Chapitre 10 : Les polynômes

Dr Nicolas Provost - PCSI1 - LMB

Dans ce chapitre les polynômes sont à coefficients dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 L'algèbre de polynômes

Définition. *Pour toute suite de coefficients $(a_n)_{n\geq 0} \in \mathbb{K}^{\mathbb{N}}$ qui stationne en 0, on définit un polynôme $P(X) = \sum_{n\in\mathbb{N}} a_n X^n$. On note $\mathbb{K}[X]$ l'ensemble des polynômes. On note $0_{\mathbb{K}[X]}$ le polynôme nul.*
Si $P \neq 0_{\mathbb{K}[X]}$, on appelle degré de P et on note $\deg(P)$ le dernier rang N tel que $a_N \neq 0$.
Le coefficient $a_{\deg(P)}$ est appelé coefficient dominant du polynôme.
On dit que le polynôme est unitaire lorsque $a_{\deg(P)} = 1$.
Si $Q(X) = \sum_{n\in\mathbb{N}} b_n X^n$ est un autre polynôme alors on dispose des opérations :

$$(\lambda P + \mu Q)(X) = \sum_{n\in\mathbb{N}} (\lambda a_n + \mu b_n) X^n. \qquad \text{(Combinaison linéaire)}$$

$$(PQ)(X) = \sum_{n\in\mathbb{N}} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n. \qquad \text{(Produit)}$$

⊗ On en déduit le passage à la puissance par récurrence sur le produit :

$$P^0(X) = 1 \text{ et } \forall n \in \mathbb{N}, P^{n+1}(X) = P^n(X)P(X). \qquad \text{(Puissance)}$$

On obtient également la composée comme combinaison linéaire des puissances par :

$$(P \circ Q)(X) = \sum_{n\in\mathbb{N}} a_n Q^n(X). \qquad \text{(Composée)}$$

Proposition 1.1. *On dispose des formules sur les degrés :*

- **a)** $\deg(\lambda P + \mu Q) \leq \max(\deg(P), \deg(Q))$ *avec égalité si* $\deg(P) \neq \deg(Q)$.
- **b)** $\deg(PQ) = \deg(P) + \deg(Q)$ *et* $\deg(P^n) = n \deg(P)$.
- **c)** *Si Q est non constant,* $\deg(P \circ Q) = \deg(P)\deg(Q)$.

⊗ On note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \text{ tel que } \deg(P) \leq n\}$ l'ensemble des polynômes de degré inférieure ou égale à n. Cet ensemble est stable par combinaison linéaire.

2 Arithmétique sur $\mathbb{K}[X]$

Théorème 2.1. *Pour tout couple $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :*

$$A = BQ + R \text{ avec } \deg(R) < \deg(B). \qquad (1)$$

Le polynôme Q s'appelle le quotient de la division euclidienne et R est le reste.

Définition. *On dit que B divise A et on note $B|A$ si le reste dans la division euclidienne est nul.*

⊗ On restreint le plus souvent la divisibilité au cas des polynômes unitaires.
En effet, $B|A \Leftrightarrow cB|A$ pour tout coefficient $c \in \mathbb{K}^*$.

Définition. *Pour $A, B \in \mathbb{K}(X)$, on définit leur Plus Grand Diviseur Commun comme étant l'unique polynôme unitaire noté $PGCD(A,B) \in \mathbb{K}[X]^*$ vérifiant :*

$$\begin{cases} PGCD(A,B)|A \text{ et } PGCD(A,B)|B \\ \forall D \in \mathbb{K}[X]^*, (D|A \text{ et } D|B) \Rightarrow D|PGCD(A,B). \end{cases}$$

Théorème 2.2 (Algorithme d'Euclide)**.** *On effectue les divisions euclidiennes successives des restes $R_n = Q_n R_{n+1} + R_{n+2}$ avec $R_0 = A$ et $R_1 = B$. Le dernier reste non nul est $PGCD(A,B)$.*

Définition. *On dit que A et B sont premiers entre eux si $PGCD(A,B) = 1$.*

Théorème 2.3 (Bézout)**.** *A et B sont premiers entre eux ssi il existe $U, V \in \mathbb{K}[X]$ tel que $AU + BV = 1$.*

$\otimes$ On obtient en particulier $A\mathbb{K}[X] + B\mathbb{K}[X] = PGCD(A,B)\mathbb{K}[X]$.

