

# Chapitre 18

## Polynômes (1)

Dans tout ce chapitre,  $K$  est un corps commutatif ( $\mathbb{R}$  ou  $\mathbb{C}$  en général), et  $n, m, p, r$  des entiers naturels. Des écritures du type  $a_i, b_i, \dots$  pour  $i \in \mathbb{N}$  désignerons toujours des éléments de  $K$ .

### 1 Définitions

#### 1.1 Polynômes à une indéterminée

**Définition 1.1 (Polynôme à une indéterminée)**

Un *polynôme à une indéterminée*  $X$  à coefficients dans  $K$  est une somme formelle

$$\sum_{k=0}^n a_k X^k \quad \text{où} \quad a_k \in K \quad \text{pour tout} \quad k = 0, \dots, n, \quad n \in \mathbb{N}$$

et où par définition on a

$$\sum_{k=0}^n a_k X^k = \sum_{k=0}^m b_k X^k \iff \forall k = 0, \dots, \max(n, m), \quad a_k = b_k,$$

où par convention  $a_k = 0$  si  $k > n$  et  $b_k = 0$  si  $k > m$ . On note  $K[X]$  l'ensemble des polynômes à une indéterminée à coefficients dans  $K$ .

#### Remarques.

1. On a bien sûr  $K \subset K[X]$ , puisque si  $a \in K$ , on a  $a = aX^0$ .
2. Si  $P = \sum_{k=0}^n a_k X^k$ , on a aussi  $P = \sum_{k=0}^m a_k X^k$  si  $m \geq n$ , et  $a_k = 0$  pour  $k > n$ .
3. Attention : on ne peut pas donner de valeur à  $X$ . C'est une notation formelle pour repérer la position du coefficient  $a_k$ . Toute écriture du type  $X = 2$  est à bannir.

**Définition 1.2 (Polynômes constants)**

1. Un polynôme  $P$  est constant s'il est de la forme  $aX^0$ , où  $a \in K$ . On note alors simplement  $P = a$ .

2. On définit le polynôme nul (et on le note 0) par :  $0 = 0X^0$ .
3. On définit le polynôme constant égal à 1 (et on le note 1) par :  $1 = 1X^0$ .

**Définition 1.3 (Degré d'un polynôme)**

Soit un polynôme  $P = \sum_{k=0}^n a_k X^k$  avec  $P \neq 0$ .

1. Le *degré* de  $P$  est le plus grand des entiers  $k \in \{0, \dots, n\}$  tel que

$$a_k \neq 0 \quad \text{et} \quad \forall j = k+1, \dots, n, a_j = 0,$$

où par convention  $a_{n+1} = 0$ . On note  $\deg(P)$  le degré de  $P$ .

2. On note  $K_n[X]$  l'ensemble des polynômes de degrés  $\leq n$ .
3. Par convention, le degré du polynôme nul est  $-\infty$ .
4. Le coefficient  $a_{\deg(P)}$  est le *coefficient* dominant de  $P$ .
5. Le polynôme  $P$  est *unitaire* si son coefficient dominant vaut 1.

**Proposition 1.4**

Soit  $P = \sum_{k=0}^n a_k X^k \in K[X]$ . Alors :

1.  $\deg(P) \leq n$ .
2.  $\deg(P) = n$  si et seulement si  $a_n \neq 0$ .
3. Si  $a_p \neq 0$  pour un certain  $p \in \llbracket 0, n \rrbracket$ , alors  $\deg(P) \geq p$ .

**Proposition 1.5**

Les polynômes de degré 0 sont les polynômes constants non nuls.

**Remarques.**

1. On voit par la définition que si  $d$  est le degré d'un polynôme  $P$ , on a

$$P = \sum_{k=0}^d a_k X^k = \sum_{k=0}^n a_k X^k$$

pour tout entier  $n \geq d$  avec  $a_k = 0$  pour  $k > d$ . Par exemple,

$$1 + 3X^2 - 7X^5 = 1 + 3X^2 - 7X^5 + 0.X^6 + 0.X^7.$$

On note parfois

$$P = \sum_{k=0}^{+\infty} a_k X^k = \sum_k a_k X^k.$$

avec  $a_k = 0$  pour  $k > d$ . Cette notation est très utile lorsqu'on ne veut pas introduire le degré d'un polynôme.

