

# Chapitre 18 : Polynômes

## Introduction

Les fonctions polynomiales sont largement utilisées en pratique, ne serait-ce que parce qu'elles donnent localement une valeur approchée de toute fonction dérivable (voir chapitre développement limité).

On verra que l'anneau  $\mathbb{K}[X]$  des polynômes à coefficients dans  $\mathbb{K}$  et l'anneau des entiers relatifs  $\mathbb{Z}$  ont des propriétés très voisines, dues, entre autre, au fait que dans chacun d'eux on peut effectuer une division euclidienne.

Dans tout ce chapitre,  $(\mathbb{K}, +, \cdot)$  désigne un corps commutatif. Dans la plupart des cas,  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$ .

## 1 Anneau des polynômes à une indéterminée

### 1.1 Polynôme formel

#### Définition 1 (Polynôme formel).

Un **polynôme formel** est une suite d'éléments de  $\mathbb{K}$  dont seul un nombre fini d'éléments sont susceptibles d'être non nuls.

On note  $P = (a_0, a_1, \dots, a_n, 0_{\mathbb{K}}, \dots) \in \mathbb{K}^{\mathbb{N}}$  ou encore  $P = (a_i)$  tel que  $\exists n \in \mathbb{N}, \forall i > n, a_i = 0_{\mathbb{K}}$  (à partir d'un certain rang, tous les coefficients sont nuls).

$$P = 0 \text{ ssi } \forall i \in \mathbb{N}, a_i = 0_{\mathbb{K}}.$$

Si  $P \neq 0$ ,  $\exists i \in \mathbb{N}, a_i \neq 0_{\mathbb{K}}$ .  $\{i \in \mathbb{N}, a_i \neq 0_{\mathbb{K}}\}$  est une partie non vide de  $\mathbb{N}$  qui est majorée. Elle possède un plus petit élément, appelé la valuation de  $P$  et noté  $\text{val}(P)$  et elle possède un plus grand élément : le **degré** de  $P$  et noté  $\text{deg}(P)$ . Si  $P = (0_{\mathbb{K}}, \dots, 0_{\mathbb{K}}, a_i, \dots, a_j, 0_{\mathbb{K}}, \dots, 0_{\mathbb{K}})$  avec  $a_i \neq 0_{\mathbb{K}}$  et  $a_j \neq 0_{\mathbb{K}}$ ,  $\text{val}(P) = i$  et  $\text{deg}(P) = j$ . Si de plus  $a_j = 1$  on dit que  $P$  est unitaire.

**Remarque 1.** 1. Si  $P \neq 0$ ,  $\text{deg}(P) \geq \text{val}(P)$ .

2. Si  $P \neq 0$  et si  $\text{deg}(P) = \text{val}(P)$ , on dit que  $P$  est un **monôme**.

3. Par convention, le degré du polynôme nul est  $-\infty$ , sa valuation est  $+\infty$  et le polynôme nul est aussi un monôme.

### 1.2 Opérations sur l'ensemble des polynômes formels sur $\mathbb{K}$

#### Propriété 1 (Addition).

Si  $P = (a_i)_{i \in \mathbb{N}}$  et  $Q = (b_i)_{i \in \mathbb{N}}$  sont des polynômes formels sur  $\mathbb{K}$  alors  $P + Q = (a_i + b_i)_{i \in \mathbb{N}}$  est un polynôme formel et  $\text{deg}(P + Q) \leq \max(\text{deg}(P), \text{deg}(Q))$ .

Résultat valable si  $P = 0$  ou  $Q = 0$ .

#### Propriété 2.

Muni de l'addition classique sur  $\mathbb{K}^{\mathbb{N}}$ , l'ensemble des polynômes formels sur  $\mathbb{K}$  est un sous-groupe du groupe commutatif  $(\mathbb{K}^{\mathbb{N}}, +)$ .

**Propriété 3 (Multiplication).**

Si  $P = (a_i)_{i \in \mathbb{N}}$  et  $Q = (b_i)_{i \in \mathbb{N}}$  sont des polynômes formels sur  $\mathbb{K}$  alors  
 $P \times Q = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \dots, a_0b_k + a_1b_{k-1} + \dots + a_kb_0, \dots)$   
 $= (c_i)_{i \in \mathbb{N}}$  où  $c_i = \sum_{j=0}^i a_j b_{i-j}$  est un polynôme formel et  $\deg(P \times Q) = \deg(P) + \deg(Q)$ .

Résultat valable si  $P = 0$  ou  $Q = 0$ .

**Propriété 4 (Propriétés du produit).**

1.  $\times$  est une LCI sur l'ensemble des polynômes formels sur  $\mathbb{K}$ .
2.  $\times$  est commutative.
3.  $\times$  est associative.
4.  $\times$  est distributive par rapport à  $+$ .
5. l'élément neutre pour  $\times$  est  $(1_{\mathbb{K}}, 0_{\mathbb{K}}, \dots) = (\delta_{0,i})$ .

**Propriété 5.**

L'ensemble des polynômes formels sur  $\mathbb{K}$ , muni de l'addition et de la multiplication, est un anneau commutatif intègre.

**Propriété 6 (Multiplication par un scalaire).**

Si  $P = (a_i)_{i \in \mathbb{N}}$  est un polynôme formel sur  $\mathbb{K}$  et si  $\alpha \in \mathbb{K}$  alors  $\alpha.P = (\alpha.a_i)_{i \in \mathbb{N}}$  est un polynôme formel et  $\deg(\alpha.P) = \deg(P)$  si  $\alpha \neq 0_{\mathbb{K}}$ , sinon  $\deg(\alpha.P) = -\infty$ .

**1.3 Notion d'indéterminée**

Soit  $U_n = (0, 0, \dots, 1, 0, \dots)$  où 1 est en  $n + 1^{\text{ème}}$  position.

$U_0 = 1 = (1, 0, \dots)$ .

Si  $P = (a_0, a_1, a_2, \dots, a_n, 0, \dots)$

$= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, \dots, a_n, 0, \dots)$

$= a_0(1, 0, \dots) + a_1(0, 1, 0, \dots) + \dots + a_n(0, \dots, 1, 0, \dots)$

$= a_0U_0 + a_1U_1 + \dots + a_nU_n$ .

On montre de plus que  $U_n \times U_p = U_{n+p}$ . Ainsi  $U_1 \times U_1 = U_2 = (U_1)^2$ ,  $U_2 \times U_1 = (U_1)^3 = U_3 \dots$  on montre par récurrence que  $\forall n \in \mathbb{N}^*$ ,  $U_n = (U_1)^n$ .

**On pose  $U_1 = X$ . Alors  $\forall n \in \mathbb{N}$ ,  $U_n = X^n$  (si  $n = 0$ , on pose  $X^0 = U_0 = 1$ ).**

**Définition 2 (Polynôme à une indéterminée).**

**Notation définitive :** Si  $P = (a_i)_{i \in \mathbb{N}}$  est de degré inférieur ou égal à  $n$ , alors on écrira  $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n = \sum_{k=0}^n a_kX^k$ .  $\sum_{k=0}^n a_kX^k$  est appelé polynôme à une indéterminée à coefficients dans  $\mathbb{K}$ .

Si de plus  $a_n \neq 0$  alors  $P$  est de degré exactement  $n$ ,  $a_nX^n$  est appelé **terme de plus haut degré** et  $a_n$  est le **coefficient dominant** de  $P$ .

L'ensemble des polynômes à une indéterminée à coefficients dans  $\mathbb{K}$  se note  $\mathbb{K}[X]$ .  $X$  est l'indéterminée.  $\mathbb{K} \subset \mathbb{K}[X]$ .

## 1.4 Fonction polynôme associée à un polynôme de $\mathbb{K}[X]$

### Définition 3 (Fonction polynôme associée).

Soit  $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{K}[X]$ , on définit la **fonction polynôme associée** à  $P$ ,  $\tilde{P}$  ainsi :  
 $\tilde{P} : \mathbb{K} \rightarrow \mathbb{K}, x \mapsto \tilde{P}(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ .

## 1.5 Composition de polynômes

### Définition 4 (Composition de polynômes).

Soit  $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{K}[X]$ .  
 On définit  $\tilde{P} : \mathbb{K}[X] \rightarrow \mathbb{K}[X], Q \mapsto \tilde{P}(Q) = a_0 \times 1 + a_1 \times Q + a_2 \times Q^2 + \dots + a_n \times Q^n$ .  
 $P \circ Q = \tilde{P}(Q)$ .  
 De plus  $P \circ Q = \tilde{P} \circ \tilde{Q}$ , où  $\tilde{P} \circ \tilde{Q} : \mathbb{K} \rightarrow \mathbb{K}, x \mapsto \tilde{P} \circ \tilde{Q}(x) = a_0 + a_1\tilde{Q}(x) + \dots + a_n\tilde{Q}^n(x)$  et  
 $\tilde{P} \circ \tilde{Q} : \mathbb{K} \rightarrow \mathbb{K}, x \mapsto \tilde{P}(\tilde{Q}(x))$ .

