, R \in \mathbb{K}[X],\ A = BQ + R$, avec $\deg R < \deg B$.

On peut « poser » une division de polynômes :

$$\begin{array}{rrrrrrrrrrrr|c}
 & 2X^5 & - & 5X^4 & + & 3X^3 & - & 2X^2 & - & 9X & - & 3 & X^2 - 2X - 1 \\ \cline{13-13}
- & (2X^5 & - & 4X^4 & - & 2X^3) & & & & & & & 2X^3 - X^2 + 3X + 3 \\
 & & & -X^4 & + & 5X^3 & - & 2X^2 & - & 9X & - & 3 & \\
 & & - & (-X^4 & + & 2X^3 & + & X^2) & & & & & \\
 & & & & & 3X^3 & - & 3X^2 & - & 9X & - & 3 & \\
 & & & & - & (3X^3 & - & 6X^2 & - & 3X) & & & \\
 & & & & & & & 3X^2 & - & 6X & - & 3 & \\
 & & & & & & - & (3X^2 & - & 6X & - & 3) & \\
 & & & & & & & & & & & 0 &
\end{array}$$

Donc $2X^5 - 5X^4 + 3X^3 - 2X^2 - 9X - 3 = (X^2 - 2X - 1)(2X^3 - X^2 + 3X + 3)$.

III Polynôme dérivé

Définition 5

Pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k$,

- On appelle polynôme dérivé de P et on note P' le polynôme $\sum_{k=1}^{n} k a_k X^{k-1}$.
- Pour tout $k \in \mathbb{N}^*$, on note $P^{(k)}$ le polynôme obtenu en dérivant k fois le polynôme P.

Théorème 3 : Propriétés de la dérivation de polynômes

- $\forall \lambda, \mu \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X]$, $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$ et $(PQ)' = P'Q + PQ'$
- Un polynôme a une dérivée nulle si et seulement si c'est un polynôme constant.
- $\forall P \in \mathbb{K}[X]$ tel que $\deg P \geq 1$, on a $\deg P' = \deg P - 1$.
- Pour tous $P, Q \in \mathbb{K}[X]$, $(P \circ Q)' = Q' \times P' \circ Q$

Démonstration :

• Posons $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$. On a $PQ = \sum_{k=0}^{2n} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k$,
donc $(PQ)' = \sum_{k=1}^{2n} k \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^{k-1} = \sum_{k=0}^{2n-1} (k+1) \left(\sum_{i=0}^{k+1} a_i b_{k+1-i}\right) X^k$.
D'autre part, $P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$ et de même $Q' = \sum_{k=0}^{n-1} (k+1) b_{k+1} X^k$,
donc $P'Q = \sum_{k=0}^{2n-1} \left(\sum_{j=0}^{k} (j+1) a_{j+1} b_{k-j}\right) X^k$ et $PQ' = \sum_{k=0}^{2n-1} \left(\sum_{j=0}^{k} a_j (k-j+1) b_{k-j+1}\right) X^k$.
Or $\sum_{j=0}^{k} (j+1) a_{j+1} b_{k-j} + \sum_{j=0}^{k} a_j (k-j+1) b_{k-j+1} = \sum_{j=1}^{k+1} j a_j b_{k-j+1} + \sum_{j=0}^{k} a_j (k-j+1) b_{k-j+1} =$
$(k+1) a_{k+1} b_0 + \sum_{j=1}^{k} (k+1) a_j b_{k+1-j} + a_0 b_{k+1} = (k+1) \sum_{i=0}^{k+1} a_i b_{k+1-i}$ donc $P'Q + PQ' = (PQ)'$.
• $P' = 0 \Leftrightarrow \forall k \in [\![0, n]\!],\ k a_k = 0 \Leftrightarrow \forall k \in [\![1, n]\!],\ a_k = 0 \Leftrightarrow P$ est un polynôme constant.
• Dès lors que $n \geq 1$, le terme de plus haut degré de P est $a_n X^n$ et le terme de plus haut degré de P' est $n a_n X^{n-1}$.
• Pour tout polynôme $Q \in \mathbb{K}[X]$,
montrons par récurrence que pour tout $k \in \mathbb{N}^*$, $\mathcal{P}_k$: « $\left(Q^k\right)' = kQ'Q^{k-1}$ ».
<u>Initialisation</u> : Pour $k = 1$, cela repose sur la convention $Q^0 = 1$, et pour $k = 2$, on a d'après ce qui précède $(Q \times Q)' = Q'Q + QQ' = 2Q'Q$.
<u>Hérédité</u> : Pour tout $k \in \mathbb{N}^*$, on suppose que $\left(Q^k\right)' = kQ'Q^{k-1}$
Alors $\left(Q^{k+1}\right)' = \left(Q \times Q^k\right)' = Q' \times Q^k + Q \times kQ'Q^{k-1} = (k+1)Q'Q^k$
<u>Conclusion</u> : D'après le principe de récurrence, $\mathcal{P}_k$ est vraie pour tout $k \in \mathbb{N}^*$.
Par conséquent, $(P \circ Q)' = \left(\sum_{k=0}^{n} a_k Q^k\right)' = \sum_{k=0}^{n} a_k \left(Q^k\right)' = \sum_{k=0}^{n} k a_k Q' Q^{k-1} = Q' \times P' \circ Q$.

