

# Module Mathématiques I : Algèbre I

## Filière: Cycle Préparatoire Sciences et Techniques Pour l'Ingénieur (STPI)

# Chapitre : Polynôme et Fractions

## 1. Définitions

### 1.1. Définitions

#### Définition 1.

Un **polynôme** à coefficients dans  $\mathbb{K}$  est une expression de la forme

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_2 X^2 + a_1 X + a_0,$$

avec  $n \in \mathbb{N}$  et  $a_0, a_1, \dots, a_n \in \mathbb{K}$ .

L'ensemble des polynômes est noté  $\mathbb{K}[X]$ .

- Les  $a_i$  sont appelés les **coefficients** du polynôme.
- Si tous les coefficients  $a_i$  sont nuls,  $P$  est appelé le **polynôme nul**, il est noté 0.
- On appelle le **degré** de  $P$  le plus grand entier  $i$  tel que  $a_i \neq 0$ ; on le note  $\deg P$ . Pour le degré du polynôme nul on pose par convention  $\deg(0) = -\infty$ .
- Un polynôme de la forme  $P = a_0$  avec  $a_0 \in \mathbb{K}$  est appelé un **polynôme constant**. Si  $a_0 \neq 0$ , son degré est 0.

#### Exemple 1.

- $X^3 - 5X + \frac{3}{4}$  est un polynôme de degré 3.
- $X^n + 1$  est un polynôme de degré  $n$ .

- 2 est un polynôme constant, de degré 0.

## 1.2. Opérations sur les polynômes

- **Égalité.** Soient  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  et  $Q = b_n X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0$  deux polynômes à coefficients dans  $\mathbb{K}$ .

$$P = Q \iff \forall i \quad a_i = b_i$$

et on dit que  $P$  et  $Q$  sont égaux.

- **Addition.** Soient  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  et  $Q = b_n X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0$ . On définit :

$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \dots + (a_1 + b_1)X + (a_0 + b_0)$$

- **Multiplication.** Soient  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  et  $Q = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ . On définit

$$P \times Q = c_r X^r + c_{r-1} X^{r-1} + \dots + c_1 X + c_0$$

$$\text{avec } r = n + m \text{ et } c_k = \sum_{i+j=k} a_i b_j \text{ pour } k \in \{0, \dots, r\}.$$

- **Multiplication par un scalaire.** Si  $\lambda \in \mathbb{K}$  alors  $\lambda \cdot P$  est le polynôme dont le  $i$ -ème coefficient est  $\lambda a_i$ .

### Exemple 2.

- Soient  $P = aX^3 + bX^2 + cX + d$  et  $Q = \alpha X^2 + \beta X + \gamma$ . Alors  $P + Q = aX^3 + (b + \alpha)X^2 + (c + \beta)X + (d + \gamma)$ ,  $P \times Q = (a\alpha)X^5 + (a\beta + b\alpha)X^4 + (a\gamma + b\beta + c\alpha)X^3 + (b\gamma + c\beta + d\alpha)X^2 + (c\gamma + d\beta)X + d\gamma$ . Enfin  $P = Q$  si et seulement si  $a = 0$ ,  $b = \alpha$ ,  $c = \beta$  et  $d = \gamma$ .
- La multiplication par un scalaire  $\lambda \cdot P$  équivaut à multiplier le polynôme constant  $\lambda$  par le polynôme  $P$ .

L'addition et la multiplication se comportent sans problème :

#### Proposition 1.

Pour  $P, Q, R \in \mathbb{K}[X]$  alors

- $0 + P = P$ ,  $P + Q = Q + P$ ,  $(P + Q) + R = P + (Q + R)$ ;
- $1 \cdot P = P$ ,  $P \times Q = Q \times P$ ,  $(P \times Q) \times R = P \times (Q \times R)$ ;
- $P \times (Q + R) = P \times Q + P \times R$ .

Pour le degré il faut faire attention :

#### Proposition 2.

Soient  $P$  et  $Q$  deux polynômes à coefficients dans  $\mathbb{K}$ .

$$\deg(P \times Q) = \deg P + \deg Q$$

$$\deg(P + Q) \leq \max(\deg P, \deg Q)$$

On note  $\mathbb{R}_n[X] = \{P \in \mathbb{R}[X] \mid \deg P \leq n\}$ . Si  $P, Q \in \mathbb{R}_n[X]$  alors  $P + Q \in \mathbb{R}_n[X]$ .

## 1.3. Vocabulaire

Complétons les définitions sur les polynômes.

#### Définition 2.

- Les polynômes comportant un seul terme non nul (du type  $a_k X^k$ ) sont appelés **monômes**.
- Soit  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ , un polynôme avec  $a_n \neq 0$ . On appelle **terme dominant** le monôme  $a_n X^n$ . 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**.

