

Dans ce chapitre,  $\mathbf{K}$  désigne  $\mathbf{R}$  ou  $\mathbf{C}$ .

# I L'ensemble $\mathbf{K}[X]$

## 1 Définition

DÉFINITION

On appelle **polynôme** à une indéterminée et à coefficients dans  $\mathbf{K}$  toute expression de la forme :

$$P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

où  $n \in \mathbf{N}$  et  $(a_0, a_1, a_2, \dots, a_n) \in \mathbf{K}^{n+1}$ .  $X$  est appelée l'indéterminée.

Les éléments  $a_0, a_1, \dots, a_n$  de  $\mathbf{K}$  sont les **coefficients** du polynôme  $P$ .

L'ensemble des polynômes à une indéterminée et à coefficients dans  $\mathbf{K}$  est noté  $\mathbf{K}[X]$ .

Dans notre programme, on identifiera les polynômes à des **fonctions polynômiales** définies sur  $\mathbf{K}$ . L'indéterminée  $X$  jouera alors le rôle d'un réel ou d'un complexe.

$$P : \begin{cases} \mathbf{R} \rightarrow \mathbf{R} \\ x \mapsto \sum_{k=0}^n a_k x^k \end{cases} \quad \text{ou} \quad P : \begin{cases} \mathbf{C} \rightarrow \mathbf{C} \\ z \mapsto \sum_{k=0}^n a_k z^k \end{cases}$$

Cas Particuliers :

- On appelle **polynôme constant** tout polynôme de la forme  $a_0$  où  $a_0 \in \mathbf{K}$ .
- Le **polynôme nul** est celui dont tous les coefficients sont nuls. On le note  $0$ .
- On appelle **monôme** tout polynôme de la forme  $a_n X^n$  où  $n \in \mathbf{N}$  et  $a_n \in \mathbf{K}$ .

## 2 Égalité de polynômes

Deux polynômes  $P = \sum_{k=0}^p a_k X^k$  et  $Q = \sum_{k=0}^q b_k X^k$  sont égaux lorsqu'ils ont les mêmes coefficients :

$\forall k \in \mathbf{N}$ ,  $a_k = b_k$ , en convenant que :  $\forall k > p$ ,  $a_k = 0$  et  $\forall k > q$ ,  $b_k = 0$ .

Ainsi, lorsque deux polynômes sont égaux, on *identifie* leurs coefficients.

**Cas particulier** : Un polynôme est nul si, et seulement si, tous ses coefficients sont nuls.

*Exemple* : Si  $a, b, c \in \mathbf{R}$  sont tels que  $(a - 1)X^3 + (a + b)X^2 + (b - c)X = 6X^2 + 2X$ , alors ...

## 3 Degré d'un polynôme

DÉFINITION

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

On appelle **degré de**  $P$  et on note  $\deg(P)$  le plus grand entier  $k$  tel que  $a_k \neq 0$ .

On convient que  $\deg(0) = -\infty$ .

*Exemples* :

- si  $P = X^2 + 5X^3 + X^9$ , on a  $\deg(P) = 9$ .
- si  $P = \sum_{k=0}^n a_k X^k$ , on n'a pas nécessairement  $\deg(P) = n$  ; ce n'est le cas que si  $a_n \neq 0$ .
- les polynômes constants ont un degré  $n \leq 0$  ,  
les polynômes de degré nul sont les polynômes constants non nuls.

DÉFINITION

Soit  $P = \sum_{k=0}^n a_k X^k$  avec  $a_n \neq 0$  (donc  $\deg(P) = n$ ).

- $a_n X^n$  est appelé **monôme dominant** de  $P$ .
- $a_n$  est appelé **coefficient dominant** de  $P$ .
- Lorsque le coefficient dominant est égal à 1, le polynôme est dit **unitaire**.

*Exemple* :

Soit  $P = 8X^2 + 4X^7$ . Alors  $4X^7$  est le monôme dominant de  $P$  et 4 est son coefficient dominant.

## II Opérations sur les polynômes

### 1 Combinaisons linéaires sur $\mathbf{K}[X]$

#### a Somme de polynômes, produit par un scalaire

Soient  $P = \sum_{k=0}^p a_k X^k$  et  $Q = \sum_{k=0}^q b_k X^k$  dans  $\mathbf{K}[X]$ , et soit  $\lambda \in \mathbf{K}$ .

DÉFINITION

On définit la somme  $P + Q$  et le produit  $\lambda P$  par :

- $P + Q = \sum_{k=0}^{\max(p,q)} (a_k + b_k) X^k$ , avec la convention que  $a_k = 0$  si  $k > p$  et  $b_k = 0$  si  $k > q$ .
- $\lambda P = \sum_{k=0}^p \lambda a_k X^k$ .

*Exemple* : Soient  $P = 1 + 3X - X^2$  et  $Q = X + X^2$ . On a alors :

- $P + Q = 1 + 4X$ .
- $2P = 2 + 6X - 2X^2$ .

Une **combinaison linéaire** de  $P$  et  $Q$  est un polynôme  $\lambda P + \mu Q$ , avec  $\lambda, \mu \in \mathbf{K}$ .

*Remarque* : On notera  $P - Q$  la combinaison linéaire  $P + (-1)Q$ .