Théorème 4 : Formule de Taylor

Pour tout polynôme $P \in \mathbb{K}[X]$ et pour tout $a \in \mathbb{K}$,

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

Remarques :

▷ En particulier, pour $a = 0$, $P = \sum_{k=0}^{\deg P} \frac{P^{(k)}(0)}{k!} X^k$,

et donc pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k$, on a $a_k = \frac{P^{(k)}(0)}{k!}$.

Démonstration :
Montrons par récurrence sur $n \in \mathbb{N}$ la propriété :

$$\mathcal{P}_n : \quad \forall P \in \mathbb{K}_n[X],\ \forall a \in \mathbb{K},\ P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Initialisation : Pour $n = 0$, pour tout polynôme constant $P = a_0$, on a $P^{(k)} = 0$ pour tout $k \geq 1$, donc pour tout $a \in \mathbb{K}$, $\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = P(a) = a_0 = P$.
Hérédité : Pour tout $n \in \mathbb{N}$, on suppose que $\mathcal{P}_n$ est vraie. Soit $P \in \mathbb{K}_{n+1}[X]$.
Alors $P' \in \mathbb{K}_n[X]$, donc, par hypothèse de récurrence, $P' = \sum_{k=0}^{n} \frac{P'^{(k)}(a)}{k!}(X-a)^k$.
Considérons le polynôme $B = \sum_{k=0}^{n+1} \frac{P^{(k+1)}(a)}{(k+1)!}(X-a)^{k+1}$. On a $B' = P'$, donc $\exists C \in \mathbb{K}$, tel que $P = B + C$. Mais alors $P(a) = B(a) + C$, c'est-à-dire que $C = P(a)$.
Finalement $P = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{(k+1)!}(X-a)^{k+1} + P(a) = \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!}(X-a)^k$
Conclusion : D'après le principe de récurrence, la propriété $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}$.

IV Racines d'un polynôme

Définition 6

Étant donnés $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$, on dit que α est une **racine**, ou un **zéro**, du polynôme P, lorsque $P(\alpha) = 0$.

Exemple :
- ▷ 2 est une racine du polynôme $X^3 + X^2 - 4X - 4$.
- ▷ Le polynôme $X^2 + 1$ n'a pas de racine lorsqu'il est considéré comme un polynôme de $\mathbb{R}[X]$, mais il en a deux lorsqu'il est considéré comme un polynôme de $\mathbb{C}[X]$.

Théorème 5

Étant donnés $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$,
$\alpha \in \mathbb{K}$ est une racine de P si et seulement si le polynôme $(X - \alpha)$ divise P.

Démonstration :
Faisons la division euclidienne de P par $(X - \alpha)$: $\exists B, Q \in \mathbb{K}[X]$, $P = (X - \alpha)B + Q$ et $\deg Q < 1$, c'est-à-dire que Q est un polynôme constant.
Donc $P(\alpha) = 0 \Leftrightarrow Q = 0 \Leftrightarrow (X - \alpha)$ divise P.

Exemple :
- ▷ Factoriser $X^3 + X^2 - 4X - 4$ par $X - 2$.

Théorème 6 (admis)

Étant donné $P \in \mathbb{K}[X]$. Le nombre de racines de P est au maximum $\deg P$.

Définition 7 : Multiplicité d'une racine

Étant donnée une racine α d'un polynôme P, on appelle multiplicité de la racine α le plus grand nombre entier k tel que $(X-\alpha)^k$ divise P.

Théorème 7

α est une racine du polynôme P de multiplicité k si et seulement si
$\exists B \in \mathbb{K}[X],\ P=(X-\alpha)^k B$ et $B(\alpha)\neq 0$.

Démonstration :
Implication : Supposons que α soit une racine du polynôme P de multiplicité k.
Alors $\exists B \in \mathbb{K}[X],\ P=(X-\alpha)^k B$. Montrons que $B(\alpha)\neq 0$:
si $B(\alpha)=0$, alors $(X-\alpha)$ divise B, c'est-à-dire que $\exists C \in \mathbb{K}[X],\ B=(X-\alpha)C$ et donc $P=(X-\alpha)^{k+1}C$ et donc α est de multiplicité $k+1$, ce qui est faux.
Réciproque : Supposons que $\exists B \in \mathbb{K}[X],\ P=(X-\alpha)^k B$ et $B(\alpha)\neq 0$.
Alors clairement α est une racine de P d'ordre au moins k. Montrons qu'elle n'est pas racine d'ordre $k+1$: si elle l'était, on aurait $P=(X-\alpha)^{k+1}C$ avec $C\in\mathbb{K}[X]$. Mais alors $(X-\alpha)^k B=(X-\alpha)^{k+1}C$, donc $B=(X-\alpha)C$, donc $B(\alpha)=0$, ce qui est faux.