► Exemple :  $P = 5X^3 - X^2 + 1, Q = X + 1$  et  $\tilde{P}(Q) = 5(X + 1)^3 - (X + 1)^2 + 1$ .

### Propriété 7.

1.  $\circ$  est une LCI sur  $\mathbb{K}[X]$ .
2.  $\forall (P, Q) \in (\mathbb{K}[X]^*)^2$ , tels que  $\deg(Q) \neq 0, \deg(P \circ Q) = \deg(P) \times \deg(Q)$ .
3.  $\circ$  est associative.
4.  $X$  est élément neutre pour la composition :  $X \circ P = P \circ X = P$ . On note parfois  $P = P(X)$ .
5.  $\circ$  n'est pas distributive par rapport à  $+$  :  $X^2 \circ (X + 1) = (X + 1)^2$  alors que  $X^2 \circ X + X^2 \circ 1 = X^2 + 1$ .

Si  $P$  est symétrisable pour  $\circ$  alors  $\deg(P) = 1$ . Si  $P = aX + b$  avec  $a \neq 0$ , chercher  $Q = \alpha X + \beta$  tel que  $P \circ Q = Q \circ P = X$ .

Ne pas confondre  $P(X + 1)$  avec le produit  $(X + 1)P$ .

## 1.6 Ensemble $\mathbb{K}_n[X]$

### Propriété 8 (Ensemble des polynômes de degré inférieur ou égal à $n$ ).

Soit  $n \in \mathbb{N}$ . On note  $\mathbb{K}_n[X]$  l'ensemble des polynômes de degré inférieur ou égal à  $n$ .  $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X], \deg(P) \leq n\}$ . ( $\mathbb{K}_n[X]$ ) est stable par combinaison linéaire.

## 2 Divisibilité et division euclidienne dans $\mathbb{K}[X]$

### 2.1 Division euclidienne

#### Théorème 1 (Division euclidienne).

Soit  $A \in \mathbb{K}[X]$  et  $B \in \mathbb{K}[X] \setminus \{0\}$ , il existe un unique couple  $(Q, R)$  de polynômes de  $\mathbb{K}[X]$  vérifiant  

$$\begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases} ; Q \text{ s'appelle } \underline{\text{quotient}} \text{ de la division euclidienne de } A \text{ par } B \text{ et } R \text{ s'appelle } \underline{\text{reste}} \text{ de la division euclidienne de } A \text{ par } B.$$

Démonstration :

**Unicité** : Supposons qu'il existe deux couples convenables :  $\begin{cases} A = BQ_1 + R_1 \\ A = BQ_2 + R_2 \end{cases}$  avec  $\deg R_1, \deg R_2 < \deg B$ . Alors  
 $B \times (Q_2 - Q_1) = R_1 - R_2$ . Si  $Q_1 = Q_2$  alors  $R_1 = R_2$ . Si  $Q_1 \neq Q_2, \deg(Q_1 - Q_2) \geq 0$ . Or  $\deg(B(Q_1 - Q_2)) = \deg B + \deg(Q_1 - Q_2) \geq \deg B$  alors que  $\deg(R_1 - R_2) \leq \max(\deg R_1, \deg R_2) < \deg B$ . Contradiction d'où l'unicité.

**Existence** : Soit  $A = \sum_{k=0}^n a_k X^k$ . Soit  $B = \sum_{k=0}^p b_k X^k$  un polynôme non nul avec  $b_p \neq 0$ .

1. Premier cas :  $A = 0$  ou  $\deg(A) < \deg(B)$ .

Si  $A = 0$ ,  $(Q, R) = (0, 0)$ . Si  $\deg(A) < \deg(B)$ ,  $A = B \times 0 + R$  avec  $R = A$  ( $\deg(R) < \deg(B)$ ).

2. Deuxième cas : si  $\deg(A) \geq \deg(B)$ . Supposons que  $a_n \neq 0$ . On pose  $M_1 = \frac{a_n}{b_p} X^{n-p}$ ; le terme de plus haut degré de  $M_1 B$  est  $a_n X^n$ .  $A - M_1 B$  est un polynôme de degré  $n_1 < n$ . Soit  $A_1 = A - M_1 B$ .  $\deg(A_1) < \deg(A)$ .

(a) Premier sous-cas :  $A_1 = 0$  ou  $\deg(A_1) < \deg(B)$  et alors  $A_1 = B \times 0 + A_1$ .  $A = A_1 + M_1 B = B \times M_1 + A_1$  avec  $\deg(A_1) < \deg(B)$ .  $(Q, R) = (M_1, A_1)$  convient.

(b) Deuxième sous-cas : si  $\deg(A_1) \geq \deg(B)$ .

$A_1 = a_0^1 + \dots + a_{n_1}^1 X^{n_1}$ . On pose  $M_2 = \frac{a_{n_1}^1}{b_p} X^{n_1-p}$ . Le terme de plus haut degré de  $M_2 B$  est  $a_{n_1}^1 X^{n_1}$ .

$A_2 = A_1 - M_2 B$  et  $\deg(A_2) < \deg(A_1)$ .

i. Premier sous-sous-cas :  $A_2 = 0$  ou  $\deg(A_2) < \deg(B)$ .

Si  $\deg(A_2) < \deg(B)$  alors  $A_2 = 0 \times B + A_2$ .  $A = M_1 B + A_1 = M_1 B + M_2 B + A_2 = (M_1 + M_2) B + A_2$  et  $\deg(A_2) < \deg(B)$ .

ii. Deuxième sous-sous-cas : si  $\deg(A_2) \geq \deg(B)$ . Alors on recommence. On construit par cet algorithme une suite de polynômes  $A_1, A_2, \dots$  tel que  $\deg(A) > \deg(A_1) > \deg(A_2) > \dots$ . On s'arrête lorsque  $\deg(A_k) < \deg(B)$ .

Le nombre maximum d'opérations est majoré par  $\deg(A) - \deg(B)$ .

Soit  $k$  tel que  $\deg(A_{k-1}) \geq \deg(B)$  et  $\deg(A_k) < \deg(B)$ .  $A = M_1 B + M_2 B + \dots + M_k B + A_k$ .

$A = \underbrace{(M_1 + \dots + M_k)}_{=Q} B + \underbrace{A_k}_{=R}$ , avec  $\deg(A_k) < \deg(B)$ .

► Exemple : Ecrire la division euclidienne de  $A = X^4 + 2X^3 - X^2 + X - 4$  par  $B = X^2 + 3X - 5$ .

► Exemple : Ecrire la division euclidienne de  $A = X^2 + 3X - 1$  par  $B = X^3 - X^2 + 2X$ . Ecrire la division euclidienne de  $A = 2X^4 + 5X^3 - X^2 + 2X + 1$  par  $B = 2X^2 - 3X + 1$  puis celle de  $A = 3X^5 - 2X^4 + \frac{1}{3}X^3 - X + 5$  par  $B = X^3 + 5X^2 + 1$  (on trouve dans ce dernier cas  $Q = 3X^2 - 17X + \frac{256}{3}$  et  $R = \frac{-1289}{3}X^2 + 16X - \frac{241}{3}$ ).

## 2.2 Divisibilité dans $\mathbb{K}[X]$

### Définition 5.

Soit  $A \in \mathbb{K}[X]$ ,  $B \in \mathbb{K}[X] \setminus \{0\}$ , on dit que  $B$  **divise**  $A$  (noté  $B|A$ ) ssi le reste de la division euclidienne de  $A$  par  $B$  est nul ssi  $\exists Q \in \mathbb{K}[X] \mid A = BQ$ . On dit aussi que  $A$  est multiple de  $B$  ou que  $A$  est divisible par  $B$ .

### Définition 6 (Polynômes proportionnels ou associés).

Soient  $A$  et  $B$  dans  $\mathbb{K}[X]$ ,  $A$  est dit **proportionnel ou associé** à  $B$  ssi  $\exists \alpha \in \mathbb{K}^*$ ,  $A = \alpha B$ .

La relation de proportionnalité est une relation réflexive, symétrique et transitive.

### Propriété 9.

Soient  $(A, B) \in \mathbb{K}[X]^2$ .

1. Si  $A|B$  alors tout polynôme proportionnel à  $A$  divise tout polynôme proportionnel à  $B$ .
2. Dans  $\mathbb{K}[X] \setminus \{0\}$ , la divisibilité est une relation réflexive, transitive mais non symétrique et non anti-symétrique.
3. Si  $A|B$  et  $B|A$  alors  $A$  et  $B$  sont proportionnels.