2. On peut bien entendu utiliser  $Y$ ,  $T$ , .. comme notation pour l'indéterminée.

3. Un polynôme et une fonction polynomiale, ce n'est pas tout à fait la même chose. On verra qu'en sup (*i.e.* si  $K = \mathbb{R}$  ou  $K = \mathbb{C}$ ), on pourra confondre les deux, mais ce n'est pas le cas si le corps  $K$  contient un nombre fini d'éléments.
4. On peut construire l'ensemble des polynômes comme l'ensemble des suites nulles à partir d'un certain rang, avec  $X = (0, 1, 0, 0, \dots)$ .

## 1.2 Somme, produit

### Définition 1.6 (Somme, produit)

Soient  $n, m \in \mathbb{N}$ ,  $\lambda \in K$ , et  $P = \sum_{k=0}^n a_k X^k \in K[X]$ ,  $Q = \sum_{k=0}^m b_k X^k \in K[X]$ .

1. On définit  $\lambda P$  par  $\lambda P = \sum_{k=0}^n \lambda a_k X^k$ .
2. On définit la somme  $P + Q$  par  $P + Q = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k$ , où  $a_k = 0$  si  $k > n$  et  $b_k = 0$  si  $k > m$ .
3. On définit le produit  $PQ$  par  $PQ = \sum_{k=0}^{n+m} \left( \sum_{i=0}^k a_i b_{k-i} \right) X^k = \sum_{k=0}^{n+m} \left( \sum_{i+j=k} a_i b_j \right) X^k$ , où  $a_i = 0$  pour  $i > n$  et  $b_j = 0$  pour  $j > m$ .

### Remarques.

1. Il n'y a aucune raison pour que  $n$  soit le degré de  $P$ , ou  $m$  le degré de  $Q$ . Cela n'a aucune importance.
2. Pour obtenir un  $X^k$  dans un produit, on multiplie un  $X^i$  par un  $X^j$  tels que  $i + j = k$ .

### Exemples.

1. On a

$$(a_0 + a_1 X)(b_0 + b_1 X + b_2 X^2) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0) X^3 = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1) X^2 + a_1 b_2 X^3.$$

2. On a

$$(a_0 + a_1 X + a_2 X^2 + a_3 X^3)(b_0 + b_1 X + b_2 X^2) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0) X^3 + (a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4) X^4 + (a_0 b_5 + a_1 b_4 + a_2 b_3 + a_3 b_2 + a_4 b_1 + a_5 b_0) X^5 = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + (a_1 b_2 + a_2 b_1 + a_3 b_0) X^3 + (a_3 b_1 + a_2 b_2) X^4 + a_3 b_2 X^5$$

**Proposition 1.7 (Structure d'anneau)**

L'ensemble  $K[X]$  muni de l'addition et de la multiplication définies en 1.6 est un anneau commutatif, dont les éléments neutres pour l'addition et la multiplication sont respectivement les polynômes constants égaux à 0 et 1.

**Proposition 1.8 (Autres écritures du produit)**

Soient  $n, m \in \mathbb{N}$ , et deux polynômes à coefficients dans  $K$  :  $P = \sum_{k=0}^n a_k X^k$  et  $Q = \sum_{k=0}^m b_k X^k$ . On a

$$PQ = \sum_{i=0}^n \sum_{j=0}^m a_i b_j X^{i+j} = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m}} a_i b_j X^{i+j},$$

où  $a_i = 0$  pour  $i > n$  et  $b_j = 0$  pour  $j > m$ .

**1.3 Intégrité de  $K[X]$** **Proposition 1.9 (Degré d'un produit)**

Soient  $P, Q \in K[X]$ . Alors  $\deg(PQ) = \deg(P) + \deg(Q)$  (somme dans  $\overline{\mathbb{R}}$ ).

**Proposition 1.10 (Degré d'une somme)**

Soient  $P, Q \in K[X]$ . Alors

1.  $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ .
2. Si  $\deg(P) \neq \deg(Q)$ , alors  $\deg(P + Q) = \max(\deg(P), \deg(Q))$ .

**Corollaire 1.11**

Soit  $P \in K[X]$ ,  $P \neq 0$ , et  $n \in \mathbb{N}$ . Alors  $\deg(P^n) = n \deg(P)$ .

**Corollaire 1.12**

Soit  $n \in \mathbb{N}^*$  et  $P_1, \dots, P_n \in K[X]$ . Alors  $\deg(P_1 + \dots + P_n) \leq \max(\deg(P_1), \dots, \deg(P_n))$ .