### Exemple 3.

$P(X) = (X - 1)(X^n + X^{n-1} + \dots + X + 1)$ . On développe cette expression :  $P(X) = (X^{n+1} + X^n + \dots + X^2 + X) - (X^n + X^{n-1} + \dots + X + 1) = X^{n+1} - 1$ .  $P(X)$  est donc un polynôme de degré  $n + 1$ , il est unitaire et est somme de deux monômes :  $X^{n+1}$  et  $-1$ .

**Remarque.**

Tout polynôme est donc une somme finie de monômes.

**Mini-exercices.**

1. Soit  $P(X) = 3X^3 - 2$ ,  $Q(X) = X^2 + X - 1$ ,  $R(X) = aX + b$ . Calculer  $P + Q$ ,  $P \times Q$ ,  $(P + Q) \times R$  et  $P \times Q \times R$ . Trouver  $a$  et  $b$  afin que le degré de  $P - QR$  soit le plus petit possible.
2. Calculer  $(X + 1)^5 - (X - 1)^5$ .
3. Déterminer le degré de  $(X^2 + X + 1)^n - aX^{2n} - bX^{2n-1}$  en fonction de  $a, b$ .
4. Montrer que si  $\deg P \neq \deg Q$  alors  $\deg(P + Q) = \max(\deg P, \deg Q)$ . Donner un contre-exemple dans le cas où  $\deg P = \deg Q$ .
5. Montrer que si  $P(X) = X^n + a_{n-1}X^{n-1} + \dots$  alors le coefficient devant  $X^{n-1}$  de  $P(X - \frac{a_{n-1}}{n})$  est nul.

## 2. Arithmétique des polynômes

Il existe de grandes similitudes entre l'arithmétique dans  $\mathbb{Z}$  et l'arithmétique dans  $\mathbb{K}[X]$ . Cela nous permet d'aller assez vite et d'omettre certaines preuves.

### 2.1. Division euclidienne

**Définition 3.**

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  $B$ .

Outre les propriétés évidentes comme  $A|A$ ,  $1|A$  et  $A|0$  nous avons :

**Proposition 3.**

Soient  $A, B, C \in \mathbb{K}[X]$ .

1. Si  $A|B$  et  $B|A$ , alors il existe  $\lambda \in \mathbb{K}^*$  tel que  $A = \lambda B$ .
2. Si  $A|B$  et  $B|C$  alors  $A|C$ .
3. Si  $C|A$  et  $C|B$  alors  $C|(AU + BV)$ , pour tout  $U, V \in \mathbb{K}[X]$ .

**Théorème 1** (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 :

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

$Q$  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  $0 \leq \deg R < \deg B$ .

Enfin  $R = 0$  si et seulement si  $B|A$ .

*Démonstration.*

**Unicité.** Si  $A = BQ + R$  et  $A = BQ' + R'$ , alors  $B(Q - Q') = R' - R$ . Or  $\deg(R' - R) < \deg B$ . Donc  $Q' - Q = 0$ . Ainsi  $Q = Q'$ , d'où aussi  $R = R'$ .

**Existence.** On montre l'existence par récurrence sur le degré de  $A$ .

- Si  $\deg A = 0$  et  $\deg B > 0$ , alors  $A$  est une constante, on pose  $Q = 0$  et  $R = A$ . Si  $\deg A = 0$  et  $\deg B = 0$ , on pose  $Q = A/B$  et  $R = 0$ .
- On suppose l'existence vraie lorsque  $\deg A \leq n - 1$ . Soit  $A = a_n X^n + \dots + a_0$  un polynôme de degré  $n$  ( $a_n \neq 0$ ). Soit  $B = b_m X^m + \dots + b_0$  avec  $b_m \neq 0$ . Si  $n < m$  on pose  $Q = 0$  et  $R = A$ .  
Si  $n \geq m$  on écrit  $A = B \cdot \frac{a_n}{b_m} X^{n-m} + A_1$  avec  $\deg A_1 \leq n - 1$ . On applique l'hypothèse de récurrence à  $A_1$  : il existe  $Q_1, R_1 \in \mathbb{K}[X]$  tels que  $A_1 = BQ_1 + R_1$  et  $\deg R_1 < \deg B$ . Il vient :

$$A = B \left( \frac{a_n}{b_m} X^{n-m} + Q_1 \right) + R_1.$$

Donc  $Q = \frac{a_n}{b_m} X^{n-m} + Q_1$  et  $R = R_1$  conviennent.

□

**Exemple 4.**

On pose une division de polynômes comme on pose 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  $R = -X + 2$ . On n'oublie pas de vérifier qu'effectivement  $A = BQ + R$ .

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

**Exemple 5.**

Pour  $X^4 - 3X^3 + X + 1$  divisé par  $X^2 + 2$  on trouve un quotient égal à  $X^2 - 3X - 2$  et un reste égale à  $7X + 5$ .

$$\begin{array}{r|l}
 X^4 - 3X^3 + X + 1 & X^2 + 2 \\
 - X^4 + 2X^2 & \hline
 \hline
 -3X^3 - 2X^2 + X + 1 & X^2 - 3X - 2 \\
 - -3X^3 - 6X & \\
 \hline
 -2X^2 + 7X + 1 & \\
 - -2X^2 - 4 & \\
 \hline
 7X + 5 & 
 \end{array}$$

**2.2. pgcd****Proposition 4.**

Soient  $A, B \in \mathbb{K}[X]$ , avec  $A \neq 0$  ou  $B \neq 0$ . Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois  $A$  et  $B$ .