#### b Degré d'une combinaison linéaire

PROPOSITION

1.  $\forall P, Q \in \mathbf{K}[X], \quad \deg(P + Q) \leq \max(\deg P, \deg Q)$
2.  $\forall \lambda \in \mathbf{K}, \forall P \in \mathbf{K}[X], \quad \deg(\lambda P) = \begin{cases} \deg P & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0 \end{cases}$

*Remarque* : Si  $P$  et  $Q$  ont des degrés différents, alors  $\deg(P + Q) = \max(\deg P, \deg Q)$ .

Si  $P$  et  $Q$  sont de même degré, il est possible que  $\deg(P + Q) < \max(\deg P, \deg Q)$ , voir l'exemple précédent.

#### c Propriétés

PROPOSITION

L'addition est associative, commutative, et elle admet un élément neutre : le polynôme nul.

$\forall P, Q, R \in \mathbf{K}[X]$  :

- $P + (Q + R) = (P + Q) + R = P + Q + R$
- $P + Q = Q + P$
- $P + 0 = 0 + P = P$

DÉFINITION

Pour  $n \in \mathbf{N}$ , on note  $\mathbf{K}_n[X]$  l'ensemble des polynômes de degré **inférieur ou égal** à  $n$ .

*Exemple* :  $\mathbf{R}_2[X] = \{aX^2 + bX + c, (a, b, c) \in \mathbf{R}^3\}$ .

PROPOSITION

|  $\mathbf{K}_n[X]$  est stable par combinaison linéaire.

## 2 Multiplication des polynômes

#### a Définition

Soient  $P = \sum_{k=0}^p a_k X^k$  et  $Q = \sum_{k=0}^q b_k X^k$  dans  $\mathbf{K}[X]$ .

DÉFINITION

On définit le produit  $PQ$  par :  $PQ = \sum_{k=0}^{p+q} c_k X^k$  avec  $\forall k \in \llbracket 0, p+q \rrbracket, c_k = \sum_{i=0}^k a_i b_{k-i}$ ,  
et comme précédemment, avec la convention que  $a_k = 0$  si  $k > p$  et  $b_k = 0$  si  $k > q$ .

Exemple : Soient  $P = 1 + 3X - X^2$  et  $Q = X + X^2$ . On a :

$k$	0	1	2	3	4
$a_k$	1	3	-1	0	0
$b_k$	0	1	1	0	0
$c_k$	0	1	4	2	-1

$$\begin{aligned} c_0 &= a_0 b_0 = 0 \\ c_1 &= a_0 b_1 + a_1 b_0 = 1 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 = 4 \\ c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 2 \\ c_4 &= a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = -1 \end{aligned}$$

Ce qui donne finalement :  $PQ = X + 4X^2 + 2X^3 - X^4$ .

## b Propriétés

### PROPOSITION

1. Le produit des polynômes est associatif, commutatif, et il admet un élément neutre, le polynôme constant égal à 1. :  
 $\forall P, Q, R \in \mathbf{K}[X], P(QR) = (PQ)R = PQR, \quad PQ = QP \quad \text{et} \quad P \times 1 = 1 \times P = P.$
2. La multiplication des polynômes est distributive par rapport à l'addition :  
 $\forall P, Q, R \in \mathbf{K}[X], P(Q + R) = PQ + PR.$
3.  $\forall P, Q \in \mathbf{K}[X], \quad \deg(PQ) = \deg P + \deg Q$
4. Les seuls polynômes inversibles sont les polynômes constants non nuls.
5.  $\forall P, Q \in \mathbf{K}[X], \quad PQ = 0 \Leftrightarrow P = 0 \text{ ou } Q = 0.$

Preuves :

## III Dérivation dans $\mathbf{K}[X]$

### 1 Dérivée d'un polynôme

#### DÉFINITION

Soit  $P = \sum_{k=0}^p a_k X^k \in \mathbf{K}[X]$ . On définit le **polynôme dérivé de  $P$** , noté  $P'$ , par :

$$P' = \sum_{k=1}^p k a_k X^{k-1} = \sum_{k=0}^{p-1} (k+1) a_{k+1} X^k$$

On définit le **polynôme dérivé  $n$ -ième de  $P$** , noté  $P^{(n)}$ , par récurrence :

$$\begin{cases} P^{(0)} = P \\ \forall k \in \mathbf{N}, \quad P^{(k+1)} = (P^{(k)})' \end{cases}$$

Exemple :  $(1 + 3X - X^2)' = 3 - 2X$  et si  $P \in \mathbf{K}_0[X], \quad P' = 0.$

Remarque : Vu comme fonction de  $\mathbf{R}$  dans  $\mathbf{R}$ , cette définition de la dérivée d'un polynôme correspond à la définition de la dérivée d'une fonction réelle d'une variable réelle.

### 2 Degré du polynôme dérivé

#### PROPOSITION

1.  $\forall P \in \mathbf{K}[X], \quad \deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg P \geq 1 \\ -\infty & \text{si } \deg P \leq 0 \end{cases}$
2.  $\forall P \in \mathbf{K}[X], \quad \deg(P) \leq n \Rightarrow P^{(n+1)} = 0$

Exemples : Soit  $P = 2X^4 - 3X^2 + 5X - 4$ . Alors :

$$P' = \dots$$

$$P'' = \dots$$

$$P^{(3)} = \dots$$

$$P^{(4)} = \dots$$

$$\forall n > 4, \quad P^{(n)} = \dots$$

Soit  $n \in \mathbf{N}$  et  $P = X^n$ . Alors  $P^{(n)} = \dots$

### 3 Dérivation et opérations

PROPOSITION

1.  $\forall P, Q \in \mathbf{K}[X], \forall \lambda, \mu \in \mathbf{K}, (\lambda P + \mu Q)' = \lambda P' + \mu Q'$ .
2.  $\forall P, Q \in \mathbf{K}[X], (PQ)' = P'Q + PQ'$ .
3.  $\forall P \in \mathbf{K}[X], \forall n \in \mathbf{N}, (P^n)' = nP'P^{n-1}$ .