Théorème 2.4 (Gauss)**.** *Si D divise AB et si D est premier avec A alors D divise B.*

Définition. *On dit qu'un polynôme unitaire P est un polynôme irréductible si P admet exactement deux diviseurs unitaires 1 et P.*

3 Racine d'un polynôme

Définition. *On dit que $\alpha \in \mathbb{K}$ est une racine de P si $P(\alpha) = 0$. On note $Rac_{\mathbb{K}}(P)$ l'ensemble des racines de P dans $\mathbb{K}$.*

Théorème 3.1. *Le nombre α est une racine de P ssi $(X - \alpha)|P$.*

Définition. *On définit la multiplicité d'une racine α de P et on note $\mathrm{mult}_\alpha(P)$ le plus grand $m \in \mathbb{N}$ tel que $(X - \alpha)^m|P$.*

Proposition 3.2. *Soient P, Q deux polynômes. On a :*

a) $\mathrm{mult}_\alpha(\lambda P + \mu Q) \geq \min(\mathrm{mult}_\alpha(P), \mathrm{mult}_\alpha(Q))$, *avec égalité si* $\mathrm{mult}_\alpha(P) \neq \mathrm{mult}_\alpha(Q)$.
b) $\mathrm{mult}_\alpha(PQ) = \mathrm{mult}_\alpha(P) + \mathrm{mult}_\alpha(Q)$.
c) $\mathrm{mult}_\alpha(P^n) = n \times \mathrm{mult}_\alpha(P)$.

Théorème 3.3. *Pour tout polynôme P non nul, on a :*

$$\sum_{\alpha \in Rac_{\mathbb{K}}(P)} \mathrm{mult}_\alpha(P) \leq \deg(P). \tag{2}$$

Corollaire 3.4. *Si P est non nul alors il admet au plus $\deg(P)$ racines.*

$\otimes$ Si $P \in \mathbb{K}_n[X]$ admet au moins $(n+1)$ racines alors P est le polynôme nul.

Définition. *On dit qu'un polynôme non nul est scindé sur $\mathbb{K}$ si $\sum_{\alpha \in Rac_{\mathbb{K}}(P)} \mathrm{mult}_\alpha(P) = \deg(P)$.*

4 Dérivation formelle sur $\mathbb{K}[X]$

Définition. *Pour tout polynôme $P(X) = \sum_{k \in \mathbb{N}} a_k X^k$, on définit sa dérivée formelle comme étant le polynôme :*

$$DP = P'(X) = \sum_{k \in \mathbb{N}} (k+1) a_{k+1} X^k. \tag{dérivée formelle}$$

On définit les dérivées n-ième par récurrence avec $D^0 P = P$ et $D^{n+1} P = D(D^n P)$.

Proposition 4.1. *On dispose des formules de calcul de dérivées :*

$$D^n(\lambda P + \mu Q) = \lambda D^n P + \mu D^n Q \tag{Linéarité}$$

$$D^n(P \times Q) = \sum_{k=0}^{n} \binom{n}{k} (D^k P) \times (D^{n-k} Q) \tag{Formule de Leibniz}$$

Théorème 4.2. *Soit a une racine de P. On a dispose de la caractérisation suivante de la multiplicité :*

$$\forall k < \mathrm{mult}_\alpha(P), D^k P(\alpha) = 0 \textit{ et } D^{\mathrm{mult}_\alpha(P)} P(\alpha) \neq 0. \tag{3}$$

$\otimes$ En particulier, si α est une racine de P alors $\mathrm{mult}_\alpha(P) = \mathrm{mult}_\alpha(P') + 1$.

Théorème 4.3 (Formule de Taylor)**.** *Pour tout polynôme P non nul et $a \in \mathbb{K}$ un point quelconque, on a :*

$$P(X) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^k. \tag{4}$$

$\otimes$ Ceci est une formule exacte à ne pas confondre avec celle asymptotique de Taylor-Young.

5 Décomposition en facteurs irréductibles

Théorème 5.1 (d'Alembert-Gauss)**.** *Tout polynôme non constant admet une racine sur $\mathbb{C}$.*

Théorème 5.2. *Tout polynôme $P \in \mathbb{C}[X]^*$ est scindé sur $\mathbb{C}$ et admet une unique décomposition sous la forme :*

$$P(X) = a_{\deg(P)} \prod_{z \in Rac_{\mathbb{C}}(P)} (X-z)^{\mathrm{mult}_z(P)}. \tag{5}$$

$\otimes$ En particulier, on a $X^n - 1 = \prod_{\omega \in \mathbb{U}_n}(X - \omega)$.

Théorème 5.3. *Tout polynôme $P \in \mathbb{R}[X]$ se décompose de manière unique sur $\mathbb{R}$ sous la forme :*

$$P(X) = a_{\deg(P)} \prod_{r \in Rac_{\mathbb{R}}(P)} (X-r)^{\mathrm{mult}_r(P)} \prod_{\{z,\bar{z}\} \subset Rac_{\mathbb{C}}(P)} (X^2 - 2\mathrm{Re}(z)X + |z|^2)^{\mathrm{mult}_z(P)}. \tag{6}$$

$\otimes$ Un polynôme est scindé sur $\mathbb{R}$ s'il admet aucune racine complexe.

Proposition 5.4. *Si P est de degré n et est scindé alors on dispose des formules de somme et produit des racines :*

$$\sum_{\alpha \in Rac_{\mathbb{K}}(P)} \mathrm{mult}_\alpha(P)\alpha = -\frac{a_{n-1}}{a_n}, \tag{7}$$

$$\prod_{\alpha \in Rac_{\mathbb{K}}(P)} \alpha^{\mathrm{mult}_\alpha(P)} = (-1)^n \frac{a_0}{a_n}. \tag{8}$$