Cet unique polynôme est appelé le **pgcd** (plus grand commun diviseur) de  $A$  et  $B$  que l'on note  $\text{pgcd}(A, B)$ .

**Remarque.**

- $\text{pgcd}(A, B)$  est un polynôme unitaire.
- Si  $A|B$  et  $A \neq 0$ ,  $\text{pgcd}(A, B) = \frac{1}{\lambda}A$ , où  $\lambda$  est le coefficient dominant de  $A$ .
- Pour tout  $\lambda \in K^*$ ,  $\text{pgcd}(\lambda A, B) = \text{pgcd}(A, B)$ .
- Comme pour les entiers : si  $A = BQ + R$  alors  $\text{pgcd}(A, B) = \text{pgcd}(B, R)$ . C'est ce qui justifie l'algorithme d'Euclide.

**Algorithme d'Euclide.**

Soient  $A$  et  $B$  des polynômes,  $B \neq 0$ .

On calcule les divisions euclidiennes successives,

$$\begin{aligned}
A &= BQ_1 + R_1 & \deg R_1 < \deg B \\
B &= R_1Q_2 + R_2 & \deg R_2 < \deg R_1 \\
R_1 &= R_2Q_3 + R_3 & \deg R_3 < \deg R_2 \\
&\vdots \\
R_{k-2} &= R_{k-1}Q_k + R_k & \deg R_k < \deg R_{k-1} \\
R_{k-1} &= R_kQ_{k+1}
\end{aligned}$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul. Le pgcd est le dernier reste non nul  $R_k$  (rendu unitaire).

### Exemple 6.

Calculons le pgcd de  $A = X^4 - 1$  et  $B = X^3 - 1$ . On applique l'algorithme d'Euclide :

$$\begin{aligned}
X^4 - 1 &= (X^3 - 1) \times X + X - 1 \\
X^3 - 1 &= (X - 1) \times (X^2 + X + 1) + 0
\end{aligned}$$

Le pgcd est le dernier reste non nul, donc  $\text{pgcd}(X^4 - 1, X^3 - 1) = X - 1$ .

### Exemple 7.

Calculons le pgcd de  $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$  et  $B = X^4 + 2X^3 + X^2 - 4$ .

$$\begin{aligned}
X^5 + X^4 + 2X^3 + X^2 + X + 2 &= (X^4 + 2X^3 + X^2 - 4) \times (X - 1) + 3X^3 + 2X^2 + 5X - 2 \\
X^4 + 2X^3 + X^2 - 4 &= (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4) - \frac{14}{9}(X^2 + X + 2) \\
3X^3 + 2X^2 + 5X - 2 &= (X^2 + X + 2) \times (3X - 1) + 0
\end{aligned}$$

Ainsi  $\text{pgcd}(A, B) = X^2 + X + 2$ .

### Définition 4.

Soient  $A, B \in \mathbb{K}[X]$ . On dit que  $A$  et  $B$  sont **premiers entre eux** si  $\text{pgcd}(A, B) = 1$ .

Pour  $A, B$  quelconques on peut se ramener à des polynômes premiers entre eux : si  $\text{pgcd}(A, B) = D$  alors  $A$  et  $B$  s'écrivent :  $A = DA'$ ,  $B = DB'$  avec  $\text{pgcd}(A', B') = 1$ .

## 2.3. Théorème de Bézout

### Théorème 2 (Théorème de Bézout).

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

Ce théorème découle de l'algorithme d'Euclide et plus spécialement de sa remontée comme on le voit sur l'exemple suivant.

### Exemple 8.

Nous avons calculé  $\text{pgcd}(X^4 - 1, X^3 - 1) = X - 1$ . Nous remontons l'algorithme d'Euclide, ici il n'y avait qu'une ligne :  $X^4 - 1 = (X^3 - 1) \times X + X - 1$ , pour en déduire  $X - 1 = (X^4 - 1) \times 1 + (X^3 - 1) \times (-X)$ . Donc  $U = 1$  et  $V = -X$  conviennent.

### Exemple 9.

Pour  $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$  et  $B = X^4 + 2X^3 + X^2 - 4$  nous avons trouvé  $D = \text{pgcd}(A, B) = X^2 + X + 2$ . En partant de l'avant dernière ligne de l'algorithme d'Euclide on a d'abord :  $B = (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4) - \frac{14}{9}D$  donc

$$-\frac{14}{9}D = B - (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4).$$

La ligne au-dessus dans l'algorithme d'Euclide était :  $A = B \times (X - 1) + 3X^3 + 2X^2 + 5X - 2$ . On substitue le reste pour obtenir :

$$-\frac{14}{9}D = B - (A - B \times (X - 1)) \times \frac{1}{9}(3X + 4).$$

On en déduit

$$-\frac{14}{9}D = -A \times \frac{1}{9}(3X + 4) + B(1 + (X - 1) \times \frac{1}{9}(3X + 4))$$

Donc en posant  $U = \frac{1}{14}(3X + 4)$  et  $V = -\frac{1}{14}(9 + (X - 1)(3X + 4)) = -\frac{1}{14}(3X^2 + X + 5)$  on a  $AU + BV = D$ .

