Polynômes

1. Définitions

Un ***polynôme*** à coefficients dans $\mathbb{K}$ ($\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$) est une expression :

$$P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$$

- Les $a_i \in \mathbb{K}$ sont appelés les ***coefficients*** du polynôme.
- Si $a_n \neq 0$, $n \in \mathbb{N}$ est le ***degré*** de P, noté $\deg P$. (Convention : le degré du polynôme nul est $-\infty$.)
- $\mathbb{K}[X]$ désigne l'ensemble des polynômes.
- $\mathbb{K}_n[X]$ est l'ensemble des polynômes de degré $\leqslant n$.
- Deux polynômes sont ***égaux*** si et seulement si ils ont les mêmes coefficients.

Multiplication. Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ et $Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$. $P \times Q$ est un polynôme de degré $n+m$ avec :

$$c_k = \sum_{i+j=k} a_ib_j \text{ pour } k \in \{0, \ldots, r\}.$$

$$\boxed{\deg(P \times Q) = \deg P + \deg Q \qquad \deg(P+Q) \leqslant \max(\deg P, \deg Q)}$$

- Les polynômes comportant un seul terme non nul (du type a_kX^k) sont appelés ***monômes***.
- Soit $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, un polynôme avec $a_n \neq 0$. On appelle ***terme dominant*** le monôme a_nX^n. Le coefficient a_n est appelé le ***coefficient dominant*** de P.
- Si le coefficient dominant est 1, on dit que P est un ***polynôme unitaire***.

2. Arithmétique des polynômes

Soient $A, B \in \mathbb{K}[X]$, on dit que B ***divise*** A s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B|A$. On dit aussi que A est multiple de B ou que A est divisible par B.

Théorème (Division euclidienne des polynômes). *Soient $A, B \in \mathbb{K}[X]$, avec $B \neq 0$, alors il existe un unique polynôme Q et il existe un unique polynôme R tels que :*

$$\boxed{A = BQ + R \quad \text{et} \quad \deg R < \deg B.}$$

Q est appelé le ***quotient*** et R le ***reste*** et cette écriture est la ***division euclidienne*** de A par B.
Notez que la condition $\deg R < \deg B$ signifie $R = 0$ ou bien $0 \leqslant \deg R < \deg B$.
Enfin $R = 0$ si et seulement si $B|A$.

Exemple. On pose une division de polynômes comme une division euclidienne de deux entiers. Par exemple si $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ et $B = X^2 - X + 1$. Alors on trouve $Q = 2X^2 + X - 3$ et $R = -X + 2$.

$$\begin{array}{rl|l}
 & 2X^4 - X^3 - 2X^2 + 3X - 1 & X^2 - X + 1 \\ \cline{3-3}
- & 2X^4 - 2X^3 + 2X^2 & \\ \cline{2-2}
 & X^3 - 4X^2 + 3X - 1 & 2X^2 + X - 3 \\
- & X^3 - X^2 + X & \\ \cline{2-2}
 & -3X^2 + 2X - 1 & \\
- & -3X^2 + 3X - 3 & \\ \cline{2-2}
 & -X + 2 &
\end{array}$$

Le ***pgcd*** (plus grand commun diviseur) de A et B est l'unique polynôme unitaire de plus grand degré qui divise à la fois A et B.
Algorithme d'Euclide. Soient A et B des polynômes, $B \neq 0$. Si $A = BQ + R$ alors $\mathrm{pgcd}(A, B) = \mathrm{pgcd}(B, R)$. On calcule des divisions euclidiennes successives,

$$\begin{array}{ll}
A = BQ_1 + R_1 & \deg R_1 < \deg B \\
B = R_1Q_2 + R_2 & \deg R_2 < \deg R_1 \\
R_1 = R_2Q_3 + R_3 & \deg R_3 < \deg R_2 \\
\ldots &
\end{array}$$

Le degré du reste diminue à chaque division. Le pgcd est le dernier reste non nul R_k (rendu unitaire).
A et B sont ***premiers entre eux*** si $\mathrm{pgcd}(A, B) = 1$. Pour A, B quelconques on peut se ramener à des polynômes premiers entre eux : si $\mathrm{pgcd}(A, B) = D$ alors A et B s'écrivent : $A = DA'$, $B = DB'$ avec $\mathrm{pgcd}(A', B') = 1$.

Théorème (de Bézout). *Soient $A, B \in \mathbb{K}[X]$ des polynômes avec $A \neq 0$ ou $B \neq 0$. On note $D = \mathrm{pgcd}(A, B)$. Il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$.*

Corollaire. *Soient A et B deux polynômes. A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $AU + BV = 1$.*

Corollaire. *Soient $A, B, C \in \mathbb{K}[X]$ avec $A \neq 0$ ou $B \neq 0$. Si $C|A$ et $C|B$ alors $C|\mathrm{pgcd}(A, B)$.*

Corollaire (Lemme de Gauss). *Soient $A, B, C \in \mathbb{K}[X]$. Si $A|BC$ et $\mathrm{pgcd}(A, B) = 1$ alors $A|C$.*

3. Racine d'un polynôme, factorisation

$\alpha \in \mathbb{K}$ est une ***racine*** (ou un ***zéro***) de $P \in \mathbb{K}[X]$ si $P(\alpha) = 0$.

$$\boxed{P(\alpha) = 0 \quad \iff \quad X - \alpha \text{ divise } P}$$

α est une ***racine de multiplicité k*** de P est équivalent à l'une des propriétés suivantes :

(i) $P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$.
(ii) Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^kQ$, avec $Q(\alpha) \neq 0$.
(iii) $(X - \alpha)^k$ divise P alors que $(X - \alpha)^{k+1}$ ne divise pas P.