Preuves :

Démonstration

1. AQT.

2. Posons  $P = \sum_{k=0}^p a_k X^k$  et  $Q = \sum_{k=0}^q b_k X^k$ .

- D'une part, par définition du produit :  $PQ = \sum_{k=0}^{p+q} d_k X^k$  avec  $\forall k \in \mathbf{N}, d_k = \sum_{i=0}^k a_i b_{k-i}$

$$\text{Et donc } (PQ)' = \sum_{k=1}^{p+q} k d_k X^{k-1} = \sum_{k=0}^{p+q-1} (k+1) d_{k+1} X^k.$$

$$\text{Notons : } (PQ)' = \sum_{k=0}^{p+q-1} d'_k X^k \quad \text{avec } \forall k \in \mathbf{N}, d'_k = (k+1) d_{k+1} = (k+1) \sum_{i=0}^{k+1} a_i b_{k+1-i}$$

- D'autre part,  $P' = \sum_{k=1}^p k a_k X^{k-1} = \sum_{k=0}^{p-1} (k+1) a_{k+1} X^k$ .

$$\text{On peut poser } P' = \sum_{k=0}^{p-1} a'_k X^k \quad \text{avec } \forall k \in \mathbf{N}, a'_k = (k+1) a_{k+1}$$

$$\text{On obtient alors le produit : } P'Q = \sum_{k=0}^{p+q-1} \alpha_k X^k \quad \text{avec } \forall k \in \mathbf{N}, \alpha_k = \sum_{i=0}^k a'_i b_{k-i}$$

De même, en posant  $Q' = \sum_{k=1}^q b'_k X^{k-1}$  avec  $b'_k = (k+1) b_{k+1}$ , on a :

$$PQ' = \sum_{k=0}^{p+q-1} \beta_k X^k \quad \text{avec } \forall k \in \mathbf{N}, \beta_k = \sum_{i=0}^k a_i b'_{k-i}$$

En réunissant ces résultats,  $P'Q + PQ' = \sum_{k=0}^{p+q-1} \gamma_k X^k$  avec :

$$\forall k \in \mathbf{N}, \gamma_k = \alpha_k + \beta_k$$

$$\gamma_k = \sum_{i=0}^k a'_i b_{k-i} + \sum_{i=0}^k a_i b'_{k-i}$$

$$\gamma_k = \sum_{i=0}^k (i+1) a_{i+1} b_{k-i} + \sum_{i=0}^k a_i (k-i+1) b_{k-i+1}$$

$$\gamma_k = \sum_{i=1}^{k+1} i a_i b_{k-i+1} + \sum_{i=0}^k (k-i+1) a_i b_{k-i+1}$$

$$\gamma_k = \underbrace{(k+1) a_0 b_{k+1}}_{i=0} + \left[ \sum_{i=1}^k i a_i b_{k-i+1} \right] + \left[ \sum_{i=1}^k (k-i+1) a_i b_{k-i+1} \right] + \underbrace{(k+1) a_{k+1} b_0}_{i=k+1}$$

$$\gamma_k = (k+1) a_0 b_{k+1} + \sum_{i=1}^k [i a_i b_{k-i+1} + (k-i+1) a_i b_{k-i+1}] + (k+1) a_{k+1} b_0$$

$$\gamma_k = (k+1) a_0 b_{k+1} + \sum_{i=1}^k [(k+1) a_i b_{k-i+1}] + (k+1) a_{k+1} b_0$$

$$\gamma_k = (k+1) \sum_{i=0}^{k+1} a_i b_{k+1-i}$$

$$\gamma_k = d'_k$$

Par conséquent, on a bien :

$$\boxed{(PQ)' = P'Q + PQ'}$$

PROPOSITION

$$\forall P, Q \in \mathbb{K}[X], \forall n \in \mathbb{N}, \quad (PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

FORMULE DE LEIBNIZ

## IV Racines d'un polynôme

### 1 Définition

DÉFINITION

Soit  $P \in \mathbb{K}[X]$  et  $\alpha \in \mathbb{K}$ .

On dit que  $\alpha$  est **une racine de  $P$**  (ou **un zéro de  $P$** ) lorsque  $P(\alpha) = 0$ .

*Exemple* : 1 est une racine de  $P = X^2 - 1$  car  $P(1) = 1^2 - 1 = 0$ .

**Rappel** : On trouve les racines dans  $\mathbb{K}$  d'un polynôme  $P$  de degré 2 en calculant son discriminant.

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

DÉFINITION

Soient  $A, P \in \mathbb{K}[X]$ . On dit que  $A$  **divise**  $P$  s'il existe un polynôme  $Q$  tel que  $P = AQ$ .

On note alors  $A|P$ , et on dit que  $A$  est **un diviseur** de  $P$  ou que  $P$  est **un multiple** de  $A$ .