**Proposition 1.13**

1. L'anneau  $K[X]$  est intègre.
2. Les éléments inversibles de  $K[X]$  sont les polynômes constants non nuls.

**1.4 Composée de polynômes****Définition 1.14**

Soient  $P, Q \in K[X]$ . On définit le polynôme composé  $P \circ Q$  par

$$P \circ Q = P(Q(X)) = \sum_k a_k Q^k \quad \text{si} \quad P = \sum_k a_k X^k.$$

**Exemples.**

1. Les polynômes pairs sont les polynômes qui s'écrivent  $P(X^2)$ , et les polynômes impairs ceux qui s'écrivent  $XP(X^2)$ .
2.  $X^2 \circ (X + 1) = (X + 1)^2$  et  $(X + 1) \circ X^2 = X^2 + 1$ .
3. Attention,  $(X + 1)P \neq P(X + 1)!!$

**Proposition 1.15**

Soient  $A, B, R \in K[X]$ . Alors  $(A \circ R) \times (B \circ R) = (AB) \circ R$  et  $(A + B) \circ R = A \circ R + B \circ R$ .

**Proposition 1.16**

Soient  $A, B \in K[X]$  avec  $B$  non constant. Alors  $\deg(A \circ B) = \deg(A) \deg(B)$ .

## 2 Division euclidienne

**Définition 2.1 (Diviseurs, multiples)**

Le polynôme  $A$  *divise*  $B$  s'il existe un polynôme  $D$  tel que

$$B = AD, \quad \text{noté } A|B.$$

Le polynôme  $B$  est alors un *multiple* de  $A$  et  $A$  un *diviseur* de  $B$ .

**Définition 2.2**

Les polynômes  $A$  et  $B$  sont *associés* s'il existe  $\lambda \in K^*$  tel que  $A = \lambda B$ , et on note  $A \sim B$ .

**Exemples.**

1.  $(X - 1)(X - 2)$  divise  $(X - 1)^2(X - 2)(X^2 + X + 1)$ .
2. Le polynôme nul ne divise que lui-même mais est divisible par tous les polynômes.
3. Les polynômes  $6X^2 - 3X + 12$  et  $4X^2 - 2X + 8$  sont associés.

**Proposition 2.3**

Soient  $A$  et  $B$  deux polynômes. Si  $A|B$  et si  $B \neq 0$ , alors  $\deg(A) \leq \deg(B)$ .

**Proposition 2.4**

Deux polynômes  $A$  et  $B$  sont associés si et seulement si  $A$  divise  $B$  et  $B$  divise  $A$ .

**Théorème 2.5 (Division euclidienne)**

Soient  $A, B$  deux polynômes avec  $B$  non nul. Alors il existe un unique couple  $(Q, R)$  de polynômes tel que

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

**Exemple.**

Division de  $A = 2X^4 - 3X^3 + 3X^2 + 6X + 1$  par  $B = 2X^2 + X - 1$ . On trouve  $Q = X^2 - 2X + 3$  et  $R = X + 4$ .

**Méthode 2.6**

Si  $a \in K$ , on a pour tout polynôme  $P$

$$P = (X - a)Q + b,$$

où  $b \in K$  puisque le reste dans la division par  $X - a$  doit être de degré nul ou  $-\infty$ . En évaluant l'égalité en  $a$ , on obtient  $b = P(a)$ .

### 3 Polynôme dérivé

Dans ce §,  $K \subset \mathbb{C}$ , donc  $\mathbb{Q} \subset K$ .

**Définition 3.1 (Polynôme dérivé)**

Soit  $P = \sum_{k=0}^n a_k X^k \in K[X]$ .

1. Le polynôme dérivé de  $P$  est le polynôme  $P' = \sum_{k=1}^n k a_k X^{k-1}$ .
2. On définit par récurrence le polynôme dérivé d'ordre  $n \in \mathbb{N}^*$

$$P^{(n)} = (P^{(n-1)})',$$

où  $P^{(0)} = P$ .

**Proposition 3.2**

Soient  $P \in K[X]$ . Alors  $P' = 0$  si et seulement si  $P$  est constant.

**Proposition 3.3**

Soient  $P, Q \in K[X]$  et  $\lambda, \mu \in K$ .

1.  $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$ .
2.  $(PQ)' = P'Q + PQ'$ .