### Définition 7 (Polynôme unitaire).

Soit  $A \in \mathbb{K}[X]$ . Parmi tous les polynômes associés à  $A$  il n'en existe qu'un dont le coefficient dominant est égal à  $1_{\mathbb{K}}$ . Ce polynôme est appelé **polynôme unitaire associé** à  $A$ .

### 3 Dérivation et formule de Taylor

Si  $P \in \mathbb{R}[X]$ ,  $\tilde{P} : \mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto a_0 + a_1x + \dots + a_nx^n$ .  
 $\tilde{P}$  est dérivable sur  $\mathbb{R}$  et  $\tilde{P}' : \mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto a_1 + 2a_2x + \dots + na_nx^{n-1}$ .  
 $P' = a_1 + 2a_2X + \dots + na_nX^{n-1} \in \mathbb{R}[X]$ . On remarque que  $\tilde{P}' = \tilde{P}'$ .

#### Définition 8 (Polynôme dérivé).

$\forall P \in \mathbb{K}[X]$ , si  $P = a_0 + a_1X + \dots + a_nX^n$  alors  $P' = a_1 + 2a_2X + \dots + na_nX^{n-1}$ .

#### Propriété 10.

1. Si  $\deg P = n \in \mathbb{N}^*$ ,  $\deg P' = n - 1$ . Si  $\deg P = 0$ ,  $P' = 0$ .
2.  $\forall (P, Q) \in \mathbb{K}[X]^2$ ,  $(P + Q)' = P' + Q'$ .
3.  $\forall \alpha \in \mathbb{K}$ ,  $(\alpha P)' = \alpha P'$ .

Autrement dit  $D : \mathbb{K}[X] \rightarrow \mathbb{K}[X]$ ,  $P \mapsto P'$  est linéaire.

#### Propriété 11 (Produit de polynômes).

1. Si  $P, Q \in \mathbb{K}[X]$ ,  $(PQ)' = P'Q + PQ'$ .
2.  $\forall n \in \mathbb{N}^*$ ,  $(P^n)' = nP^{n-1}P'$ . Démonstration par récurrence.

#### Définition 9 (Dérivées successives).

Soit  $P \in \mathbb{K}[X]$ .  
 $P'' = (P')' = P^{(2)}$ .  
 $P^{(1)} = P'$ .  
 $P^{(0)} = P$ .  
 $\forall n \in \mathbb{N}^*$ ,  $P^{(n)} = (P^{(n-1)})'$ .

#### Propriété 12.

$D^n : \mathbb{K}[X] \rightarrow \mathbb{K}[X]$ ,  $P \mapsto P^{(n)}$  est linéaire.

► Exemple :  $(PQ)'' = P''Q + 2P'Q' + PQ''$ .

#### Propriété 13 (Formule de Leibniz).

$\forall n \in \mathbb{N}^*$ ,  $(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$ .

#### Propriété 14.

Soient  $(p, n) \in \mathbb{N}^{*2}$  et  $a \in \mathbb{K}$ .

- Si  $n \leq p$ ,  $D^n[(X - a)^p] = \frac{p!}{(p - n)!} (X - a)^{p-n}$ .
- Si  $n > p$ ,  $D^n[(X - a)^p] = 0$ .
- Si  $n = p$ ,  $D^n[(X - a)^p] = n!$ .

#### Théorème 2 (Formule de Taylor).

Soit  $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X]$  ( $a_n \neq 0$ ) et  $\alpha \in \mathbb{K}$ .  $P = \sum_{k=0}^n \frac{\tilde{P}^{(k)}(\alpha)}{k!} (X - \alpha)^k$ .  
 $P = \tilde{P}(\alpha) + \tilde{P}'(\alpha)(X - \alpha) + \frac{\tilde{P}''(\alpha)}{2}(X - \alpha)^2 + \dots + \frac{\tilde{P}^{(n)}(\alpha)}{n!}(X - \alpha)^n$ .

Cas particulier : si  $\alpha = 0$ ,  $P = \sum_{k=0}^n \frac{\tilde{P}^{(k)}(0)}{k!} X^k$ .  $\forall k \in [[0, n]]$ ,  $a_k = \frac{\tilde{P}^{(k)}(0)}{k!}$ .

Un deuxième énoncé possible est le suivant :  $\forall P \in \mathbb{K}[X], \forall \alpha \in \mathbb{K}$ ,

$$P = \sum_{k=0}^{+\infty} \frac{\tilde{P}^{(k)}(\alpha)}{k!} (X - \alpha)^k$$

$$= \sum_{k=0}^{\deg P} \frac{\tilde{P}^{(k)}(\alpha)}{k!} (X - \alpha)^k. \text{ Si } k > \deg P, P^{(k)} = 0.$$

## 4 Racines d'un polynôme

### Définition 10.

Soit  $\alpha \in K$  et  $P \in \mathbb{K}[X]$ .  $\alpha$  est racine ou zéro de  $P$  lorsque  $P(\alpha) = 0$ .

Méthode de Horner pour l'évaluation polynomiale d'un polynôme de degré au plus  $n$  en  $n$  additions et  $n$  multiplications. Si  $P = \sum_{k=0}^n a_k X^k$  alors  $P(a) = (((((a_n \times a + a_{n-1}) \times a + a_{n-2}) \times a + \dots) \times a + a_1) \times a + a_0$ .

### Propriété 15.

$\alpha \in K$  est racine de  $P$  si et seulement si  $(X - \alpha) | P$  ssi le reste de la division euclidienne de  $P$  par  $(X - \alpha)$  est nul.

► Exemple : Le polynôme  $P = X^2 + 1$  est à coefficients réels donc appartient à  $\mathbb{R}[X]$  et à  $\mathbb{C}[X]$ .  $P$  n'a pas de racine dans  $\mathbb{R}$  mais a des racines dans  $\mathbb{C}$  ( $i$  et  $-i$ ).

### Théorème 3.

Soit  $n \in \mathbb{N}$ , tout polynôme non nul de degré  $n$  admet au plus  $n$  racines deux à deux distinctes.

### Propriété 16 (Corollaire).

Soit  $P \in \mathbb{K}[X]$  de degré inférieur ou égal à  $n$ . Si  $P$  admet au moins  $n + 1$  racines deux à deux distinctes alors  $P = 0$ .

► Méthode : On retient que pour montrer qu'un polynôme  $P$  est nul, on peut montrer qu'il a une infinité de racines (ce qui est faux pour une fonction en général : penser à la fonction sinus par exemple) et que pour montrer que deux polynômes  $P$  et  $Q$  sont égaux, on peut montrer que  $P - Q$  a une infinité de racines.

### Théorème 4 (Détermination d'un polynôme par sa fonction polynomiale).

Si  $P$  et  $Q$  sont deux polynômes de  $\mathbb{K}[X]$  dont les fonctions polynomiales associées coïncident sur une partie infinie de  $\mathbb{K}$  alors  $P = Q$ .

**Remarque 2.** Un polynôme est parfaitement déterminé par la donnée de sa fonction polynomiale associée.

L'application  $\varphi : \mathbb{K}[X] \rightarrow \mathcal{F}(\mathbb{K}, \mathbb{K})$ ,  $P \mapsto \tilde{P}$  est un morphisme d'anneau injectif. L'image de ce morphisme s'appelle ensemble des applications polynomiales sur  $\mathbb{K}$ .

On peut donc identifier  $P$  et  $\tilde{P}$  et dans la suite du cours on notera  $P(x)$  pour  $\tilde{P}(x)$ .

► Exemple : Soit  $P \in \mathbb{K}[X]$  tel que  $P(0) = 0$  et  $P(X + 1) - P(X) = 0$ . Montrer que  $P = 0$ .

► Exemple : Soit  $P \in \mathbb{K}[X]$ . Soient  $a$  et  $b$  deux réels distincts, avec  $a \neq b$ . Soient  $\alpha$  et  $\beta$  les restes respectifs de la division de  $P$  par  $(X - a)$  et par  $(X - b)$ . Quel est le reste de la division de  $P$  par  $(X - a)(X - b)$  ?

### Définition 11 (Racines multiples).

Soient  $P \in \mathbb{K}[X]$ ,  $P$  non nul,  $\alpha \in \mathbb{K}$  et  $k \in \mathbb{N}^*$ , on dit que  $\alpha$  est racine d'ordre de multiplicité  $k$  de  $P$  lorsque  $(X - \alpha)^k | P$  et  $(X - \alpha)^{k+1}$  ne divise pas  $P$ .