*Exemples* :

- $(X - 1)|(X^2 - 1)$  car  $X^2 - 1 = (X - 1)(X + 1)$ .
- Tous les polynômes divisent 0.
- Si  $\deg P = 0$ , alors  $P$  divise tout polynôme.
- $\forall P \in \mathbb{K}[X], \quad 0|P \Leftrightarrow P = 0$ .
- Si  $P, Q \in \mathbb{K}[X]$  et  $P|Q$  avec  $Q \neq 0$ , alors  $\deg P \leq \deg Q$ .
- $X - 2$  divise  $X^3 - X^2 - 4$  car ...

PROPOSITION

1.  $\forall A \in \mathbb{K}[X], \quad A|A$
2.  $\forall A, B \in \mathbb{K}[X], \quad \begin{cases} A|B \\ B|A \end{cases} \iff \exists \lambda \in \mathbb{K}^*, \quad B = \lambda A.$
3.  $\forall A, B, C \in \mathbb{K}[X], \quad \begin{cases} A|B \\ B|C \end{cases} \Rightarrow A|C.$

Remarque : La divisibilité dans  $\mathbb{K}[X]$  n'est pas une relation d'ordre.

PROPOSITION

1.  $\forall A, P, Q \in \mathbb{K}[X], \quad A|P \Rightarrow A|PQ$
2.  $\forall A, P, Q \in \mathbb{K}[X], \quad \begin{cases} A|P \\ A|Q \end{cases} \Rightarrow A|P + Q$
3.  $\forall A, P, B, Q \in \mathbb{K}[X], \quad \begin{cases} A|P \\ B|Q \end{cases} \Rightarrow AB|PQ$
4.  $\forall A, P \in \mathbb{K}[X], \forall n \in \mathbb{N}, \quad A|P \Rightarrow A^n|P^n$

Attention :  $\begin{cases} A|P \\ B|P \end{cases} \not\Rightarrow AB|P.$

**Exercice** : Montrer que  $\forall n \in \mathbb{N}, \quad X^2|(X + 1)^n - nX - 1$ .

### 3 Caractérisation des racines

THÉORÈME

Soit  $P \in \mathbb{K}[X]$  et  $\alpha \in \mathbb{K}$ .

$\alpha$  est une racine de  $P$  si, et seulement si  $P$  est divisible par  $X - \alpha$ .

*Preuve (hors programme)* :

Démonstration

( $\Leftarrow$ ) Si  $P$  est divisible par  $X - \alpha$ , alors on peut écrire  $P = (X - \alpha)Q$ , avec  $Q \in \mathbb{K}[X]$ .

Alors,  $\forall x \in \mathbb{K}$ ,  $\tilde{P}(x) = (\overline{X - \alpha})Q(x) = (x - \alpha)\tilde{Q}(x)$ .

Par conséquent,  $\tilde{P}(\alpha) = (\alpha - \alpha)\tilde{Q}(\alpha) = 0$  donc  $\alpha$  est une racine de  $P$ .

( $\Rightarrow$ ) Effectuons la division euclidienne de  $P$  par  $X - \alpha$  :  $P = (X - \alpha)Q + R$  avec  $Q, R \in \mathbb{K}[X]$  et  $\deg R < \deg(X - \alpha) = 1$ . On en déduit que  $\deg R \leq 0$ , i.e.  $R$  est un polynôme constant. Posons  $R = r_0$ .

On a donc  $P = (X - \alpha)Q + r_0$  et donc  $\forall x \in \mathbb{K}$ ,  $\tilde{P}(x) = (x - \alpha)\tilde{Q}(x) + r_0$ .

En évaluant en  $x = \alpha$ , on obtient  $\tilde{P}(\alpha) = r_0$ .

D'où  $P = (X - \alpha)Q + \tilde{P}(\alpha)$ .

Par hypothèse,  $\alpha$  est une racine de  $P$ , donc  $\tilde{P}(\alpha) = 0$  et  $P = (X - \alpha)Q$ , i.e.  $(X - \alpha) | P$ .

Remarque : On a vu, au cours de la démonstration que le reste dans la division euclidienne de  $P$  par  $X - \alpha$  est  $\tilde{P}(\alpha)$ .

COROLLAIRE

| Soit  $P \in \mathbb{K}[X]$ . Si  $P$  admet  $n$  racines distinctes  $\alpha_1, \dots, \alpha_n$ , alors  $P$  est divisible par  $\prod_{k=1}^n (X - \alpha_k)$ .

*Preuve :*

Démonstration

Par récurrence sur  $n$

1. Si  $n = 1$ , c'est le théorème précédent.
2. Supposons que la propriété soit vraie pour  $n$  racines ( $n \geq 1$ ).

Soit  $P$  admettant  $n + 1$  racines  $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$ .

En utilisant le théorème, on peut écrire  $P = (X - \alpha_{n+1})Q$ .

On a donc  $\forall x \in \mathbb{K}$ ,  $\tilde{P}(x) = (x - \alpha_{n+1})\tilde{Q}(x)$ .

Pour  $k \in \llbracket 1, n \rrbracket$ ,  $(\alpha_k - \alpha_{n+1})\tilde{Q}(\alpha_k) = \tilde{P}(\alpha_k) = 0$ .

Or les racines sont supposées distinctes, d'où  $\alpha_k - \alpha_{n+1} \neq 0$  et donc  $\tilde{Q}(\alpha_k) = 0$  : les  $\alpha_1, \dots, \alpha_n$  sont racines de  $Q$ .