**Proposition 3.4**

Pour  $p, n \in \mathbb{N}$ , on a

$$(X^n)^{(p)} = \begin{cases} \frac{n!}{(n-p)!} X^{n-p} & \text{si } n \geq p \\ 0 & \text{sinon.} \end{cases}$$

**Proposition 3.5**

Soient  $P \in K[X]$  non constant.

1.  $\deg(P') = \deg(P) - 1$  et  $\text{dom}(P') = \deg(P)\text{dom}(P)$ .

2. Pour tout  $n \leq \deg(P)$ , on a  $\deg(P^{(n)}) = \deg(P) - n$ .
3.  $P^{(\deg(P))} = (\deg(P))! \operatorname{dom}(P)$ .
4.  $P^{(\deg(P)+1)} = 0$ .

**Proposition 3.6 (Formule de Leibniz)**

Soient  $P, Q$  deux polynômes et  $n \in \mathbb{N}$ . Alors  $(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$ .

## 4 Racines d'un polynôme

### 4.1 Fonction polynomiale, formule de Taylor

**Définition 4.1 (Fonction polynomiale)**

Soit  $P = \sum_{k=0}^n a_k X^k \in K[X]$ .

1. La fonction polynomiale associée à  $P$  est la fonction

$$\begin{aligned} \tilde{P} : K &\longrightarrow K \\ x &\longmapsto \sum_{k=0}^n a_k x^k. \end{aligned}$$

2. Soit  $\alpha \in K$ . On note  $P(\alpha) = \tilde{P}(\alpha) = \sum_{k=0}^n a_k \alpha^k$ .

**Théorème 4.2 (Formule de Taylor)**

Soit  $P \in K[X]$  et  $a \in K$ . Alors

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

**Remarque.**

Soit  $P \in K[X]$  et  $a \in K$ . Alors, pour tout  $m \geq \deg(P)$ , on a  $P(X) = \sum_{k=0}^m \frac{P^{(k)}(a)}{k!} (X - a)^k$ , puisque  $P^{(k)}(a) = 0$  si  $k > \deg(P)$ .

**Méthode 4.3 (Quotient et reste par  $(X - a)^n$ )**

Soient  $P \in K[X]$ ,  $n \in \mathbb{N}^*$  et  $a \in K$ . Alors le quotient et le reste de la division euclidienne de  $P$  par

$(X - a)^n$  sont respectivement  $\sum_{k=n}^{+\infty} \frac{P^{(k)}(a)}{k!} (X - a)^{k-n}$  et  $\sum_{k=0}^{n-1} \frac{P^{(k)}(a)}{k!} (X - a)^k$ , car

$$P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} (X - a)^k = (X - a)^n \sum_{k=n}^{+\infty} \frac{P^{(k)}(a)}{k!} (X - a)^{k-n} + \sum_{k=0}^{n-1} \frac{P^{(k)}(a)}{k!} (X - a)^k.$$

## 4.2 Racine simple

### Définition 4.4 (Racine)

Un scalaire  $a \in K$  est *racine* d'un polynôme  $P$  si  $P(a) = 0$ .

### Exemple.

$i$  et  $-i$  sont des (les!) racines de  $X^2 + 1$  vu dans  $\mathbb{C}[X]$ .

### Proposition 4.5

Soient  $A$  et  $B$  deux polynômes et  $a \in K$  une racine de  $A$ . Si  $A|B$ , alors  $a$  est une racine de  $B$ .

### Proposition 4.6

Soit  $P \in K[X]$  et  $\alpha \in K$ . Alors  $\alpha$  est une racine de  $P$  si et seulement si  $X - \alpha | P$ .

### Proposition 4.7

Soit  $P \in K[X]$  et  $\alpha_1, \dots, \alpha_n \in K$  des scalaires deux à deux distincts. Alors les  $\alpha_i$  sont des racines de  $P$  si et seulement si  $\prod_{i=1}^n (X - \alpha_i) | P$ .

### Corollaire 4.8

Un polynôme de degré  $n \in \mathbb{N}$  admet au plus  $n$  racines distinctes.

### Méthode 4.9

On utilise souvent cette proposition par contraposée, pour montrer qu'un polynôme est nul.

1. Si un polynôme  $P$  vérifie  $\deg(P) \leq n$ ,  $n \in \mathbb{N}$ , et a au moins  $n + 1$  racines distinctes, alors  $P = 0$ .
2. On peut mélanger avec une démonstration par l'absurde : soit  $P$  un polynôme, et on suppose qu'il est non nul, et on note  $n \in \mathbb{N}$  son degré. Si on montre qu'alors  $P$  a au moins  $n + 1$  racines distinctes, on aboutit à une contradiction.
3. Un polynôme qui admet une infinité de racines distinctes est nul.