Le corollaire suivant s'appelle aussi le théorème de Bézout.

**Corollaire 1.**

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 2.**

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

**Corollaire 3** (Lemme de Gauss).

Soient  $A, B, C \in \mathbb{K}[X]$ . Si  $A|BC$  et  $\text{pgcd}(A, B) = 1$  alors  $A|C$ .

## 2.4. ppcm

**Proposition 5.**

Soient  $A, B \in \mathbb{K}[X]$  des polynômes non nuls, alors il existe un unique polynôme unitaire  $M$  de plus petit degré tel que  $A|M$  et  $B|M$ .

Cet unique polynôme est appelé le **ppcm** (plus petit commun multiple) de  $A$  et  $B$  qu'on note  $\text{ppcm}(A, B)$ .

**Exemple 10.**

$$\text{ppcm}(X(X-2)^2(X^2+1)^4, (X+1)(X-2)^3(X^2+1)^3) = X(X+1)(X-2)^3(X^2+1)^4.$$

De plus le ppcm est aussi le plus petit au sens de la divisibilité :

**Proposition 6.**

Soient  $A, B \in \mathbb{K}[X]$  des polynômes non nuls et  $M = \text{ppcm}(A, B)$ . Si  $C \in \mathbb{K}[X]$  est un polynôme tel que  $A|C$  et  $B|C$ , alors  $M|C$ .

**Mini-exercices.**

1. Trouver les diviseurs de  $X^4 + 2X^2 + 1$  dans  $\mathbb{R}[X]$ , puis dans  $\mathbb{C}[X]$ .
2. Montrer que  $X - 1 | X^n - 1$  (pour  $n \geq 1$ ).
3. Calculer les divisions euclidiennes de  $A$  par  $B$  avec  $A = X^4 - 1$ ,  $B = X^3 - 1$ . Puis  $A = 4X^3 + 2X^2 - X - 5$  et  $B = X^2 + X$ ;  $A = 2X^4 - 9X^3 + 18X^2 - 21X + 2$  et  $B = X^2 - 3X + 1$ ;  $A = X^5 - 2X^4 + 6X^3$  et  $B = 2X^3 + 1$ .
4. Déterminer le pgcd de  $A = X^5 + X^3 + X^2 + 1$  et  $B = 2X^3 + 3X^2 + 2X + 3$ . Trouver les coefficients de Bézout  $U, V$ .  
Mêmes questions avec  $A = X^5 - 1$  et  $B = X^4 + X + 1$ .
5. Montrer que si  $AU + BV = 1$  avec  $\deg U < \deg B$  et  $\deg V < \deg A$  alors les polynômes  $U, V$  sont uniques.

## 3. Racine d'un polynôme, factorisation

### 3.1. Racines d'un polynôme

**Définition 5.**

Soit  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in \mathbb{K}[X]$ . Pour un élément  $x \in \mathbb{K}$ , on note  $P(x) = a_n x^n + \dots + a_1 x + a_0$ . On associe ainsi au polynôme  $P$  une **fonction polynôme** (que l'on note encore  $P$ )

$$P : \mathbb{K} \rightarrow \mathbb{K}, \quad x \mapsto P(x) = a_n x^n + \dots + a_1 x + a_0.$$

**Définition 6.**

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

**Proposition 7.**

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

*Démonstration.* Lorsque l'on écrit la division euclidienne de  $P$  par  $X - \alpha$  on obtient  $P = Q \cdot (X - \alpha) + R$  où  $R$  est une constante car  $\deg R < \deg(X - \alpha) = 1$ . Donc  $P(\alpha) = 0 \iff R(\alpha) = 0 \iff R = 0 \iff X - \alpha | P$ .  $\square$

### Définition 7.

Soit  $k \in \mathbb{N}^*$ . On dit que  $\alpha$  est une **racine de multiplicité  $k$**  de  $P$  si  $(X - \alpha)^k$  divise  $P$  alors que  $(X - \alpha)^{k+1}$  ne divise pas  $P$ . Lorsque  $k = 1$  on parle d'une **racine simple**, lorsque  $k = 2$  d'une **racine double**, etc.

On dit aussi que  $\alpha$  est une **racine d'ordre  $k$** .

### Proposition 8.

Il y a équivalence entre :

- (i)  $\alpha$  est une racine de multiplicité  $k$  de  $P$ .
- (ii) Il existe  $Q \in \mathbb{K}[X]$  tel que  $P = (X - \alpha)^k Q$ , avec  $Q(\alpha) \neq 0$ .
- (iii)  $P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0$  et  $P^{(k)}(\alpha) \neq 0$ .