- Remarque 3.**
1. Si  $(X - \alpha)^k \mid P$ ,  $\alpha$  est au moins racine d'ordre  $k$  de  $P$ .
  2.  $\alpha$  est racine d'ordre  $k$  de  $P$  si et seulement si  $\exists Q \in \mathbb{K}[X] \quad P = Q(X - \alpha)^k$  avec  $Q(\alpha) \neq 0$ .
  3. Si  $k = 1$ ,  $\alpha$  est racine simple de  $P$ .
  4. Si  $k = 2$ ,  $\alpha$  est racine double ou d'ordre 2 de  $P$ .
  5. Si  $k = 3$ ,  $\alpha$  est racine triple de  $P$ .
  6.  $\alpha$  est racine multiple lorsque  $\alpha$  est racine d'ordre au moins 2.

### Propriété 17.

Soit  $k \in \mathbb{N}^*$  et  $P \in \mathbb{K}[X]$ . Si  $\alpha \in \mathbb{K}$  est racine d'ordre  $k$  de  $P$ , alors  $\alpha$  est racine d'ordre  $k - 1$  de  $P'$ .

**Remarque 4.** En particulier, si  $\alpha$  est racine simple de  $P$  alors  $\alpha$  n'est pas racine de  $P'$ .

### Propriété 18 (Caractérisation de l'ordre des racines).

$\alpha \in \mathbb{K}$  est racine d'ordre  $k$  de  $P$  si et seulement si  $\begin{cases} P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0 \\ P^{(k)}(\alpha) \neq 0 \end{cases}$ .

Cas particulier : si  $k = 2$ ,  $\alpha$  est racine double de  $P$  ssi  $P(\alpha) = 0$ ,  $P'(\alpha) = 0$  et  $P''(\alpha) \neq 0$ .

### Propriété 19.

Soit  $P$  un polynôme non nul admettant  $\alpha_1, \dots, \alpha_p$  pour racines distinctes avec ordres de multiplicité  $r_1, \dots, r_p$ .  
Alors  $\prod_{k=1}^p (X - \alpha_k)^{r_k} \mid P$  et  $\deg(P) \geq r_1 + r_2 + \dots + r_p$ .

### Définition 12 (Polynôme scindé).

Un polynôme non nul est **scindé** ssi il admet des racines dont la somme des multiplicités est égale à son degré.

### Propriété 20.

On reprend le contexte de la propriété précédente.  $P$  est scindé ssi  $\exists a \in \mathbb{K}^*$  tel que  $P = a \prod_{k=1}^p (X - \alpha_k)^{r_k}$ .

Si  $\deg P = 0$  ou  $\deg P = 1$ ,  $P$  est scindé.  $X^2 + 1$  est scindé dans  $\mathbb{C}[X]$  mais pas dans  $\mathbb{R}[X]$ .

**Remarque 5.** Un polynôme de degré  $n \geq 0$  admet au plus  $n$  racines comptées avec multiplicité.

► Exemple :  $X^4 + X^2 + 1$  est-il scindé dans  $\mathbb{R}[X]$  ?

### Définition 13 (Fonctions symétriques élémentaires des racines).

Soit  $P = a_0 + a_1X + \dots + a_nX^n$  un polynôme de degré  $n \in \mathbb{N}^*$  scindé de  $K[X]$ .

Soient  $x_1, \dots, x_n$  les racines de  $P$  (distinctes ou non).

$\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}$  est appelée  $k^{\text{ème}}$  fonction symétrique élémentaire des racines du polynôme  $P$ .

**Remarque 6.** Dans  $\sigma_k$  on a ajouté tous les produits possibles de  $k$  racines.  $\sigma_1$  est la somme des racines,  $\sigma_2$  est la somme des produits deux-à-deux des racines,  $\sigma_n$  est le produit des racines.

### Propriété 21 (Relations entre coefficients et racines d'un polynôme scindé : formules de Viète).

Dans le contexte de la définition précédente,  $\sigma_k = \frac{(-1)^k a_{n-k}}{a_n}$ .

En particulier  $\sigma_1 = x_1 + \dots + x_n = \frac{-a_{n-1}}{a_n}$  et  $\sigma_n = x_1 \times \dots \times x_n = (-1)^n \frac{a_0}{a_n}$ .

Démonstration :  $P = a_0 + a_1X + \dots + a_nX^n = a_n(X - x_1)(X - x_2) \dots (X - x_n)$ . On développe et on identifie les termes constants, les termes de premier degré, etc...

► Exemples :

1. si  $n = 2$ ,  $P = aX^2 + bX + c = a(X - x_1)(X - x_2)$  ( $a \neq 0$ )
 
$$\begin{cases} \sigma_1 = x_1 + x_2 = \frac{-b}{a} \\ \sigma_2 = x_1x_2 = \frac{c}{a} \end{cases}.$$
2. si  $n = 3$ ,  $P = a_3X^3 + a_2X^2 + a_1X + a_0 = a(X - x_1)(X - x_2)(X - x_3)$  ( $a_3 \neq 0$ )
 
$$\begin{cases} \sigma_1 = x_1 + x_2 + x_3 = \frac{-a_2}{a_3} \\ \sigma_2 = x_1x_2 + x_2x_3 + x_1x_3 = \frac{a_1}{a_3} \\ \sigma_3 = x_1x_2x_3 = \frac{-a_0}{a_3} \end{cases}.$$
3. si  $n = 4$ ,  $P = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = a(X - x_1)(X - x_2)(X - x_3)(X - x_4)$  ( $a_4 \neq 0$ )
 
$$\begin{cases} \sigma_1 = x_1 + x_2 + x_3 + x_4 = \frac{-a_3}{a_4} \\ \sigma_2 = x_1x_2 + x_2x_3 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4 = \frac{a_2}{a_4} \\ \sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_2x_3x_4 + x_1x_3x_4 = \frac{-a_1}{a_4} \\ \sigma_4 = x_1x_2x_3x_4 = \frac{a_0}{a_4} \end{cases}.$$

### Définition 14.

Une **équation algébrique** est une équation du type  $P(x) = 0$ , où  $P \in \mathbb{K}[X]$ .

Résoudre une équation algébrique c'est trouver les racines d'un polynôme.

### Définition 15.

Les équations  $Q(x) = 0$  et  $P(x) = 0$  sont équivalentes ssi  $P$  et  $Q$  ont les mêmes racines avec les mêmes ordres de multiplicité ssi  $P$  et  $Q$  sont proportionnels.

Rappel : Si  $P \in \mathbb{K}[X]$  est de degré  $n$  ( $n \in \mathbb{N}^*$ ) alors  $P(x) = 0$  a au plus  $n$  racines (distinctes ou confondues).

★ Exercice : Déterminer  $x, y, z$  tels que

$$\begin{cases} x + y + z = 1 \\ x^2 + y^2 + z^2 = 9 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1 \end{cases}$$

► Méthode : exprimer le système en fonction des fonctions symétriques élémentaires  $\sigma_1, \sigma_2$  et  $\sigma_3$ . Puis trouver un polynôme dont  $x, y$  et  $z$  soient les racines.

## 5 Polynômes irréductibles

### Définition 16.

Soit  $P \in \mathbb{K}[X]^*$ .  $P$  est **irréductible** ssi les seuls polynômes qui divisent  $P$  sont

- les constantes non nulles,
- les polynômes proportionnels (associés) à  $P$ .

Cette définition dépend du corps de référence.

$P$  n'est **pas irréductible** ssi  $\exists (A_1, A_2) \in (\mathbb{K}[X])^2$  tel que  $P = A_1A_2$ ,  $\deg(A_1) \geq 1$  et  $\deg(A_2) \geq 1$ .

$P$  n'est **pas irréductible** ssi  $\exists (A_1, A_2) \in (\mathbb{K}[X])^2$  tel que  $P = A_1A_2$ ,  $\deg(A_1) < \deg(P)$  et  $\deg(A_2) < \deg(P)$ .

► Exemple :  $X^2 + 1$  est irréductible dans  $\mathbb{R}[X]$  mais est réductible dans  $\mathbb{C}[X]$  :  $X^2 + 1 = (X - i)(X + i)$ .

► Exemple :  $X^2 - 2$  est irréductible dans  $\mathbb{Q}[X]$  mais est réductible dans  $\mathbb{R}[X]$  :  $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ .

Les polynômes constants non nuls sont irréductibles.

### 5.1 Factorisation dans $\mathbb{C}[X]$ :

**Théorème 5 (Théorème de d'Alembert-Gauss).**

Tout polynôme de  $\mathbb{C}[X]$  de degré supérieur ou égal à 1 possède au moins une racine dans  $\mathbb{C}$ . On en déduit les deux propriétés suivantes :

- Tout polynôme de  $\mathbb{C}[X]$  de degré  $n \in \mathbb{N}$  possède exactement  $n$  racines (distinctes ou non).
  - Les polynômes irréductibles de  $\mathbb{C}[X]$  sont les polynômes de degré 1 et les polynômes constants non nuls.
- On dit que  $\mathbb{C}$  est un corps algébriquement clos.