### Exemples.

1. On a vu dans le chapitre sur  $\mathbb{C}$  que pour tout entier  $n$ , il existe un polynôme  $P$  tel que pour tout  $x \in \mathbb{R}$ ,

$$\cos(nx) = P(\cos(x)).$$

(Écrire que  $\cos(nx)$  est la partie réelle de  $(\cos(x) + i \sin(x))^n$ ). Un tel polynôme est unique. En effet, si  $Q$  en est un autre, on a

$$(P - Q)(\cos(x)) = 0$$

pour tout réel  $x$ , donc  $P - Q$  s'annule sur  $[0, 1]$ , donc  $P - Q = 0$ .

2. La fonction exponentielle n'est pas polynomiale. En effet, si elle l'était, il existerait un polynôme  $P$  tel que pour tout nombre complexe  $z$ , on ait

$$P(z) = e^z.$$



En particulier, pour tout nombre entier  $k$ ,

$$P(2ik\pi) = 1,$$

donc  $P = 1$  et l'exponentielle serait constante : absurde.

3. Le polynôme  $X^n - 1$  admet  $n$  racines complexes distinctes qui sont les racines  $n^{\text{ème}}$  de l'unité, et

$$X^n - 1 = \prod_{k=0}^{n-1} \left( X - e^{\frac{2ik\pi}{n}} \right).$$

4. Le corollaire 4.8 permet d'identifier un polynôme et sa fonction polynomiale lorsque le corps  $K$  est infini (par exemple  $\mathbb{R}$  ou  $\mathbb{C}$ ), *i.e.* si  $P$  et  $Q$  sont deux polynômes, on a

$$P = Q \iff \tilde{P} = \tilde{Q} \iff \forall a \in K, P(a) = Q(a).$$

En effet, l'implication de gauche à droite est évidente. Pour l'autre, si  $P(a) = Q(a)$  pour tout  $a \in K$ , le polynôme  $P - Q$  admet une infinité de racines, donc est nul.

### 4.3 Racines multiples

#### Définition 4.10 (Ordre de multiplicité)

1. Un polynôme  $P$  admet  $a \in K$  comme racine d'ordre  $n \in \mathbb{N}^*$  si  $(X - a)^n$  divise  $P$  et  $(X - a)^{n+1}$  ne divise pas  $P$ . L'entier  $n$  est *l'ordre de multiplicité* de la racine  $a$ .
2. Un polynôme  $P$  admet  $a \in K$  comme racine d'ordre au moins  $n \in \mathbb{N}^*$  si  $(X - a)^n$  divise  $P$ .

#### Remarques.

1. On peut prolonger cette définition à  $n = 0$  : une racine d'ordre 0 n'est pas une racine.
2.  $(X - a)^n$  divise  $P$  et  $(X - a)^{n+1}$  ne divise pas  $P$  signifie que  $P = (X - a)^n Q$  avec  $Q(a) \neq 0$ .

#### Définition 4.11 (Racine simple, multiple)

Une racine simple (resp. multiple) de  $P \in K[X]$  est une racine d'ordre exactement 1 (resp. d'ordre au moins 2).

#### Remarques.

1. Il y a donc deux manières de compter les racines : on compte les racines distinctes, où on les compte avec leur ordre de multiplicité. L'exemple  $(X - 2)^2(X + 3)^4(X - 1)$  a 3 racines distinctes et 7 racines comptées avec leur ordre de multiplicité.
2. Une racine d'ordre  $n$  n'est pas une racine d'ordre  $p$  si  $p < n$  ou  $p > n$ .
3. Si  $a$  est une racine d'ordre exactement  $r$  de  $P$ , alors  $(X - a)^s \mid P$  si et seulement si  $s \leq r$ . En effet,  $(X - a)^{r+1} \nmid P$ .

**Exemple.**

Le polynôme  $(X - 2)^2(X + 3)^4(X - 1)$  admet 2 comme racine double,  $-3$  comme racine d'ordre 4 et 1 comme racine simple.

**Proposition 4.12 (Caractérisation d'une racine d'ordre au moins  $n$ )**

Un polynôme  $P \in K[X]$  admet  $a \in K$  comme racine d'ordre au moins  $n \in \mathbb{N}^*$  si et seulement si  $P(a) = \dots = P^{(n-1)}(a) = 0$ .