Par H.R., on peut écrire  $Q = \left( \prod_{k=1}^n (X - \alpha_k) \right) Q_1$ , et donc :

$$P = (X - \alpha_{n+1})Q = (X - \alpha_{n+1}) \left( \prod_{k=1}^n (X - \alpha_k) \right) Q_1 = \left( \prod_{k=1}^{n+1} (X - \alpha_k) \right) Q_1.$$

THÉORÈME

| Soit  $P \in \mathbb{K}[X]$  non nul, de degré  $n \geq 0$ .

| Alors,  $P$  possède au maximum  $n$  racines.

**Formulation équivalente :**

Si un polynôme de degré inférieur ou égal à  $n$  possède au moins  $n + 1$  racines, alors il est nul.

*Preuve :*

Démonstration

Supposons que  $P$  possède au moins  $n + 1$  racines distinctes  $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$ .

Alors, on peut écrire  $P = \left( \prod_{k=1}^{n+1} (X - \alpha_k) \right) Q_1$  avec  $Q_1 \in \mathbb{K}[X]$ .

D'où  $\deg P = n + 1 + \deg Q_1$  et  $\deg Q_1 = -1$ . Absurde!

COROLLAIRE

| Tout polynôme non nul possède un nombre fini de racines.

*Exemple :* la fonction  $\cos$  n'est pas polynomiale.

## 4 Multiplicité d'une racine

DÉFINITION

Soit  $P \in \mathbb{K}[X]$  et  $\alpha \in \mathbb{K}$ . Soit  $\alpha$  une racine de  $P$ .

On appelle **multiplicité de la racine  $\alpha$  dans  $P$**  le plus grand entier  $n$  tel que  $(X - \alpha)^n | P$ .

Remarques :

Si la multiplicité de  $\alpha$  est 1,2,3, on parle de racine simple, double, triple.

On convient que si  $\alpha$  n'est pas une racine de  $P$ , alors sa multiplicité est 0 .

Si pour un certain entier  $k \geq 1$ ,  $(X - \alpha)^k | P$ , alors  $\alpha$  est racine de  $P$  de multiplicité au moins  $k$ .

On pourra donc parler de racines au moins simples, au moins doubles ...

Exemple : Soit  $P = aX^2 + bX + c$  avec  $a \neq 0$ . Si  $\Delta = b^2 - 4ac = 0$ , alors  $-\frac{b}{2a}$  est une racine double de  $P$ .

PROPOSITION

Soit  $P \in \mathbf{K}[X]$  et  $\alpha \in \mathbf{K}$ .

Les trois propositions suivantes sont équivalentes :

- \*  $\alpha$  est une racine de  $P$  de multiplicité  $m$ .
- \*  $\exists Q \in \mathbf{K}[X]$ ,  $P = (X - \alpha)^m Q$  avec  $Q(\alpha) \neq 0$ .
- \*  $P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$  et  $P^{(m)}(\alpha) \neq 0$ .

Preuve :

Démonstration

(1)  $\Rightarrow$  (2) Si  $\alpha$  est une racine de  $P$  de multiplicité  $m$ , par définition  $(X - \alpha)^m | P$  et  $(X - \alpha)^{m+1} \nmid P$ . On peut donc écrire  $P = (X - \alpha)^m Q$ .

Si l'on avait  $Q(\alpha) = 0$ , on pourrait écrire  $Q = (X - \alpha)Q_1$  et donc  $P = (X - \alpha)^{m+1}Q_1$ . Absurde.

(2)  $\Rightarrow$  (1) Supposons que  $P = (X - \alpha)^m Q$  et  $Q(\alpha) \neq 0$ .

Alors  $(X - \alpha)^m | P$ . La multiplicité de  $\alpha$  est donc  $\geq m$ .

Supposons que  $(X - \alpha)^k | P$  avec  $k > m$ . Alors  $P = (X - \alpha)^k Q_1$ . On en déduit que  $(X - \alpha)^m Q = (X - \alpha)^k Q_1$ .

D'où  $(X - \alpha)^m [Q - (X - \alpha)^{k-m} Q_1] = 0$  et  $Q = (X - \alpha)^{k-m} Q_1$ . Mais comme  $k > m$ , on a  $Q(\alpha) = 0$  : absurde ! Donc la multiplicité de  $\alpha$  dans  $P$  est exactement  $m$ .

(3)  $\Rightarrow$  (2) Supposons que  $P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$  et  $P^{(m)}(\alpha) \neq 0$ .

On applique la formule de Taylor à  $P$  :

$$\begin{aligned} P &= \sum_{n=0}^p \frac{P^{(n)}(\alpha)}{n!} (X - \alpha)^n \\ &= \sum_{n=m}^p \frac{P^{(n)}(\alpha)}{n!} (X - \alpha)^n \\ &= (X - \alpha)^m \underbrace{\sum_{n=m}^p \frac{P^{(n)}(\alpha)}{n!} (X - \alpha)^{n-m}}_Q \\ &= (X - \alpha)^m Q \end{aligned}$$

Or  $Q(\alpha) = \frac{P^{(m)}(\alpha)}{m!} \neq 0$ .