Ce théorème est admis en MPSI.

**Remarque 7.** Tout polynôme  $P$  de  $\mathbb{C}[X]$  s'écrit donc  $P = a \prod_{i=1}^m (X - z_i)^{r_i}$ ,  $a \in \mathbb{C}^*$ ,  $\sum_{i=1}^m r_i = \deg(P)$ .

Par conséquent, tout polynôme de  $\mathbb{C}[X]$  est scindé.

**Définition 17 (Polynôme conjugué).**

On appelle **polynôme conjugué** de  $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{C}[X]$  le polynôme  $\bar{P} = \bar{a}_0 + \bar{a}_1X + \dots + \bar{a}_nX^n$ .

**Propriété 22.**

Soient  $P, Q \in \mathbb{C}[X]$  et  $\lambda, \alpha \in \mathbb{C}$ .

1.  $\overline{P + Q} = \bar{P} + \bar{Q}$ .
2.  $\overline{\lambda \cdot Q} = \bar{\lambda} \cdot \bar{Q}$ .
3.  $\overline{PQ} = \bar{P} \bar{Q}$ .
4.  $\overline{\bar{P}} = P$ .
5.  $\bar{P} = P$  ssi  $P \in \mathbb{R}[X]$ .
6. Si  $P|Q$  alors  $\bar{P}|\bar{Q}$ .
7.  $\alpha$  est racine de  $P$  ssi  $\bar{\alpha}$  est racine de  $\bar{P}$ .
8.  $\alpha$  est racine d'ordre de multiplicité  $p$  de  $P$  ssi  $\bar{\alpha}$  est racine d'ordre de multiplicité  $p$  de  $\bar{P}$ .

► Exemple :  $j$  est racine de  $X^4 + X^2 + 1$  donc  $\bar{j}$  aussi.

► Exemple : Factorisation de  $x^n - 1$ .

**5.2 Factorisation dans  $\mathbb{R}[X]$  :**

Soit  $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{R}[X]$  avec  $a_n \neq 0$ .

$P \in \mathbb{C}[X]$  et  $\bar{P} = P$ .

$P$  a  $n$  racines complexes réparties en  $k$  racines réelles distinctes  $x_1, \dots, x_k$  d'ordre de multiplicité  $p_1, \dots, p_k$  et  $2j$  racines non réelles :  $z_1$  et  $\bar{z}_1$  d'ordre de multiplicité  $q_1$ ,  $z_2$  et  $\bar{z}_2$  d'ordre de multiplicité  $q_2$ ,  $\dots$ ,  $z_j$  et  $\bar{z}_j$  d'ordre de multiplicité  $q_j$ .

$P$  s'écrit donc :

$P = a_n(X - x_1)^{p_1} \dots (X - x_k)^{p_k} (X - z_1)^{q_1} (X - \bar{z}_1)^{q_1} \dots (X - z_j)^{q_j} (X - \bar{z}_j)^{q_j}$  et  $n = p_1 + \dots + p_k + 2(q_1 + \dots + q_j)$ .

On peut donc énoncer la propriété suivante :

**Propriété 23.**

Si  $n$  est impair,  $p_1 + \dots + p_k \neq 0$ ,  $P$  possède au moins une racine réelle.

Or  $(X - z_i)^{q_i} (X - \bar{z}_i)^{q_i} = [(X - z_i)(X - \bar{z}_i)]^{q_i} = [X^2 - (z_i + \bar{z}_i)X + z_i\bar{z}_i]^{q_i}$

$= [X^2 - 2\operatorname{Re}(z_i)X + |z_i|^2]^{q_i}$

$X^2 - 2\operatorname{Re}(z_i)X + |z_i|^2$  est irréductible dans  $\mathbb{R}[X]$ .  $\Delta = (\operatorname{Re}(z_i))^2 - |z_i|^2 = -(\operatorname{Im}(z_i))^2 < 0$  car  $z_i \notin \mathbb{R}$ .

On obtient la **décomposition de Gauss** suivante, où  $n = p_1 + \dots + p_k + 2(q_1 + \dots + q_j)$  :

$$P = a_n(X - x_1)^{p_1} \dots (X - x_k)^{p_k} [X^2 - 2\operatorname{Re}(z_1)X + |z_1|^2]^{q_1} \dots [X^2 - 2\operatorname{Re}(z_j)X + |z_j|^2]^{q_j} .$$

**Propriété 24.**

Les polynômes irréductibles de  $\mathbb{R}[X]$  sont

- les polynômes de degré 0,
- les polynômes de degré 1,
- les polynômes de degré 2 dont le discriminant est strictement négatif.

► Méthode : Pour décomposer un polynôme en produit de facteurs irréductibles sur  $\mathbb{R}$ , on peut le décomposer d'abord sur  $\mathbb{C}$ , puis regrouper tous les facteurs conjugués.

► Exemple :  $X^6 - 1 = (X^3 + 1)(X^3 - 1) = (X + 1)(X^2 - X + 1)(X - 1)(X^2 + X + 1)$ .

► Exemple :  $X^n - 1 = (X - e^{0\frac{i\pi}{n}})(X - e^{2\frac{i\pi}{n}})(X - e^{4\frac{i\pi}{n}}) \cdots (X - e^{2(n-1)\frac{i\pi}{n}})$ .

Si  $n$  est impair,  $X^n - 1 = (X - 1)(X^2 - 2 \cos \frac{2\pi}{n} X + 1) \cdots (X^2 - 2 \cos \frac{(n-1)\pi}{n} X + 1)$ .

Si  $n$  est pair,  $X^n - 1 = (X - 1)(X + 1)(X^2 - 2 \cos \frac{2\pi}{n} X + 1) \cdots (X^2 - 2 \cos \frac{(n-2)\pi}{n} X + 1)$ .

► Exemple :  $X^4 + 1 = (X^2 + i)(X^2 - i) = (X + e^{\frac{i\pi}{4}})(X - e^{\frac{i\pi}{4}})(X + e^{-\frac{i\pi}{4}})(X - e^{-\frac{i\pi}{4}})$

$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ .

Autre méthode :  $X^4 + 1 = (X^2 + 1)^2 - 2X^2$ .

**6 Arithmétique dans  $\mathbb{K}[X]$** **6.1 PGCD****Définition 18 (Un PGCD de deux polynômes dont l'un au moins est non nul).**

Soient  $P$  et  $Q$  deux polynômes dont l'un au moins est non nul. Un PGCD de  $P$  et de  $Q$  est un polynôme qui appartient à l'ensemble des diviseurs communs à  $P$  et à  $Q$  et qui est de degré maximal.

**Propriété 25 (Propriétés d'un PGCD).**

Soient  $P$  et  $Q$  deux polynômes non nuls.

- Si  $Q|P$  alors les PGCD de  $P$  et de  $Q$  sont les polynômes associés à  $Q$ .
- Les PGCD de  $P$  et de  $0$  sont les polynômes associés à  $P$ .
- Si  $P = BQ + R$  avec  $B \neq 0$  et  $(Q, R) \in \mathbb{K}[X]^2$  alors l'ensemble des diviseurs communs à  $P$  et  $B$  est égal à l'ensemble des diviseurs de  $B$  et de  $R$ .
- Si  $A$  et  $B$  sont deux polynômes, l'un au moins étant non nul. Soit  $D$  un PGCD de  $A$  et de  $B$ , alors l'ensemble des diviseurs de  $D$  est égal à l'ensemble des diviseurs de  $A$  et de  $B$ .
- Si  $A$  et  $B$  sont deux polynômes, l'un au moins étant non nul. Soient  $D_1$  et  $D_2$  deux PGCD de  $A$  et de  $B$ .  $D_1$  et  $D_2$  sont non nuls et associés.

**Définition 19 (Le PGCD de deux polynômes dont l'un au moins est non nul).**

Soient  $A$  et  $B$  deux polynômes dont l'un au moins est non nul. Il existe un unique polynôme unitaire  $D$  tel que  $D$  est un PGCD de  $A$  et de  $B$ . On l'appelle le PGCD de  $A$  et de  $B$  et on le note  $A \wedge B$ .

Remarque :  $A \wedge B = B \wedge A$ .

Point méthode : le pgcd de  $P$  et de  $Q$  est le polynôme unitaire  $D$  tel que  $D|A$ ,  $D|B$  et si  $P \in \mathbb{K}[X]$  est tel que  $P|A$  et  $P|B$  alors  $P|D$ .

**Propriété 26 (Calcul pratique du PGCD).**

Le dernier reste non nul dans l'algorithme d'Euclide donne un PGCD.