**Proposition 4.13 (Caractérisation d'une racine d'ordre  $n$ )**

Un polynôme  $P \in K[X]$  admet  $a \in K$  comme racine d'ordre  $n \in \mathbb{N}^*$  si et seulement si  $P(a) = \dots = P^{(n-1)}(a) = 0$  et  $P^{(n)}(a) \neq 0$ .

**Méthode 4.14 (Montrer qu'un scalaire est une racine multiple/simple)**

Soient  $a \in K$  et  $P \in K[X]$ .

1. Pour montrer que  $a$  est racine multiple de  $P$ , on montre que  $P(a) = P'(a) = 0$  ou que  $(X - a)^2$  divise  $P$ . Mais attention, cela ne donne pas son ordre de multiplicité.
2. Pour montrer que  $a$  est racine simple de  $P$ , on montre que  $P(a) = 0$  et  $P'(a) \neq 0$ , ou que  $X - a$  divise  $P$  et  $(X - a)^2$  ne divise pas  $P$ .

**Proposition 4.15**

Soient  $P \in K[X]$ ,  $a \in K$  et  $n \in \mathbb{N}^*$ . Si  $a$  est racine d'ordre (exactement)  $n$  de  $P$ , alors  $a$  est racine d'ordre (exactement)  $n - 1$  de  $P'$ .

**Remarque.**

Attention, la réciproque est fautive. Par exemple si  $P = X^2 + 1$ , alors  $P' = 2X$  admet 0 comme racine simple, mais 0 n'est pas racine double de  $P$ .

**Proposition 4.16**

Soient  $a_1, \dots, a_n \in K$  des scalaires distincts deux à deux, et  $r_1, \dots, r_n \in \mathbb{N}^*$ . Un polynôme  $P$  admet  $a_i$  comme racine d'ordre au moins  $r_i$  ( $i = 1, \dots, n$ ) si et seulement si

$$\prod_{i=1}^n (X - a_i)^{r_i} \mid P.$$

**Corollaire 4.17**

Un polynôme de degré  $n$  admet au plus  $n$  racines comptées avec leur ordre de multiplicité.

**Méthode 4.18 (Comparez avec la méthode 4.9)**

On utilise souvent ce corollaire par contraposée, pour montrer qu'un polynôme est nul.

1. Si un polynôme  $P$  vérifie  $\deg(P) \leq n$ ,  $n \in \mathbb{N}$ , et a au moins  $n + 1$  racines comptées avec multiplicités, alors  $P = 0$ .

2. On peut mélanger avec une démonstration par l'absurde : soit  $P$  un polynôme, et on suppose qu'il est non nul, et on note  $n \in \mathbb{N}$  son degré. Si on montre qu'alors  $P$  a au moins  $n + 1$  racines comptées avec multiplicités, on aboutit à une contradiction.
3. Un polynôme qui admet une infinité de racines comptées avec multiplicités est nul.

**Corollaire 4.19**

Soient  $a_1, \dots, a_n \in K$  des scalaires distincts deux à deux, et  $r_1, \dots, r_n \in \mathbb{N}^*$ . Un polynôme  $P$  de degré  $r_1 + \dots + r_n$  admet les  $a_i$  comme racine d'ordre  $r_i$  ( $i = 1, \dots, n$ ) si et seulement si

$$P = \lambda \prod_{i=1}^n (X - a_i)^{r_i}, \quad \lambda \in K^*.$$

**4.4 Polynômes scindés****Définition 4.20 (Polynôme scindé)**

Un polynôme  $P$  est *scindé sur*  $K$  s'il est non constant et s'il est produit de polynômes de degré 1.

**Remarque.**

Autrement dit, un polynôme est scindé s'il existe  $n \in \mathbb{N}^*$ ,  $x_1, \dots, x_n \in K$  et  $\lambda \in K^*$  tels que

$$P = \lambda \prod_{i=1}^n (X - x_i).$$

**Exemples.**

1.  $X^2 + 1$  n'est pas scindé sur  $\mathbb{R}$  mais est scindé sur  $\mathbb{C}$ .
2. D'après le corollaire 4.19, un polynôme est scindé si et seulement s'il admet  $n$  racines comptées avec leur multiplicité.