La preuve est laissée en exercice.

### Remarque.

Par analogie avec la dérivée d'une fonction, si  $P(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X]$  alors le polynôme  $P'(X) = a_1 + 2a_2X + \dots + na_nX^{n-1}$  est le **polynôme dérivé** de  $P$ .

## 3.2. Théorème de d'Alembert-Gauss

Passons à un résultat essentiel de ce chapitre :

### Théorème 3 (Théorème de d'Alembert-Gauss).

Tout polynôme à coefficients complexes de degré  $n \geq 1$  a au moins une racine dans  $\mathbb{C}$ . Il admet exactement  $n$  racines si on compte chaque racine avec multiplicité.

Nous admettons ce théorème.

### Exemple 11.

Soit  $P(X) = aX^2 + bX + c$  un polynôme de degré 2 à coefficients réels :  $a, b, c \in \mathbb{R}$  et  $a \neq 0$ .

- Si  $\Delta = b^2 - 4ac > 0$  alors  $P$  admet 2 racines réelles distinctes  $\frac{-b+\sqrt{\Delta}}{2a}$  et  $\frac{-b-\sqrt{\Delta}}{2a}$ .
- Si  $\Delta < 0$  alors  $P$  admet 2 racines complexes distinctes  $\frac{-b+i\sqrt{|\Delta|}}{2a}$  et  $\frac{-b-i\sqrt{|\Delta|}}{2a}$ .
- Si  $\Delta = 0$  alors  $P$  admet une racine réelle double  $\frac{-b}{2a}$ .

En tenant compte des multiplicités on a donc toujours exactement 2 racines.

### Exemple 12.

$P(X) = X^n - 1$  admet  $n$  racines distinctes.

Sachant que  $P$  est de degré  $n$  alors par le théorème de d'Alembert-Gauss on sait qu'il admet  $n$  racines comptées avec multiplicité. Il s'agit donc maintenant de montrer que ce sont des racines simples. Supposons –par l'absurde– que  $\alpha \in \mathbb{C}$  soit une racine de multiplicité  $\geq 2$ . Alors  $P(\alpha) = 0$  et  $P'(\alpha) = 0$ . Donc  $\alpha^n - 1 = 0$  et  $n\alpha^{n-1} = 0$ . De la seconde égalité on déduit  $\alpha = 0$ , contradictoire avec la première égalité. Donc toutes les racines sont simples. Ainsi les  $n$  racines sont distinctes. (Remarque : sur cet exemple particulier on aurait aussi pu calculer les racines qui sont ici les racines  $n$ -ième de l'unité.)

Pour les autres corps que les nombres complexes nous avons le résultat plus faible suivant :

### Théorème 4.

Soit  $P \in \mathbb{K}[X]$  de degré  $n \geq 1$ . Alors  $P$  admet au plus  $n$  racines dans  $\mathbb{K}$ .

### Exemple 13.

$P(X) = 3X^3 - 2X^2 + 6X - 4$ . Considéré comme un polynôme à coefficients dans  $\mathbb{Q}$  ou  $\mathbb{R}$ ,  $P$  n'a qu'une seule racine (qui est simple)  $\alpha = \frac{2}{3}$  et il se décompose en  $P(X) = 3(X - \frac{2}{3})(X^2 + 2)$ . Si on considère maintenant  $P$  comme un polynôme à coefficients dans  $\mathbb{C}$  alors  $P(X) = 3(X - \frac{2}{3})(X - i\sqrt{2})(X + i\sqrt{2})$  et admet 3 racines simples.

### 3.3. Polynômes irréductibles

#### Définition 8.

Soit  $P \in \mathbb{K}[X]$  un polynôme de degré  $\geq 1$ , on dit que  $P$  est *irréductible* si pour tout  $Q \in \mathbb{K}[X]$  divisant  $P$ , alors, soit  $Q \in \mathbb{K}^*$ , soit il existe  $\lambda \in \mathbb{K}^*$  tel que  $Q = \lambda P$ .

#### Remarque.

- 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).
- La notion de polynôme irréductible pour l'arithmétique de  $\mathbb{K}[X]$  correspond à la notion de nombre premier pour l'arithmétique de  $\mathbb{Z}$ .
- Dans le cas contraire, on dit que  $P$  est *réductible*; il existe alors des polynômes  $A, B$  de  $\mathbb{K}[X]$  tels que  $P = AB$ , avec  $\deg A \geq 1$  et  $\deg B \geq 1$ .

#### Exemple 14.

- Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.
- $X^2 - 1 = (X - 1)(X + 1) \in \mathbb{R}[X]$  est réductible.
- $X^2 + 1 = (X - i)(X + i)$  est réductible dans  $\mathbb{C}[X]$  mais est irréductible dans  $\mathbb{R}[X]$ .
- $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$  est réductible dans  $\mathbb{R}[X]$  mais est irréductible dans  $\mathbb{Q}[X]$ .