► Exemple : Déterminer le PGCD de  $X^4 + 2X^3 + 2X^2 + 7X + 6$  et  $X^5 + 3X^4 + 2X^3 - X^2 - 3X - 2$  avec l'algorithme d'Euclide.

**Propriété 27 (Relation de Bézout).**

Si  $P$  et  $Q$  sont deux polynômes non nuls,  $\exists(U, V) \in \mathbb{K}[X]^2$ ,  $PU + QV = P \wedge Q$ .  $(U, V)$  est appelé couple de coefficients de Bézout.

► Exemple : Reprise de l'exercice précédent en déterminant  $U$  et  $V$ .

**6.2 Polynômes premiers entre eux****Définition 20 (Couples de polynômes premiers entre eux).**

Soient  $A$  et  $B$  deux polynômes de  $\mathbb{C}[X]$ , l'un au moins étant non nul. Alors  $A$  et  $B$  sont premiers entre eux ssi leur PGCD est égal à 1.

**Théorème 6 (Théorème de Bézout).**

Pour tout  $A, B \in \mathbb{K}[X]^*$ ,  $A \wedge B = 1$  ssi  $\exists U, V \in \mathbb{K}[X]$ ,  $AU + BV = 1$ .

**Propriété 28 (Lemme de Gauss).**

Soient  $A, B, C$  trois polynômes non nuls. Si  $A|BC$  et si  $A \wedge B = 1$  alors  $A|C$ .

**Propriété 29.**

Soient  $A$  et  $B$  deux polynômes non tous les deux nuls et  $D$  leur PGCD. Il existe deux polynômes  $A_1$  et  $B_1$  premiers entre eux tels que  $A = DA_1$  et  $B = DB_1$ .

**Propriété 30 (Produit et nombres premiers entre eux).**

1. Soient  $A, B, C$  trois polynômes non nuls. Si  $A \wedge B = 1$  et si  $A \wedge C = 1$  alors  $A \wedge BC = 1$ .
2. Pour tout  $(A, B_1, \dots, B_n) \in (\mathbb{K}[X]^*)^{n+1}$ , si  $\forall i \in [[1, n]]$ ,  $A \wedge B_i = 1$  alors  $A \wedge (B_1 B_2 \dots B_n) = 1$
3. Si  $A$  et  $B$  sont premiers entre eux et divisent  $C$ , alors  $AB$  divise  $C$ .

**Propriété 31 (Couples de polynômes premiers entre eux).**

Soient  $A$  et  $B$  deux polynômes de  $\mathbb{C}[X]$ , l'un au moins étant non nul. Alors  $A$  et  $B$  sont premiers entre eux ssi ils n'ont pas de racine (complexe) commune.

**Définition 21 (PGCD d'un nombre fini de polynômes).**

Soit  $p \in \mathbb{N}^*$ . Soit  $(A_1, \dots, A_p) \in \mathbb{K}[X]^p \setminus \{(0, \dots, 0)\}$ . Le PGCD de  $A_1, \dots, A_p$ , noté  $A_1 \wedge \dots \wedge A_p$ , est le polynôme unitaire  $D$  tel que  $\mathcal{D}(D) = \mathcal{D}(A_1) \cap \mathcal{D}(A_2) \cap \dots \cap \mathcal{D}(A_p)$ .

**Propriété 32 (Identité de Bézout).**

Soit  $p \in \mathbb{N}^*$ . Soit  $(A_1, \dots, A_p) \in \mathbb{K}[X]^p \setminus \{(0, \dots, 0)\}$  et  $D$  leur PGCD. Il existe  $(U_1, \dots, U_p) \in \mathbb{K}[X]^p$  tel que  $D = A_1 U_1 + \dots + A_p U_p$ .

**Propriété 33 (Polynômes premiers entre eux dans leur ensemble).**

$A_1, \dots, A_p$  sont dits premiers entre eux dans leur ensemble ssi  $A_1 \wedge \dots \wedge A_p = 1$ .

Cela signifie qu'ils n'ont pas de diviseurs communs autres que les polynômes constants non nuls.

**Propriété 34 (Polynômes premiers entre eux deux à deux).**

$A_1, \dots, A_p$  sont dits premiers entre eux deux à deux ssi  $\forall (i, j) \in [[1, p]]^2, i \neq j \Rightarrow A_i \wedge A_j = 1$ .

Si les  $A_i$  sont premiers entre eux deux à deux alors ils sont premiers entre eux dans leur ensemble mais la réciproque est fautive. Par exemple,  $(X - 1)(X - 2)$ ,  $(X - 5)(X - 2)$  et  $(X - 5)(X - 1)$  sont premiers entre eux dans leur ensemble mais ne sont pas premiers entre eux deux à deux.

**Propriété 35 (Corollaire - Identité de Bézout).**

Soit  $p \in \mathbb{N}^*$ . Soit  $(A_1, \dots, A_p) \in \mathbb{K}[X]^p \setminus \{(0, \dots, 0)\}$ .  $A_1, \dots, A_p$  sont premiers entre eux dans leur ensemble ssi il existe  $(U_1, \dots, U_p) \in \mathbb{K}[X]^p$  tel que  $1 = A_1 U_1 + \dots + A_p U_p$ .

**6.3 PPCM****Définition 22 (un PPCM de deux polynômes dont l'un au moins est non nul).**

Soient  $A$  et  $B$  deux polynômes dont l'un au moins est non nul. Un PPCM de  $A$  et de  $B$  est un polynôme de l'ensemble des multiples de  $A$  et de  $B$  qui a un degré minimal.

Point méthode : un ppcm de  $A$  et de  $B$  est un polynôme  $M$  tel que  $A|M, B|M$  et si  $P \in \mathbb{K}[X]$  est tel que  $A|P$  et  $B|P$  alors  $M|P$ .

**Définition 23 (le PPCM de deux polynômes dont l'un au moins est non nul).**

Soient  $A$  et  $B$  deux polynômes dont l'un au moins est non nul. Le PPCM de  $A$  et de  $B$  est l'unique polynôme de l'ensemble des multiples de  $A$  et de  $B$  qui a un degré minimal et qui est unitaire.

**Propriété 36 (Propriétés du PPCM).**

Soient  $A$  et  $B$  deux polynômes non nuls.

- Si  $A$  et  $B$  sont premiers entre eux alors  $(A \vee B)$  et  $AB$  sont associés.
- Les polynômes  $AB$  et  $(A \vee B)(A \wedge B)$  sont associés.

- Exemple : Montrer qu'un polynôme irréductible est premier avec tous les polynômes qu'il ne divise pas.
- Exemple : Montrer que  $P$  et  $Q$  sont premiers entre eux ssi  $P + Q$  et  $PQ$  le sont.

**7 Fractions rationnelles****Définition 24 (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  $Q \neq 0$ .

Une fraction rationnelle est donc le quotient de deux polynômes.

Si  $P_1, Q_1, P_2$  et  $Q_2$  sont quatre polynômes tels que  $Q_1 \neq 0$  et  $Q_2 \neq 0$ , on a :

$$\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{P_1 Q_2 + P_2 Q_1}{Q_1 Q_2} \quad \text{et} \quad \frac{P_1}{Q_1} \times \frac{P_2}{Q_2} = \frac{P_1 P_2}{Q_1 Q_2}$$

**Définition 25 (Corps des fractions rationnelles).**

On admet que l'ensemble noté  $\mathbb{K}(X)$ , contenant l'anneau commutatif  $\mathbb{K}[X]$  et dont tout élément s'écrit comme le quotient d'un élément de  $\mathbb{K}[X]$  par un élément non nul de  $\mathbb{K}[X]$ , muni des opérations  $+$  et  $\times$ , est un corps commutatif.

$$K(X) = \left\{ \frac{P}{Q} / P, Q \in \mathbb{K}[X], Q \neq 0 \right\}$$

Ce corps  $K(X)$  s'appelle le corps des fractions rationnelles à coefficients dans  $\mathbb{K}$ .

Soit  $F \in \mathbb{K}(X)$ . On dit qu'un couple  $(P, Q) \in \mathbb{K}[X]^2$  tel que  $Q \neq 0$  et  $F = \frac{P}{Q}$  est un représentant de la fraction rationnelle  $F$ . Ce couple n'est pas unique.  $P$  est appelé numérateur et  $Q$  dénominateur.