(2)  $\Rightarrow$  (3) Supposons que  $P = (X - \alpha)^m Q$  et  $Q(\alpha) \neq 0$ . Posons  $R = (X - \alpha)^m$ .

$$\text{On a } R^{(i)} = \begin{cases} \frac{m!}{(m-i)!} (X - \alpha)^{m-i} & \text{si } i \leq m \\ 0 & \text{si } i > m \end{cases} \quad \text{d'où } R^{(i)}(\alpha) = \begin{cases} 0 & \text{si } i < m \\ m! & \text{si } i = m \\ 0 & \text{si } i > m \end{cases} .$$

D'après la formule de Leibniz :  $P^{(k)} = (RQ)^{(k)} = \sum_{i=0}^k \binom{k}{i} R^{(i)} Q^{(k-i)}$ .

$$\text{D'où } P^{(k)}(\alpha) = \sum_{i=0}^k \binom{k}{i} R^{(i)}(\alpha) Q^{(k-i)}(\alpha) = \begin{cases} 0 & \text{si } k < m \\ \binom{k}{m} R^{(m)}(\alpha) Q^{(k-m)}(\alpha) & \text{si } k \geq m \end{cases} .$$

$P^{(m)}(\alpha) = 1 \times m! \times Q(\alpha) \neq 0$ .

Exercice :

Déterminer les racines de  $P = (X - 1)(X^2 - 1)(X^3 - 1)(X^4 - 1) \in \mathbf{R}[X]$  et leurs multiplicités.

$$\begin{aligned} P &= (X - 1)(X^2 - 1)(X^3 - 1)(X^4 - 1) \\ &= (X - 1)[(X - 1)(X + 1)][(X - 1)(X^2 + X + 1)][(X - 1)(X + 1)(X^2 + 1)] \\ &= (X - 1)^4 (X + 1)^2 (X^2 + X + 1)(X^2 + 1) \end{aligned}$$

$X^2 + X + 1$  n'a pas de racine réelle ( $\Delta = -3$ ) et  $X^2 + 1$  non plus.

$P$  a donc deux racines réelles : 1 de multiplicité 4 et -1 de multiplicité 2.

PROPOSITION

Soit  $P \in \mathbf{K}[X]$ .

Si  $P$  admet  $n$  racines distinctes  $\alpha_1, \dots, \alpha_n$  de multiplicités respectives  $m_1, m_2, \dots, m_n$ ,

alors  $P$  est divisible par  $\prod_{k=1}^n (X - \alpha_k)^{m_k}$ .

### Démonstration

Par récurrence sur  $n$

1. Si  $n = 1$ , c'est le théorème précédent.

2. Supposons que la propriété soit vraie pour  $n$  racines ( $n \geq 1$ ).

Soit  $P$  admettant  $n + 1$  racines  $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$  de multiplicités respectives  $m_1, m_2, \dots, m_n, m_{n+1}$ .

En utilisant le théorème, on peut écrire  $P = (X - \alpha_{n+1})^{m_{n+1}} Q_1$ .

Soit  $k \in \llbracket 1, n \rrbracket$ . On va montrer que  $a_k$  est encore une racine de multiplicité  $m_k$  dans  $Q_1$ .

Considérons pour cela  $\mu_k$  la multiplicité (éventuellement nulle) de  $a_k$  dans  $Q_1$ .

On a donc  $Q_1 = (X - a_k)^{\mu_k} Q_2$  avec  $Q_2(a_k) \neq 0$ .

$P = (X - \alpha_{n+1})^{m_{n+1}} Q_1 = (X - \alpha_{n+1})^{m_{n+1}} (X - a_k)^{\mu_k} Q_2 = (X - a_k)^{\mu_k} [(X - \alpha_{n+1})^{m_{n+1}} Q_2]$

Or  $a_k \neq \alpha_{n+1}$  (les racines sont supposées distinctes) et  $Q_2(a_k) \neq 0$ , donc  $(X - \alpha_{n+1})^{m_{n+1}} Q_2$  est non nul en  $a_k$ . On en déduit que  $\mu_k$  est la multiplicité de  $a_k$  dans  $P$ , i.e.  $\mu_k = m_k$ . CQFD.

Les  $a_k$  sont de multiplicité  $m_k$  dans  $Q_1$ . Par H.R., on peut écrire  $Q_1 = \left[ \prod_{k=1}^n (X - \alpha_k)^{m_k} \right] Q_3$ .

Par conséquent,  $P = \left[ \prod_{k=1}^{n+1} (X - \alpha_k)^{m_k} \right] Q_3$ . La propriété est héréditaire.

## V Décomposition d'un polynôme

### 1 Polynôme scindé

#### DÉFINITION

Soit  $P \in \mathbf{K}[X]$  un polynôme non nul. On dit que  $P$  est **scindé** lorsqu'il est constant, ou lorsqu'il s'écrit comme un produit de facteurs de degré 1.

Exemples :

- $(X - 2)(X - 3)$  est scindé.
- $(X - 1)^8$  est scindé.
- $X^2 + 1$  n'est pas scindé dans  $\mathbf{R}[X]$ .  
Il est scindé dans  $\mathbf{C}[X]$  puisqu'on peut écrire  $X^2 + 1 = (X - i)(X + i)$ .

### 2 Factorisation dans $\mathbf{C}[X]$

THÉORÈME de d'Alembert-Gauss (admis)

| Dans  $\mathbf{C}[X]$ , tout polynôme est scindé.

#### COROLLAIRE

Dans  $\mathbf{C}[X]$ , tout polynôme **non constant** admet au moins une racine.

Plus précisément :

Dans  $\mathbf{C}[X]$ , tout polynôme non constant  $P$  s'écrit sous la forme :

$$P = \lambda \prod_{k=1}^n (X - \alpha_k)^{m_k}$$

où  $\alpha_1, \alpha_2, \dots, \alpha_n$  sont les racines de  $P$  de multiplicités  $m_1, m_2, \dots, m_n$  et  $\lambda$  est le coefficient

dominant de  $P$ . On a sous cette forme :  $\deg P = \sum_{k=1}^n m_k$ .