**Proposition 4.21 (Divisibilité en termes de racines)**

Soient  $A, B$  deux polynômes non nul, tel que  $A$  soit scindé. Soient  $a_1, \dots, a_n$  les racines de  $A$  deux à deux distinctes, et  $r_1, \dots, r_n \in \mathbb{N}^*$  leur ordre de multiplicité. Alors

$$A|B \iff \forall k = 1, \dots, n, a_k \text{ est une racine de } B \text{ d'ordre } \geq r_k.$$

**Méthode 4.22**

1. Soient  $A, B$  deux polynômes non nuls, tel que  $A$  soit scindé. Pour montrer que  $A|B$ , on peut déterminer les racines de  $A$  ainsi que leur ordre de multiplicité. On vérifie qu'elles sont racines de  $B$  avec un ordre supérieur ou égal.
2. Cas particulier des polynômes à coefficients complexes : ils sont tous scindés, donc on peut appliquer le 1.
3. Cas particulier des polynômes à coefficients réels : si  $A, B \in \mathbb{R}[X]$ , on les considère comme des polynômes à coefficients complexes. On applique alors le 1 avec les racines (réelles et) complexes de  $A$ .

## 5 Étude de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

### Théorème 5.1 (Théorème fondamental de l'algèbre)

Tout polynôme complexe non constant admet au moins une racine dans  $\mathbb{C}$ .

### Corollaire 5.2

Tout polynôme complexe non constant est scindé sur  $\mathbb{C}$ .

### Remarque.

FAUX pour les polynômes réels dans  $\mathbb{R}$  :  $X^2 + 1$  n'est pas scindé sur  $\mathbb{R}$ .

### Méthode 5.3

On peut appliquer la méthode 4.22 pour montrer que  $A|B$ , puisque si  $A \in \mathbb{C}[X]$  est non constant, il est scindé.

### Méthode 5.4

Si  $A, B \in \mathbb{R}[X]$ , pour montrer que  $A|B$ , on peut appliquer la méthode 4.22 en considérant les racines complexes de  $A$ .

### Définition 5.5 (Polynôme conjugué)

Soit  $P = \sum_{k=0}^n a_k X^k \in \mathbb{C}[X]$ . On définit son polynôme conjugué par  $\overline{P} = \sum_{k=0}^n \overline{a_k} X^k$ .

### Proposition 5.6

Soit  $P \in \mathbb{C}[X]$  et  $z \in \mathbb{C}$ . Alors  $\overline{P(z)} = \overline{P}(\overline{z})$ .

### Proposition 5.7

Soit  $P \in \mathbb{C}[X]$  et  $k \in \mathbb{N}$ . Alors  $\overline{P^{(k)}} = \overline{P}^{(k)}$ .

### Proposition 5.8

Si  $P \in \mathbb{C}[X]$ , on a  $P \in \mathbb{R}[X] \iff P = \overline{P}$ .

### Proposition 5.9

Soit  $P \in \mathbb{C}[X]$  et  $a \in \mathbb{C}$ . Alors  $a$  est une racine d'ordre  $r$  de  $P$  si et seulement si  $\overline{a}$  est une racine d'ordre  $r$  de  $\overline{P}$ .

### Corollaire 5.10

Soit  $P \in \mathbb{R}[X]$  et  $a \in \mathbb{C}$ . Alors  $a$  est une racine d'ordre  $r$  de  $P$  si et seulement si  $\overline{a}$  est une racine d'ordre  $r$  de  $P$ .

### Proposition 5.11

Soit  $z \in \mathbb{C}$ . Alors  $(X - z)(X - \overline{z}) = X^2 - 2\operatorname{Re}(z)X + |z|^2$ .

**Proposition 5.12 (Décomposition dans  $\mathbb{R}[X]$ )**

Tout polynôme réel non constant est un produit de polynômes de degré 1 et de polynômes de degré 2 sans racine réelle.

**Remarque.**

Cela signifie donc qu'il existe  $a_1, \dots, a_n \in \mathbb{R}$ ,  $r_1, \dots, r_n \in \mathbb{N}^*$ ,  $b_1, \dots, b_m, c_1, \dots, c_m \in \mathbb{R}$ ,  $s_1, \dots, s_m \in \mathbb{N}^*$  et  $\lambda \in \mathbb{R}^*$  tels que

$$P = \lambda \left( \prod_{i=1}^n (X - a_i)^{r_i} \right) \left( \prod_{i=1}^m (X^2 + b_i X + c_i)^{s_i} \right),$$

où les  $X^2 + b_i X + c_i$  sont sans racine réelle.