Nous avons l'équivalent du lemme d'Euclide de  $\mathbb{Z}$  pour les polynômes :

#### Proposition 9 (Lemme d'Euclide).

Soit  $P \in \mathbb{K}[X]$  un polynôme irréductible et soient  $A, B \in \mathbb{K}[X]$ . Si  $P|AB$  alors  $P|A$  ou  $P|B$ .

*Démonstration.* Si  $P$  ne divise pas  $A$  alors  $\text{pgcd}(P, A) = 1$  car  $P$  est irréductible. Donc, par le lemme de Gauss,  $P$  divise  $B$ . □

### 3.4. Théorème de factorisation

#### Théorème 5.

Tout polynôme non constant  $A \in \mathbb{K}[X]$  s'écrit comme un produit de polynômes irréductibles unitaires :

$$A = \lambda P_1^{k_1} P_2^{k_2} \dots P_r^{k_r}$$

où  $\lambda \in \mathbb{K}^*$ ,  $r \in \mathbb{N}^*$ ,  $k_i \in \mathbb{N}^*$  et les  $P_i$  sont des polynômes irréductibles distincts.

De plus cette décomposition est unique à l'ordre près des facteurs.

Il s'agit bien sûr de l'analogie de la décomposition d'un nombre en facteurs premiers.

### 3.5. Factorisation dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

#### Théorème 6.

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

Donc pour  $P \in \mathbb{C}[X]$  de degré  $n \geq 1$  la factorisation s'écrit  $P = \lambda(X - \alpha_1)^{k_1}(X - \alpha_2)^{k_2} \dots (X - \alpha_r)^{k_r}$ , où  $\alpha_1, \dots, \alpha_r$  sont les racines distinctes de  $P$  et  $k_1, \dots, k_r$  sont leurs multiplicités.

*Démonstration.* Ce théorème résulte du théorème de d'Alembert-Gauss. □

#### Théorème 7.

Les polynômes irréductibles de  $\mathbb{R}[X]$  sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant  $\Delta < 0$ .

Soit  $P \in \mathbb{R}[X]$  de degré  $n \geq 1$ . Alors la factorisation s'écrit  $P = \lambda(X - \alpha_1)^{k_1}(X - \alpha_2)^{k_2} \dots (X - \alpha_r)^{k_r} Q_1^{\ell_1} \dots Q_s^{\ell_s}$ , où les  $\alpha_i$  sont exactement les racines réelles distinctes de multiplicité  $k_i$  et les  $Q_i$  sont des polynômes irréductibles de degré 2 :  $Q_i = X^2 + \beta_i X + \gamma_i$  avec  $\Delta = \beta_i^2 - 4\gamma_i < 0$ .

**Exemple 15.**

$P(X) = 2X^4(X-1)^3(X^2+1)^2(X^2+X+1)$  est déjà décomposé en facteurs irréductibles dans  $\mathbb{R}[X]$  alors que sa décomposition dans  $\mathbb{C}[X]$  est  $P(X) = 2X^4(X-1)^3(X-i)^2(X+i)^2(X-j)(X-j^2)$  où  $j = e^{\frac{2i\pi}{3}} = \frac{-1+i\sqrt{3}}{2}$ .

**Exemple 16.**

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

- Sur  $\mathbb{C}$ . On peut d'abord décomposer  $P(X) = (X^2 + i)(X^2 - i)$ . Les racines de  $P$  sont donc les racines carrées complexes de  $i$  et  $-i$ . Ainsi  $P$  se factorise dans  $\mathbb{C}[X]$  :

$$P(X) = \left(X - \frac{\sqrt{2}}{2}(1+i)\right)\left(X + \frac{\sqrt{2}}{2}(1+i)\right)\left(X - \frac{\sqrt{2}}{2}(1-i)\right)\left(X + \frac{\sqrt{2}}{2}(1-i)\right).$$

- Sur  $\mathbb{R}$ . Pour un polynôme à coefficient réels, si  $\alpha$  est une racine alors  $\bar{\alpha}$  aussi. Dans la décomposition ci-dessus on regroupe les facteurs ayant des racines conjuguées, cela doit conduire à un polynôme réel :

$$\begin{aligned} P(X) &= \left[\left(X - \frac{\sqrt{2}}{2}(1+i)\right)\left(X - \frac{\sqrt{2}}{2}(1-i)\right)\right]\left[\left(X + \frac{\sqrt{2}}{2}(1+i)\right)\left(X + \frac{\sqrt{2}}{2}(1-i)\right)\right] \\ &= [X^2 + \sqrt{2}X + 1][X^2 - \sqrt{2}X + 1], \end{aligned}$$

qui est la factorisation dans  $\mathbb{R}[X]$ .