Théorème (Théorème de d'Alembert-Gauss). *Tout polynôme à coefficients complexes de degré $n \geqslant 1$ a au moins une racine dans $\mathbb{C}$. Il admet exactement n racines si on compte chaque racine avec multiplicité.*

Exemple. Soit $P(X) = aX^2 + bX + c$ de degré 2 à coefficients a, b, c réels.

- Si $\Delta = b^2 - 4ac > 0$, P a 2 racines réelles distinctes $\frac{-b \pm \sqrt{\Delta}}{2a}$.
- Si $\Delta < 0$, P a 2 racines complexes conjuguées $\frac{-b \pm \mathrm{i}\sqrt{|\Delta|}}{2a}$.
- Si $\Delta = 0$ P a une racine réelle double $\frac{-b}{2a}$.

Polynômes irréductibles

- Un polynôme ***irréductible*** P est donc un polynôme non constant dont les seuls diviseurs de P sont les constantes ou P lui-même (à une constante multiplicative près). Cela correspond à la notion de nombre premier pour l'arithmétique de $\mathbb{Z}$.
- Dans le cas contraire, P est ***réductible*** : il existe $A, B \in \mathbb{K}[X]$ tels que $P = AB$, avec $\deg A \geqslant 1$ et $\deg B \geqslant 1$.

Théorème (Factorisation sur $\mathbb{C}$ et $\mathbb{R}$).

1. *Tout polynôme unitaire s'écrit de manière unique comme un produit de polynômes irréductibles unitaires.*
2. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
   Tout $P \in \mathbb{C}[X]$ se factorise en produit de polynômes de degré 1 dans $\mathbb{C}[X]$.
3. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 ayant un discriminant $\Delta < 0$.*
   Tout $P \in \mathbb{C}[X]$ se factorise en produit de polynômes irréductibles de degré 1 ou 2 dans $\mathbb{C}[X]$.

Exemple. Soit $P(X) = X^4 + 1$.

- Sur $\mathbb{C}$. D'abord $P(X) = (X^2 + \mathrm{i})(X^2 - \mathrm{i})$. Les racines de P sont les racines carrées complexes de i et $-\mathrm{i}$. Ainsi P se factorise dans $\mathbb{C}[X]$:
$$P(X) = \left(X - \tfrac{\sqrt{2}}{2}(1+\mathrm{i})\right)\left(X + \tfrac{\sqrt{2}}{2}(1+\mathrm{i})\right)\left(X - \tfrac{\sqrt{2}}{2}(1-\mathrm{i})\right)\left(X + \tfrac{\sqrt{2}}{2}(1-\mathrm{i})\right)$$
- Sur $\mathbb{R}$ on regroupe les facteurs ayant des racines conjuguées :
$$P(X) = \left[X^2 + \sqrt{2}X + 1\right]\left[X^2 - \sqrt{2}X + 1\right]$$

4. Fractions rationnelles

Une ***fraction rationnelle*** à coefficients dans $\mathbb{K}$ est une expression de la forme $F = \frac{P}{Q}$ où $P, Q \in \mathbb{K}[X]$ sont deux polynômes et $Q \neq 0$.

Théorème (Décomposition en éléments simples sur $\mathbb{C}$). *Soit P/Q une fraction rationnelle avec $P, Q \in \mathbb{C}[X]$, $\mathrm{pgcd}(P, Q) = 1$ et $Q = (X - \alpha_1)^{k_1} \cdots (X - \alpha_r)^{k_r}$. Alors il existe une et une seule écriture :*

$$\begin{aligned}
\frac{P}{Q} = E(X) \quad & + \frac{a_{1,1}}{(X-\alpha_1)^{k_1}} + \frac{a_{1,2}}{(X-\alpha_1)^{k_1-1}} + \cdots + \frac{a_{1,k_1}}{(X-\alpha_1)} \\
& + \frac{a_{2,1}}{(X-\alpha_2)^{k_2}} + \cdots + \frac{a_{2,k_2}}{(X-\alpha_2)} + \cdots
\end{aligned}$$

Le polynôme E s'appelle la ***partie polynomiale*** (ou ***partie entière***). Les termes $\frac{a}{(X-\alpha)^i}$ sont les ***éléments simples*** sur $\mathbb{C}$.

Théorème (Décomposition en éléments simples sur $\mathbb{R}$). *Soit P/Q une fraction rationnelle avec $P, Q \in \mathbb{R}[X]$, $\mathrm{pgcd}(P, Q) = 1$. Alors P/Q s'écrit de manière unique comme somme :*

- *d'une partie polynomiale $E(X)$,*
- *d'éléments simples du type $\frac{a}{(X-\alpha)^i}$,*
- *d'éléments simples du type $\frac{aX+b}{(X^2+\alpha X+\beta)^i}$,*

où les $X - \alpha$ et $X^2 + \alpha X + \beta$ sont les facteurs irréductibles de $Q(X)$ et les exposants i sont inférieurs ou égaux à la puissance correspondante dans cette factorisation.