### Définition 26 (Forme irréductible d'une fraction rationnelle).

- On appelle représentant irréductible d'une fraction rationnelle  $F$  tout couple  $(P, Q) \in \mathbb{K}[X]^2$  tel que  $Q \neq 0$ ,  $P$  et  $Q$  sont premiers entre eux et  $F = \frac{P}{Q}$ . On dit que  $\frac{P}{Q}$  est une forme irréductible de  $F$ .
- Toute fraction rationnelle  $F \in K(X)$  s'écrit de façon unique sous la forme  $F = \frac{A}{B}$  avec  $A$  et  $B$  polynômes premiers entre eux et  $B$  unitaire;  $A$  est le numérateur réduit de  $F$  et  $B$  son dénominateur réduit. On dit que  $\frac{A}{B}$  est la forme irréductible unitaire de  $F$ .

Si  $\frac{P_1}{Q_1}$  est la forme irréductible unitaire d'une fraction rationnelle  $F$  alors les représentants de  $F$  sont les couples  $(AP_1, AQ_1)$  avec  $A \in \mathbb{K}[X]$  non nul. Les représentants irréductibles de  $F$  sont les couples  $(aP_1, aQ_1)$  avec  $a \in \mathbb{K}^*$ . Donner la forme unitaire irréductible de  $P \in \mathbb{K}[X]$ , de  $O$ .

## 7.1 Racines et pôles d'une fraction rationnelle

### Définition 27 (Racines et pôles).

Les racines d'une fraction rationnelle sont les racines de son numérateur réduit, et ses pôles celles de son dénominateur réduit, avec les ordres de multiplicité correspondants.

Ex : racines et pôles de  $\frac{X^4 - 1}{X^2(X + 1)}$ , sur  $\mathbb{R}$ , sur  $\mathbb{C}$ .

## 7.2 Degré d'une fraction rationnelle

### Définition 28 (Degré).

Si  $F \in K(X)$  s'écrit  $\frac{A}{B}$  et  $\frac{C}{D}$ , alors  $\deg A - \deg B = \deg C - \deg D$ ; par définition, cet entier est le degré de  $F$ .

Remarque : une fraction rationnelle de degré positif n'est pas forcément un polynôme. C'est le cas par exemple de  $F = \frac{X^4 + 1}{X^2}$ .

### Propriété 37 (Propriétés sur les degrés des fractions rationnelles).

Si  $F$  et  $G$  sont deux fractions rationnelles, alors

$$\deg(F + G) \leq \max(\deg F, \deg G)$$

$$\deg(FG) = \deg F + \deg G$$

## 7.3 Evaluation en un point - fonction rationnelle

### Définition 29 (Fonction rationnelle).

Si  $F$  est une fraction rationnelle d'écriture irréductible unitaire  $\frac{A}{B}$  et  $x$  un scalaire non pôle de  $F$ , on pose  $F(x) = \frac{A(x)}{B(x)}$ ; la fonction rationnelle associée à  $F$ , d'ensemble de définition  $\mathbb{K} \setminus \{\text{pôles de } F\}$  est la fonction  $x \mapsto F(x)$ .

**Propriété 38 (Fonctions rationnelles égales).**

Si deux fractions rationnelles prennent les mêmes valeurs en tout point d'une partie infinie de  $\mathbb{K}$ , alors elles sont égales.

De même qu'un polynôme est caractérisé par sa fonction polynomiale, une fraction rationnelle est caractérisée par sa fonction rationnelle associée.

**7.4 Partie entière d'une fraction rationnelle****Définition 30.**

Si  $F \in K(X)$  s'écrit  $\frac{A}{B}$  et  $\frac{C}{D}$ , alors le quotient de la division euclidienne de  $A$  par  $B$  est le même que celui de la division euclidienne de  $C$  par  $D$ ; on appelle ce polynôme la partie entière (ou polynomiale) de  $F$ .

**Remarque 8.** — Toute fraction rationnelle s'écrit de manière unique comme la somme de sa partie entière et d'une fraction rationnelle de degré strictement négatif que l'on appelle partie fractionnaire.

- si  $F$  est de degré  $< 0$ , sa partie entière est le polynôme nul.
- la partie entière d'une somme de fractions rationnelles est la somme des parties entières de chaque fraction rationnelle (différence avec la partie entière définie sur  $\mathbb{R}$ ).
- la partie entière d'une fonction rationnelle  $f$  de degré  $> 0$  est une fonction polynomiale asymptote à  $f$  au voisinage de  $+\infty$  et  $-\infty$ .

► Exemple : Déterminer la partie entière de  $F = \frac{X^4}{X^3 + 5X + 1}$ . Déterminer l'équation de l'asymptote oblique en  $\pm\infty$  à la courbe représentative de  $x \mapsto \frac{x^4}{x^3 + 5x + 1}$ .

**8 Décomposition en éléments simples sur  $\mathbb{R}$  et sur  $\mathbb{C}$** **8.1 Existence et unicité de la décomposition****Théorème 7 (Partie polaire relative à un pôle, admis).**

Soit  $F \in K(X)$ ,  $x_0$  un pôle d'ordre  $k$  de  $F$  ; alors il existe un unique  $(a_1, \dots, a_k) \in K^k$  et une unique  $G \in K(X)$  tels que

$$F = \frac{a_1}{X - x_0} + \dots + \frac{a_k}{(X - x_0)^k} + G$$

avec  $x_0$  non pôle de  $G$

$\frac{a_1}{X - x_0} + \dots + \frac{a_k}{(X - x_0)^k}$  est appelé partie polaire de  $F$  relative au pôle  $x_0$ ,  $a_q$  est appelé résidu d'ordre  $q$  de  $F$  relatif au pôle  $x_0$  et  $a_1$  est appelé résidu.

**Théorème 8 (Décomposition en éléments simples, admis).**

Toute fraction rationnelle est somme de ses parties polaires et d'une fraction rationnelle sans pôle; cette écriture s'appelle la décomposition de  $F$  en éléments simples de première espèce.

Plus précisément, si  $F = \frac{A}{(X - x_1)^{\alpha_1} \dots (X - x_p)^{\alpha_p} Q}$  avec  $Q$  sans racine dans  $K$ , alors

$F = F_1 + \dots + F_p + H$  où  $F_i$  est la partie polaire de  $F$  relative à  $x_i$  et  $H$  est une fraction rationnelle qui n'a pas de pôle dans

**Propriété 39 (Détermination de la partie polaire d'un pôle simple).**

Si  $x_0$  est un pôle simple de  $F = \frac{A}{B}$ , alors  $B$  s'écrit  $(X - x_0)Q$  avec  $Q(x_0) \neq 0$ .

La partie polaire associée au pôle  $x_0$  est alors :  $\frac{a_1}{X - x_0}$  avec

$$a_1 = \frac{A(x_0)}{Q(x_0)} = \frac{A(x_0)}{B'(x_0)}$$

► Exemple : Déterminer les parties polaires de  $F = \frac{X^2 - 1}{X^2 - 5X + 6}$ .

**Propriété 40 (Détermination de la partie polaire d'un pôle double).**

Si  $x_0$  est un pôle double de  $F = \frac{A}{B}$ , alors  $B$  s'écrit  $(X - x_0)^2 Q$  avec  $Q(x_0) \neq 0$ .

La partie polaire associée au pôle  $x_0$  est alors :  $\frac{a_1}{X - x_0} + \frac{a_2}{(X - x_0)^2}$  avec

$$a_1 \in \mathbb{K} \text{ et } a_2 = \frac{A(x_0)}{Q(x_0)}$$

Pour trouver  $a_1$ , retrancher à la fraction rationnelle  $F - \frac{a_2}{(X - x_0)^2}$  pour obtenir une nouvelle fraction rationnelle dont  $x_0$  n'est pas un pôle ou est un pôle simple. ► Exemple : Déterminer les parties polaires de  $\frac{X^4 - 8X^2 + 9X - 7}{(X - 2)^2(X + 3)}$ .

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

Soit  $F = \frac{P}{Q}$  une fraction rationnelle complexe irréductible dont le dénominateur est décomposé en produit de facteurs irréductibles :  $Q = (X - \alpha_1)^{k_1} \cdots (X - \alpha_r)^{k_r}$ .

Alors on peut écrire, sous une unique forme : Alors la décomposition suivante est unique :

$$F = \frac{P}{Q} = E(F) + \frac{a_{1,1}}{(X - \alpha_1)^{k_1}} + \frac{a_{1,2}}{(X - \alpha_1)^{k_1-1}} + \cdots + \frac{a_{1,k_1}}{(X - \alpha_1)} \\ + \frac{a_{2,1}}{(X - \alpha_2)^{k_2}} + \frac{a_{2,2}}{(X - \alpha_2)^{k_2-1}} + \cdots + \frac{a_{2,k_2}}{(X - \alpha_2)} \\ + \cdots \\ + \frac{a_{r,1}}{(X - \alpha_r)^{k_r}} + \frac{a_{r,2}}{(X - \alpha_r)^{k_r-1}} + \cdots + \frac{a_{r,k_r}}{(X - \alpha_r)}$$

► Exemple : Vérifier que  $\frac{1}{X^2 + 1} = \frac{a}{X + i} + \frac{b}{X - i}$  avec  $a = \frac{1}{2}i$ ,  $b = -\frac{1}{2}i$ .