**Mini-exercices.**

1. Trouver un polynôme  $P(X) \in \mathbb{Z}[X]$  de degré minimal tel que :  $\frac{1}{2}$  soit une racine simple,  $\sqrt{2}$  soit une racine double et  $i$  soit une racine triple.
2. Montrer cette partie de la proposition 8 : «  $P(\alpha) = 0$  et  $P'(\alpha) = 0 \iff \alpha$  est une racine de multiplicité  $\geq 2$  ».
3. Montrer que pour  $P \in \mathbb{C}[X]$  : «  $P$  admet une racine de multiplicité  $\geq 2 \iff P$  et  $P'$  ne sont pas premiers entre eux ».
4. Factoriser  $P(X) = (2X^2 + X - 2)^2(X^4 - 1)^3$  et  $Q(X) = 3(X^2 - 1)^2(X^2 - X + \frac{1}{4})$  dans  $\mathbb{C}[X]$ . En déduire leur pgcd et leur ppcm. Mêmes questions dans  $\mathbb{R}[X]$ .
5. Si  $\text{pgcd}(A, B) = 1$  montrer que  $\text{pgcd}(A + B, A \times B) = 1$ .
6. Soit  $P \in \mathbb{R}[X]$  et  $\alpha \in \mathbb{C} \setminus \mathbb{R}$  tel que  $P(\alpha) = 0$ . Vérifier que  $P(\bar{\alpha}) = 0$ . Montrer que  $(X - \alpha)(X - \bar{\alpha})$  est un polynôme irréductible de  $\mathbb{R}[X]$  et qu'il divise  $P$  dans  $\mathbb{R}[X]$ .

## 4. Fractions rationnelles

**Définition 9.**

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  $Q \neq 0$ .

Toute fraction rationnelle se décompose comme une somme de fractions rationnelles élémentaires que l'on appelle des « éléments simples ». Mais les éléments simples sont différents sur  $\mathbb{C}$  ou sur  $\mathbb{R}$ .

### 4.1. Décomposition en éléments simples sur $\mathbb{C}$

**Théorème 8** (Décomposition en éléments simples sur  $\mathbb{C}$ ).

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

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

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

**Exemple 17.**

- Vérifier que  $\frac{1}{x^2+1} = \frac{a}{x+i} + \frac{b}{x-i}$  avec  $a = \frac{1}{2}i$ ,  $b = -\frac{1}{2}i$ .
- Vérifier que  $\frac{x^4-8x^2+9x-7}{(x-2)^2(x+3)} = X + 1 + \frac{-1}{(x-2)^2} + \frac{2}{x-2} + \frac{-1}{x+3}$ .

Comment se calcule cette décomposition ? En général on commence par déterminer la partie polynomiale. Tout d'abord si  $\deg Q > \deg P$  alors  $E(X) = 0$ . Si  $\deg P \leq \deg Q$  alors effectuons la division euclidienne de  $P$  par  $Q$  :  $P = QE + R$  donc  $\frac{P}{Q} = E + \frac{R}{Q}$  où  $\deg R < \deg Q$ . La partie polynomiale est donc le quotient de cette division. Et on s'est ramené au cas d'une fraction  $\frac{R}{Q}$  avec  $\deg R < \deg Q$ . Voyons en détails comment continuer sur un exemple.

**Exemple 18.**

Décomposons la fraction  $\frac{P}{Q} = \frac{X^5 - 2X^3 + 4X^2 - 8X + 11}{X^3 - 3X + 2}$ .

- **Première étape : partie polynomiale.** On calcule la division euclidienne de  $P$  par  $Q$  :  $P(X) = (X^2 + 1)Q(X) + 2X^2 - 5X + 9$ . Donc la partie polynomiale est  $E(X) = X^2 + 1$  et la fraction s'écrit  $\frac{P(X)}{Q(X)} = X^2 + 1 + \frac{2X^2 - 5X + 9}{Q(X)}$ . Notons que pour la fraction  $\frac{2X^2 - 5X + 9}{Q(X)}$  le degré du numérateur est strictement plus petit que le degré du dénominateur.
- **Deuxième étape : factorisation du dénominateur.**  $Q$  a pour racine évidente  $+1$  (racine double) et  $-2$  (racine simple) et se factorise donc ainsi  $Q(X) = (X - 1)^2(X + 2)$ .
- **Troisième étape : décomposition théorique en éléments simples.** Le théorème de décomposition en éléments simples nous dit qu'il existe une unique décomposition :  $\frac{P(X)}{Q(X)} = E(X) + \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$ . Nous savons déjà que  $E(X) = X^2 + 1$ , il reste à trouver les nombres  $a, b, c$ .
- **Quatrième étape : détermination des coefficients.** Voici une première façon de déterminer  $a, b, c$ . On réécrit la fraction  $\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$  au même dénominateur et on l'identifie avec  $\frac{2X^2 - 5X + 9}{Q(X)}$  :

$$\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2} = \frac{(b+c)X^2 + (a+b-2c)X + 2a-2b+c}{(X-1)^2(X+2)}$$

qui doit être égale à

$$\frac{2X^2 - 5X + 9}{(X-1)^2(X+2)}.$$

On en déduit  $b + c = 2$ ,  $a + b - 2c = -5$  et  $2a - 2b + c = 9$ . Cela conduit à l'unique solution  $a = 2$ ,  $b = -1$ ,  $c = 3$ .  
Donc

$$\frac{P}{Q} = \frac{X^5 - 2X^3 + 4X^2 - 8X + 11}{X^3 - 3X + 2} = X^2 + 1 + \frac{2}{(X-1)^2} + \frac{-1}{X-1} + \frac{3}{X+2}.$$

Cette méthode est souvent la plus longue.