### Démonstration

- Si  $\deg P \geq 2$ ,  $P$  est scindé. Il existe un polynôme de degré 1 divisant  $P$ , donc  $P$  n'est pas irréductible.
- Si  $\deg P = 1$ , supposons que  $P = Q_1 Q_2$ . Alors  $\deg Q_1 + \deg Q_2 = 1$ . On a donc  $\deg Q_1 = 0$  et  $\deg Q_2 = 1$  (quitte à renommer). Le polynôme  $Q_1$  est donc constant non nul. On peut poser  $Q_1 = \lambda$ , et on a  $P = \lambda Q_2$ .  $P$  n'admet comme diviseurs que les  $\lambda$  et les  $\mu P$ .  $P$  est donc irréductible.

*Exemple* : Soit  $P = X^n - 1$  avec  $n \geq 1$ .

Dans  $\mathbf{C}$ , les racines de  $P$  sont les complexes  $z$  tels que  $z^n = 1$ .

En écrivant sous forme exponentielle  $z = re^{i\theta}$ , il vient :  $r^n e^{ni\theta} = 1 = 1e^{i0}$  donc : 
$$\begin{cases} r^n = 1 \\ n\theta = 0 \quad [2\pi] \end{cases}$$

Ainsi,  $r = 1$  et  $\theta = 0 \quad [2\pi]$ . Donc  $z = e^{\frac{2ik\pi}{n}}$ , pour  $k \in \llbracket 0, n-1 \rrbracket$ .

$P$  possède donc  $n$  racines distinctes. Donc  $\prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}}) | P$ .

On a donc  $P = \left[ \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}}) \right] Q$  avec  $Q \in \mathbf{C}[X]$ .

Or  $\deg P = n + \deg Q$  d'où  $\deg Q = 0$  et  $Q = \lambda$  avec  $\lambda \in \mathbf{C}^*$ .

$P = \lambda \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}})$ . Par identification des coefficients dominants,  $\lambda = 1$ .

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

### 3 Factorisation dans $\mathbf{R}[X]$

#### a Racines complexes d'un polynôme réel

PROPOSITION

| Soit  $P \in \mathbf{R}[X]$  et  $\alpha \in \mathbf{C}$ . Si  $\alpha$  est une racine de  $P$ , alors  $\bar{\alpha}$  est aussi une racine de  $P$ .

*Preuve* : Soit  $P = \sum_{k=0}^p a_k X^k$  avec  $a_k \in \mathbf{R}$ .  $P(\bar{\alpha}) = \sum_{k=0}^p a_k (\bar{\alpha})^k = \sum_{k=0}^p a_k \overline{\alpha^k} = \sum_{k=0}^p \overline{a_k \alpha^k} = \overline{\sum_{k=0}^p a_k \alpha^k} = \overline{0} = 0$ .

PROPOSITION

| Soit  $P \in \mathbf{R}[X]$  et  $\alpha \in \mathbf{C}$ . Si  $\alpha$  est une racine de  $P$  de multiplicité  $m$ , alors  $\bar{\alpha}$  est une racine de  $P$  de multiplicité  $m$  également.

*Preuve* :

Démonstration

On a  $\forall k \in \mathbb{N}$ ,  $P^{(k)} \in \mathbf{R}[X]$ .

Pour tout  $k \in \llbracket 1, m-1 \rrbracket$ ,  $P^{(k)}(\alpha) = 0$  donc  $P^{(k)}(\bar{\alpha}) = 0$  (proposition précédente).

Supposons qu'on ait  $P^{(m)}(\bar{\alpha}) = 0$ . On aurait alors  $P^{(m)}(\alpha) = 0$  : absurde.

On en déduit que  $P(\bar{\alpha}) = P'(\bar{\alpha}) = \dots = P^{(m-1)}(\bar{\alpha}) = 0$  et  $P^{(m)}(\bar{\alpha}) \neq 0$ .

$\bar{\alpha}$  est donc une racine de  $P$  de multiplicité  $m$ .

#### b Factorisation dans $\mathbf{R}[X]$

Soit  $P \in \mathbf{R}[X]$ . Alors  $P$  se factorise dans  $\mathbf{R}[X]$  sous la forme :

$$P = \lambda \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{\ell=1}^s (a_\ell X^2 + b_\ell X + c_\ell)^{n_\ell}$$

où  $\lambda$  est le coefficient dominant de  $P$ ,  $\alpha_1, \dots, \alpha_r$  sont les racines réelles de  $P$  de multiplicités respectives  $m_1, \dots, m_r$ , et où  $(a_\ell X^2 + b_\ell X + c_\ell)$  sont des trinômes de discriminant  $\Delta_\ell < 0$ .

On a  $P \in \mathbf{C}[X]$ .