► Exemple : Décomposition de  $\frac{P'}{P}$ .

**8.3 Décomposition en éléments simples sur  $\mathbb{R}$**

**Théorème 10 (Décomposition en éléments simples de première et deuxième espèce sur  $\mathbb{R}$ ).**

Soit  $F = \frac{A}{B}$  une fraction rationnelle réelle irréductible dont le dénominateur est décomposé en produit de facteurs irréductibles :  $B = (X - x_1)^{\alpha_1} \dots (X - x_p)^{\alpha_p} (X^2 + u_1X + v_1)^{\beta_1} \dots (X^2 + u_qX + v_q)^{\beta_q}$ .

Alors on peut écrire, sous une unique forme :

$$F = E(F) + \left( \frac{a_{11}}{X - x_1} + \dots + \frac{a_{1\alpha_1}}{(X - x_1)^{\alpha_1}} \right) + \dots + \left( \frac{a_{p1}}{X - x_p} + \dots + \frac{a_{p\alpha_p}}{(X - x_p)^{\alpha_p}} \right) \\ + \left( \frac{b_{11}X + c_{11}}{X^2 + u_1X + v_1} + \dots + \frac{b_{1\beta_1}X + c_{1\beta_1}}{(X^2 + u_1X + v_1)^{\beta_1}} \right) + \dots + \left( \frac{b_{q1}X + c_{q1}}{X^2 + u_qX + v_q} + \dots + \frac{b_{q\beta_q}X + c_{q\beta_q}}{(X^2 + u_qX + v_q)^{\beta_q}} \right)$$

Autrement dit,  $\frac{A}{B}$  s'écrit de manière unique comme somme :

- d'une partie polynomiale,
- d'éléments simples de première espèce du type  $\frac{a}{(X - \alpha)^i}$ ,
- d'éléments simples de deuxième espèce 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  $B(X)$  et les exposants  $i$  sont inférieurs ou égaux à la puissance correspondante dans cette factorisation.

On peut passer par la décomposition en éléments simples sur  $\mathbb{C}$  puis regrouper les termes conjugués ou directement déterminer les termes de la décomposition du théorème.

► Exemple : Décomposition en éléments simples de  $\frac{P(X)}{Q(X)} = \frac{3X^4 + 5X^3 + 11X^2 + 5X + 3}{(X^2 + X + 1)^2(X - 1)}$ . Comme  $\deg P < \deg Q$  alors  $E = 0$ . 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 utiliser les méthodes qui suivent pour déterminer les coefficients afin d'obtenir :

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

Quelques méthodes pour déterminer les coefficients de la décomposition en éléments simples d'une fraction rationnelle, dans le cas où le dénominateur est scindé :

1. Simplifier la fraction.
2. Déterminer la partie entière par division euclidienne.
3. Écrire la décomposition avec des coefficients à calculer.
4. On peut toujours mettre au même dénominateur et égaliser les coefficients des numérateurs ; on obtient alors un système d'équations linéaires à résoudre.

Exemple :  $\frac{X^3 + 1}{X^3(X - 1)^2} = \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X^3} + \frac{d}{X - 1} + \frac{e}{(X - 1)^2}$  aboutit au système 
$$\begin{cases} a + d = 0 \\ -2a + b - d + e = 1 \\ a - 2b + c = 0 \\ b - 2c = 0 \\ c = 1 \end{cases}$$

Mais on peut souvent être plus rapide.

5. Les résidus d'ordre maximum se calculent directement avec la formule  $a_k = \frac{A(x_0)}{Q'(x_0)}$ .
6. Pour les autres résidus, on peut retrancher les fractions obtenues de la fraction de départ, simplifier, et chercher les résidus précédents.

7. Evaluer en des valeurs particulières (non pôles) donne des relations.

Exemple :  $\frac{X}{(X-1)^2(X+1)} = \frac{1}{2} \frac{1}{(X-1)^2} + \frac{a}{X-1} - \frac{1}{4} \frac{1}{X+1}$

$X := 0$  donne immédiatement  $a = \dots\dots\dots$

8. Si la fraction rationnelle est paire ou impaire, changer  $X$  en  $-X$  et utiliser l'unicité.

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

L'imparité donne :

Calcul de  $b$

9. Si la fraction rationnelle est réelle et qu'il y a des pôles complexes non réels, conjuguer ; les résidus des pôles conjugués sont conjugués.

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

La conjugaison donne :

10. exploiter la limite de  $x \mapsto x^{-deg(F)} f(x)$  où  $f$  est la fonction rationnelle associée à  $F$ .

11. s'il reste encore  $q$  coefficients à calculer, multiplier par  $X^q$  et égaliser les parties entières des deux membres. On obtient l'égalité de deux polynômes de degré  $\leq q-1$ , d'où  $q$  relations, et les  $q$  coefficients restants.

$$\frac{X^3+1}{X^3(X-1)^2} = \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X^3} + \frac{d}{X-1} + \frac{e}{(X-1)^2}$$

(a) multiplier par  $X^3$  et faire  $X := 0$  donne  $c = 1$ .

(b) multiplier par  $(X-1)^2$  et faire  $X := 1$  donne  $e = 2$ .

(c) multiplier par  $X^3$  et prendre les parties entières des deux membres donne

$$\left\lfloor \frac{X^3+1}{X^2-2X+1} \right\rfloor = aX^2 + bX + 1 + d \left\lfloor \frac{X^3}{X-1} \right\rfloor + 2 \left\lfloor \frac{X^3}{X^2-2X+1} \right\rfloor$$

soit  $X+2 = aX^2 + bX + 1 + d(X^2 + X + 1) + 2(X+2)$

$$\text{d'où } \begin{cases} 0 = a + d \\ 1 = b + d + 2 \\ 2 = 1 + d + 4 \end{cases}$$

Pour (c) on aurait aussi pu faire d'abord  $X := -1$  qui donnait une relation, puis multiplier par  $X^2$  et prendre les parties entières des deux membres.

### 8.4 Application au calcul de primitives, de dérivées $k$ -ièmes

— Déterminer une primitive de  $f : x \mapsto \frac{3x^4 + 5x^3 + 11x^2 + 5x + 3}{(x^2 + x + 1)^2(x - 1)}$  sur  $]1, +\infty[$ .

— Soit  $n \in \mathbb{N}$ . Calculer la dérivée d'ordre  $n$  de  $f : x \mapsto \frac{x^2 - 1}{x^2 - 5x + 6}$ .

## 9 Polynômes interpolateurs de Lagrange

### Définition 31 (Polynômes de Lagrange).

Soit  $n \in \mathbb{N}^*$  et  $x_1, \dots, x_n$   $n$  éléments de  $\mathbb{K}$  distincts. On considère alors la famille de polynômes  $(L_i)_{1 \leq i \leq n}$  définie par

$$\forall i \in \llbracket 1, n \rrbracket, L_i = \prod_{k=1, k \neq i}^n \frac{X - x_k}{x_i - x_k}$$

Ecrire les trois polynômes de Lagrange associés aux nombres -1, 2 et 3.

**Théorème 11 (Interpolation de Lagrange).**

Soit  $n \in \mathbb{N}^*$ ,  $x_1, \dots, x_n$   $n$  éléments de  $\mathbb{K}$  distincts et  $y_1, \dots, y_n$  des éléments de  $\mathbb{K}$ . Il existe un unique polynôme  $P$  de  $\mathbb{K}_{n-1}[X]$  tel que

$$\forall i \in [[1, n]], P(x_i) = y_i$$

Existence : on montre que le polynôme  $P = \sum_{j=1}^n y_j L_j$  convient. Unicité : on montre que si deux polynômes conviennent alors ils coïncident en suffisamment de points et sont donc égaux.

Soit  $f$  une fonction définie sur une partie  $I$  de  $\mathbb{R}$  à valeurs dans  $\mathbb{R}$ . Soit  $n \in \mathbb{N}^*$ . Etant donné  $x_1, \dots, x_n$  des éléments de  $I$  distincts, il existe un unique polynôme  $P$  de  $\mathbb{K}_{n+1}[X]$  tel que

$$\forall i \in [[1, n]], P(x_i) = f(x_i)$$

Ce polynôme est appelé polynôme d'interpolation de Lagrange de  $f$  associé à la famille  $(x_1, \dots, x_n)$ .

► Exemple : Déterminer le polynôme de  $\mathbb{R}_2[X]$  tel que  $P(-1) = 2$ ,  $P(2) = 3$  et  $P(3) = 5$ .