- **Quatrième étape (bis) : détermination des coefficients.** Voici une autre méthode plus efficace.

Notons  $\frac{P'(X)}{Q(X)} = \frac{2X^2 - 5X + 9}{(X-1)^2(X+2)}$  dont la décomposition théorique est :  $\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$

Pour déterminer  $a$  on multiplie la fraction  $\frac{P'}{Q}$  par  $(X-1)^2$  et on évalue en  $x = 1$ .

Tout d'abord en partant de la décomposition théorique on a :

$$F_1(X) = (X-1)^2 \frac{P'(X)}{Q(X)} = a + b(X-1) + c \frac{(X-1)^2}{X+2} \quad \text{donc} \quad F_1(1) = a$$

D'autre part

$$F_1(X) = (X-1)^2 \frac{P'(X)}{Q(X)} = (X-1)^2 \frac{2X^2 - 5X + 9}{(X-1)^2(X+2)} = \frac{2X^2 - 5X + 9}{X+2}$$

donc  $F_1(1) = 2$ . On en déduit  $a = 2$ .

On fait le même processus pour déterminer  $c$  : on multiplie par  $(X+2)$  et on évalue en  $-2$ . On calcule  $F_2(X) = (X+2) \frac{P'(X)}{Q(X)} = \frac{2X^2 - 5X + 9}{(X-1)^2} = a \frac{X+2}{(X-1)^2} + b \frac{X+2}{X-1} + c$  de deux façons et lorsque l'on évalue  $x = -2$  on obtient d'une part  $F_2(-2) = c$  et d'autre part  $F_2(-2) = 3$ . Ainsi  $c = 3$ .

Comme les coefficients sont uniques tous les moyens sont bons pour les déterminer. Par exemple lorsque l'on évalue la décomposition théorique  $\frac{P'(X)}{Q(X)} = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$  en  $x = 0$ , on obtient :

$$\frac{P'(0)}{Q(0)} = a - b + \frac{c}{2}$$

Donc  $\frac{9}{2} = a - b + \frac{c}{2}$ . Donc  $b = a + \frac{c}{2} - \frac{9}{2} = -1$ .

## 4.2. Décomposition en éléments simples sur $\mathbb{R}$

**Théorème 9** (Décomposition en éléments simples sur  $\mathbb{R}$ ).

Soit  $P/Q$  une fraction rationnelle avec  $P, Q \in \mathbb{R}[X]$ ,  $\text{pgcd}(P, Q) = 1$ . 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.

### Exemple 19.

Décomposition en éléments simples de  $\frac{P(X)}{Q(X)} = \frac{3X^4+5X^3+8X^2+5X+3}{(X^2+X+1)^2(X-1)}$ . Comme  $\deg P < \deg Q$  alors  $E(X) = 0$ . Le dénominateur est déjà factorisé sur  $\mathbb{R}$  car  $X^2 + X + 1$  est irréductible. La décomposition théorique est donc :

$$\frac{P(X)}{Q(X)} = \frac{aX+b}{(X^2+X+1)^2} + \frac{cX+d}{X^2+X+1} + \frac{e}{X-1}.$$

Il faut ensuite mener au mieux les calculs pour déterminer les coefficients afin d'obtenir :

$$\frac{P(X)}{Q(X)} = \frac{2X+1}{(X^2+X+1)^2} + \frac{-1}{X^2+X+1} + \frac{3}{X-1}.$$

### Mini-exercices.

1. Soit  $Q(X) = (X-2)^2(X^2-1)^3(X^2+1)^4$ . Pour  $P \in \mathbb{R}[X]$  quelle est la forme théorique de la décomposition en éléments simples sur  $\mathbb{C}$  de  $\frac{P}{Q}$  ? Et sur  $\mathbb{R}$  ?
2. Décomposer les fractions suivantes en éléments simples sur  $\mathbb{R}$  et  $\mathbb{C}$  :  $\frac{1}{X^2-1}$  ;  $\frac{X^2+1}{(X-1)^2}$  ;  $\frac{X}{X^3-1}$ .
3. Décomposer les fractions suivantes en éléments simples sur  $\mathbb{R}$  :  $\frac{X^2+X+1}{(X-1)(X+2)^2}$  ;  $\frac{2X^2-X}{(X^2+2)^2}$  ;  $\frac{X^6}{(X^2+1)^2}$ .
4. Soit  $F(X) = \frac{2X^2+7X-20}{X+2}$ . Déterminer l'équation de l'asymptote oblique en  $\pm\infty$ . Étudier la position du graphe de  $F$  par rapport à cette droite.