On sait factoriser  $P$  dans  $\mathbf{C}[X]$  connaissant son coefficient dominant  $\lambda$  et ses racines notées :

- Racines réelles :  $\alpha_1, \alpha_2, \dots, \alpha_r$  de multiplicités  $m_1, m_2, \dots, m_r$ .
- Racines complexes :  $\beta_1, \bar{\beta}_1, \beta_2, \bar{\beta}_2, \dots, \beta_s, \bar{\beta}_s$ , de multiplicités  $\mu_1, \mu_2, \dots, \mu_s$ .

$$\begin{aligned} P &= \lambda \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{\ell=1}^s (X - \beta_\ell)^{\mu_\ell} (X - \bar{\beta}_\ell)^{\mu_\ell} \\ &= \lambda \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{\ell=1}^s [(X - \beta_\ell)(X - \bar{\beta}_\ell)]^{\mu_\ell} \\ &= \lambda \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{\ell=1}^s [X^2 - (\beta_\ell + \bar{\beta}_\ell)X + \beta_\ell \bar{\beta}_\ell]^{\mu_\ell} \end{aligned}$$

$$P = \lambda \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{\ell=1}^s [X^2 + u_\ell X + v_\ell]^{\mu_\ell}$$

en posant 
$$\begin{cases} u_\ell = -(\beta_\ell + \bar{\beta}_\ell) = -2\operatorname{Re}(\beta_\ell) \in \mathbb{R} \\ v_\ell = \beta_\ell \bar{\beta}_\ell = |\beta_\ell|^2 \in \mathbb{R} \end{cases} .$$

Et on a  $\Delta_\ell = (u_\ell)^2 - 4v_\ell = 4\operatorname{Re}(\beta_\ell)^2 - 4|\beta_\ell|^2 < 0$ .

en effet,  $|\operatorname{Re}(\beta_\ell)| \leq |\beta_\ell|$  avec égalité uniquement si  $\beta_\ell \in \mathbb{R}$ , ce qui n'est pas le cas ici.

La factorisation d'un polynôme dans  $\mathbb{R}[X]$  est donc de la forme :

$$P = \lambda \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{\ell=1}^s [X^2 + u_\ell X + v_\ell]^{\mu_\ell}$$

FACTORISATION DANS  $\mathbb{R}[X]$

où :

- $\lambda$  est le coefficient dominant de  $P$ .
- $\alpha_1, \alpha_2, \dots, \alpha_r$  sont les racines réelles de  $P$  de multiplicités  $m_1, m_2, \dots, m_r$
- $(u_1, v_1), (u_2, v_2), \dots, (u_s, v_s)$ , sont des couples de réels tels que  $\forall \ell, u_\ell^2 - 4v_\ell < 0$ , i.e.  $X^2 + u_\ell X + v_\ell$  n'a pas de racine réelle.

COROLLAIRE

Les seuls polynômes normalisés irréductibles dans  $\mathbb{R}[X]$  sont :

- Les polynômes  $X - \alpha$  avec  $\alpha \in \mathbb{R}$  ;
- Les polynômes  $X^2 + uX + v$  avec  $u, v \in \mathbb{R}$  et  $u^2 - 4v < 0$ .

*Exemple* : Factoriser  $P = X^6 - 1$  dans  $\mathbb{R}[X]$ .

On le factorise dans  $\mathbb{C}[X]$ , puis on regroupe les racines avec leur conjugué.

$$\begin{aligned} P &= \prod_{k=0}^5 \left( X - e^{\frac{2ik\pi}{6}} \right) \\ &= (X - 1) \left( X - e^{\frac{i\pi}{3}} \right) \left( X - e^{\frac{2i\pi}{3}} \right) (X + 1) \left( X - e^{\frac{4i\pi}{3}} \right) \left( X - e^{\frac{5i\pi}{3}} \right) \\ &= (X - 1)(X + 1) \left( X - e^{\frac{i\pi}{3}} \right) \left( X - e^{-\frac{i\pi}{3}} \right) \left( X - e^{\frac{2i\pi}{3}} \right) \left( X - e^{-\frac{2i\pi}{3}} \right) \\ &= (X - 1)(X + 1)(X^2 - X + 1)(X^2 + X + 1) \end{aligned}$$

$$X^6 - 1 = (X - 1)(X + 1)(X^2 - X + 1)(X^2 + X + 1)$$

## VI Somme et produit des racines

Il est très difficile d'exprimer les racines en fonction des coefficients d'un polynôme. C'est même impossible dans le cas général à partir du degré 5.

En revanche on peut facilement exprimer les coefficients en fonction des racines d'un polynôme scindé :

### 1 Cas général

Considérons  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$ .

Posons  $P = a_n (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$  (les  $\alpha_i$  éventuellement identiques en cas de racines multiples).

En développant, on a  $P = a_n [X^n - (\alpha_1 + \alpha_2 + \dots + \alpha_n) X^{n-1} + \dots + (-1)^n \alpha_1 \alpha_2 \dots \alpha_n]$

En identifiant, on a (entre autres) 
$$\begin{cases} a_{n-1} = -a_n (\alpha_1 + \alpha_2 + \dots + \alpha_n) \\ a_0 = a_n (-1)^n \alpha_1 \alpha_2 \dots \alpha_n \end{cases} .$$

On peut donc trouver facilement la somme et le produit des racines :

$$\boxed{\begin{cases} \alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n} \\ \alpha_1 \alpha_2 \dots \alpha_n = (-1)^n \frac{a_0}{a_n} \end{cases}}$$

### 2 Degré 2

Dans le cas du degré 2, on obtient, en identifiant  $P = aX^2 + bX + c$  et  $P = a(X - \alpha_1)(X - \alpha_2)$  :

$$\boxed{\begin{cases} \alpha_1 + \alpha_2 = -\frac{b}{a} \\ \alpha_1 \alpha_2 = \frac{c}{a} \end{cases}}$$