**Méthode 5.13 (Factorisation d'un polynôme à coefficients réels)**

Soit  $P \in \mathbb{R}[X]$ . Pour le factoriser, on peut soit le factoriser dans  $\mathbb{R}[X]$  par des techniques "astucieuses", puis déterminer ses racines complexes, soit déterminer d'abord toutes les racines complexes, pour ensuite les regrouper avec leur conjugué, pour en déduire la factorisation dans  $\mathbb{R}[X]$ . Exemple avec  $X^6 - 1$ .

## 6 Fonctions symétriques élémentaires

**Définition 6.1 (Fonctions symétriques élémentaires)**

Soit

$$P = \sum_{k=0}^n a_k X^k$$

un polynôme de degré  $n$  (donc  $a_n \neq 0$ ). Pour  $i = 1, \dots, n$ , on définit les *fonctions symétriques élémentaires* par

$$\sigma_i = (-1)^i \frac{a_{n-i}}{a_n} \in K.$$

**Exemple.**

Si  $P = 2X^3 - X^2 + 1$ , on a

$$\sigma_1 = -\frac{-1}{2}, \quad \sigma_2 = \frac{0}{2}, \quad \sigma_3 = -\frac{1}{2}.$$

**Proposition 6.2**

Soit

$$P = \sum_{k=0}^n a_k X^k$$

un polynôme de degré  $n$  scindé sur  $K$ , et  $x_1, \dots, x_n$  ses racines (non nécessairement distinctes). Alors pour tout  $i = 1, \dots, n$ , on a

$$\sigma_i = \sum_{1 \leq k_1 < \dots < k_i \leq n} x_{k_1} \cdots x_{k_i}.$$

**Exemples.**

1. Si

$$P = 4(X - 2)(X + 3)(X - 1) = 4X^3 - 28X + 24,$$

on a

$$\sigma_1 = -2+3-1 = 0 = -\frac{0}{4}, \quad \sigma_2 = 2 \times (-3) + 2 \times 1 + (-3) \times 1 = -7 = \frac{-28}{4}, \quad \sigma_3 = 2 \times (-3) \times 1 = -6 = -\frac{24}{4}.$$

2.  $\sigma_1$  est la somme des racines et  $\sigma_n$  le produit des racines.

3. On a

$$a_n(X - x_1)(X - x_2)(X - x_3) = a_n(X^3 - (x_1 + x_2 + x_3)X^2 + (x_1x_2 + x_1x_3 + x_2x_3)X - x_1x_2x_3).$$

## 7 Polynôme d'interpolation de Lagrange

**Proposition 7.1**

Soient  $n \in \mathbb{N}^*$ ,  $(x_1, \dots, x_n) \in K^n$  deux à deux distincts, et  $(y_1, \dots, y_n) \in K^n$ . Il existe un unique polynôme  $P$  de degré  $\leq n - 1$  tel que

$$\forall k = 1, \dots, n, P(x_k) = y_k.$$

C'est le polynôme d'interpolation de Lagrange associé aux familles  $(x_k)_{1 \leq k \leq n}$  et  $(y_k)_{1 \leq k \leq n}$ .

**Définition 7.2**

Soit  $f$  est une fonction définie sur une partie de  $K$ ,  $(x_k)_{1 \leq k \leq n}$  une famille de scalaires deux à deux distincts dans le domaine de définition de  $f$ , et  $y_k = f(x_k)$  pour  $k = 1, \dots, n$ . Le polynôme de la proposition 7.1 est le polynôme d'interpolation de Lagrange de  $f$  associé à la famille  $(x_k)_{1 \leq k \leq n}$ .

**Proposition 7.3**

Soient  $n \in \mathbb{N}^*$ ,  $(x_1, \dots, x_n) \in K^n$  deux à deux distincts, et  $(y_1, \dots, y_n) \in K^n$ . Soit  $P_0$  le polynôme d'interpolation de Lagrange associé aux familles  $(x_k)_{1 \leq k \leq n}$  et  $(y_k)_{1 \leq k \leq n}$ . Les polynômes  $A \in K[X]$  tels que

$$\forall k = 1, \dots, n, A(x_k) = y_k$$

sont les polynômes  $P_0 + \left( \prod_{k=1}^n (X - x_k) \right) Q$ , où  $Q \in K[X]$ .