Exemple :

- ▷ 1 est une racine double du polynôme X^3-X^2-X+1 car $X^3-X^2-X+1=(X-1)^2(X+1)$

Théorème 8

Étant donnée une racine α d'un polynôme P,
α est de multiplicité k si et seulement si $\forall j\in[\![0,k-1]\!],\ P^{(j)}(\alpha)=0$ et $P^{(k)}(\alpha)\neq 0$.

Démonstration :
Implication : Supposons que α soit de multiplicité k.
Alors $\exists B \in \mathbb{K}[X],\ P=(X-\alpha)^k B$ et $B(\alpha)\neq 0$.
On montre alors par récurrence que :

$$\forall j\in[\![0,k]\!],\ P^{(j)}(X)=\sum_{i=0}^{j}\frac{k!}{(k-j+i)!}\binom{j}{i}(X-\alpha)^{k-j+i}B^{(i)}(X).$$

Donc on a bien $P^{(j)}(\alpha)=0$ pour tout $j\in[\![0,k-1]\!]$, et $P^{(k)}(\alpha)=k!\times B(\alpha)\neq 0$.
Réciproque : On suppose désormais que $\forall j\in[\![0,k-1]\!],\ P^{(j)}(\alpha)=0$ et $P^{(k)}(\alpha)\neq 0$.
Appliquons la formule de Taylor :

$$P=\sum_{j=k}^{\deg P}\frac{P^{(j)}(\alpha)}{j!}(X-\alpha)^j=(X-\alpha)^k\sum_{j=0}^{\deg P-k}\frac{P^{(j+k)}(\alpha)}{(j+k)!}(X-\alpha)^j=(X-\alpha)^k B(X),$$

avec $B(X)=\sum_{j=0}^{\deg P-k}\frac{P^{(j+k)}(\alpha)}{(j+k)!}(X-\alpha)^j$ et donc $B(\alpha)=\dfrac{P^{(k)}(\alpha)}{k!}\neq 0$,
donc α est une racine de multiplicité k de P.

Définition 8 : Polynôme irréductible

Un polynôme $P\in\mathbb{K}[X]$ est dit irréductible lorsqu'il n'est pas constant et que ses seuls diviseurs sont les polynômes de la forme λP avec $\lambda\in\mathbb{K}$.

Exemple :

- ▷ Le polynôme X^2+X+1 est irréductible dans $\mathbb{R}[X]$: ses seuls diviseurs sont les constantes et les polynômes de la forme $\lambda(X^2+X+1)$ avec $\lambda \in \mathbb{R}$.

Définition 9 : Polynôme scindé

Un polynôme P est dit scindé lorsqu'il s'écrit sous la forme $C\prod_{i=1}^{n}(X-\alpha_i)$, où C et les α_i sont des éléments de $\mathbb{K}$.

Remarque :

- ▷ X^2+X+1 est scindé dans $\mathbb{C}[X]$, égal à $(X-j)(X-j^2)$, avec $j=e^{\frac{2i\pi}{3}}$, mais pas dans $\mathbb{R}[X]$ où il est irréductible.

Théorème 9 : Théorème de d'Alembert-Gauss (admis)

Tous les polynômes de $\mathbb{C}[X]$ sont scindés. C'est-à-dire que les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Corollaire

Tout polynôme de $\mathbb{R}[X]$ peut s'écrire sous la forme d'un produit de polynômes à coefficients réels de degrés un ou deux. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré 2 qui ont un discriminant strictement négatif.

Exemple :

- ▷ Dans $\mathbb{C}[X]$, $X^5-1=\prod_{k=0}^{4}\left(X-e^{\frac{2ik\pi}{5}}\right)$

  Dans $\mathbb{R}[X]$, $X^5-1=(X-1)\left(X^2-\frac{\sqrt{5}-1}{2}X+1\right)\left(X^2+\frac{\sqrt{5}+1}{2}X+1\right)$

Démonstration :
Soit $P\in\mathbb{R}[X]$.
On peut considérer P comme un polynôme de $\mathbb{C}[X]$. Donc $P=C\prod_{i=1}^{n}(X-\alpha_i)$.
C est le coefficient de X^n, donc $C\in\mathbb{R}$.
Pour chaque valeur de i,
- soit α_i est un nombre réel ,
- soit α_i est un nombre complexe non réel. Dans ce deuxième cas, comme les coefficients de P sont tous des nombres réels, $P(\overline{\alpha_i})=\overline{P(\alpha_i)}=0$, donc $\overline{\alpha_i}$ est aussi une racine de P. Mais alors $(X-\alpha_i)(X-\overline{\alpha_i})=X^2-2\text{Re }(\alpha_i)X+|\alpha_i|^2$ est un polynôme du deuxième degré à coefficients réels.

Théorème 11

Soit $P=\sum_{k=0}^{n}a_kX^k$ un polynôme scindé unitaire de $\mathbb{K}[X]$ de degré n.

On a $P=\prod_{i=1}^{n}(X-\alpha_i)$, où les $\alpha_i\in\mathbb{K}$ sont les n racines de P.

Donc $a_0=(-1)^n\prod_{i=1}^{n}\alpha_i$ et $a_{n-1}=-\sum_{k=1}^{n}\alpha_i$.