

# Polynômes

Cours de É. Bouchet – ECS1

14 janvier 2021

## Table des matières

<b>1 Généralités sur les polynômes</b>	<b>2</b>
1.1 Définitions . . . . .	2
1.2 Fonction polynôme, opérations sur les polynômes . . . . .	2
1.3 Degré d'un polynôme . . . . .	3
<b>2 Polynôme dérivé</b>	<b>5</b>
2.1 Définition . . . . .	5
2.2 Formule de Taylor . . . . .	6
<b>3 Division de polynômes</b>	<b>7</b>
3.1 Théorème de division euclidienne . . . . .	7
3.2 Multiples et diviseurs . . . . .	8
<b>4 Racines d'un polynôme</b>	<b>8</b>
4.1 Définition . . . . .	8
4.2 Racines et divisibilité . . . . .	9
4.3 Ordre de multiplicité d'une racine . . . . .	10
<b>5 Factorisation</b>	<b>11</b>
5.1 Factorisations dans $\mathbb{C}[X]$ . . . . .	11
5.2 Factorisations dans $\mathbb{R}[X]$ . . . . .	12

Dans tout ce chapitre, on notera  $n$  un entier naturel et  $\mathbb{K}$  l'un des ensembles  $\mathbb{R}$  ou  $\mathbb{C}$ .

## 1 Généralités sur les polynômes

### 1.1 Définitions

#### Définition.

Un **polynôme** d'indéterminée  $X$ , à coefficients dans  $\mathbb{K}$  est une expression pouvant s'écrire sous la forme

$$P(X) = \sum_{k=0}^n \alpha_k X^k = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n,$$

(avec la convention  $X^0 = 1$ ), où  $\alpha_k \in \mathbb{K}$  pour tout  $k \in \llbracket 0, n \rrbracket$ .

Les  $\alpha_k$  s'appellent les **coefficients** du polynôme  $P$ . On note  $\mathbb{K}[X]$  l'ensemble des polynômes d'indéterminée  $X$  à coefficients dans  $\mathbb{K}$ .

**Remarque.** En particulier :

- Si tous les coefficients de  $P$  sont nuls,  $P$  est le polynôme nul. On note  $P(X) = 0$ .
- Si pour tout  $k \in \llbracket 1, n \rrbracket$ ,  $\alpha_k = 0$ ,  $P$  est un polynôme constant.
- Deux polynômes sont égaux si tous leurs coefficients sont égaux.

**Exemple 1.** Montrer que la famille  $(1, X + 1, X^2)$  est libre dans  $\mathbb{R}[X]$ .

Soit  $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^3$ . On suppose que  $\alpha_1 + \alpha_2(X + 1) + \alpha_3 X^2 = 0$ . En regroupant les coefficients, on trouve :

$$(\alpha_1 + \alpha_2) + \alpha_2 X + \alpha_3 X^2 = 0.$$

Par identification des coefficients du polynôme  $(0 = 0 + 0X + 0X^2)$ , on obtient  $\alpha_1 + \alpha_2 = 0$ ,  $\alpha_2 = 0$  et  $\alpha_3 = 0$ , c'est-à-dire  $\alpha_1 = \alpha_2 = \alpha_3 = 0$ . La famille  $(1, X + 1, X^2)$  est donc libre dans  $\mathbb{R}[X]$ .

### 1.2 Fonction polynôme, opérations sur les polynômes

#### Définition (Fonction polynôme).

Soit  $P(X) = \sum_{k=0}^n \alpha_k X^k$  un polynôme de  $\mathbb{K}[X]$ . On appelle **fonction polynôme associée** à  $P$  la fonction  $p$ , définie de  $\mathbb{K}$  dans  $\mathbb{K}$  par :  $\forall x \in \mathbb{K}$ ,

$$p(x) = \sum_{k=0}^n \alpha_k x^k.$$

**Remarque.** Par abus de langage, on pourra identifier polynôme et fonction polynôme.

#### Proposition (Opérations sur les polynômes).

L'addition des polynômes, la multiplication d'un polynôme par un scalaire et la multiplication de deux polynômes entre eux se déduisent directement des opérations usuelles sur les fonctions.

**Exemple 2.** On pose  $P(X) = 5X^2 + 3X + 2$ ,  $Q(X) = X^2 + 1$ . Alors :

$$(P + Q)(X) = 6X^2 + 3X + 3 = 3(2X^2 + X + 1)$$

et

$$(PQ)(X) = 5X^4 + 3X^3 + 7X^2 + 3X + 2.$$

**Proposition.**

L'ensemble  $\mathbb{K}[X]$  des polynômes muni de ces opérations est un  $\mathbb{K}$ -espace vectoriel.

### 1.3 Degré d'un polynôme

**Définition** (Degré, coefficient dominant).

Soit  $P(X) = \sum_{k=0}^n \alpha_k X^k$  un polynôme de  $\mathbb{K}[X]$  tel que  $\alpha_n \neq 0$ . L'entier  $n$  est appelé **degré** du polynôme  $P$ , et  $\alpha_n$  est appelé **coefficient dominant** de  $P$ .

On note  $\deg(P) = n$ , et  $\mathbb{K}_n[X]$  désigne l'ensemble des polynômes de degré inférieur ou égal à  $n$ .

**Remarque.** Par convention le degré du polynôme nul est donné par :  $\deg(0) = -\infty$ . Cela signifie notamment que  $\mathbb{K}_n[X]$  contient le polynôme nul, et que  $\mathbb{K}_0[X] = \mathbb{K}$ .

**Remarque.** Le degré est très pratique pour manipuler les polynômes dont il n'est pas simple de déterminer les coefficients.

**Exemple 3.** Montrer que la famille  $(1, (X + 1)^5, (X - 2)^7)$  est libre dans  $\mathbb{R}[X]$ .

Soit  $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^3$ . On suppose que  $\alpha_1 + \alpha_2(X + 1)^5 + \alpha_3(X - 2)^7 = 0$ .

On raisonne par l'absurde : supposons de plus que  $\alpha_3 \neq 0$ . On a alors :

$$\deg(\alpha_1 + \alpha_2(X + 1)^5 + \alpha_3(X - 2)^7) = 7 \neq -\infty = \deg(0).$$

C'est impossible, donc  $\alpha_3 = 0$ . Donc  $\alpha_1 + \alpha_2(X + 1)^5 = 0$ .

On itère ensuite ce raisonnement : si  $\alpha_2 \neq 0$ ,  $\deg(\alpha_1 + \alpha_2(X + 1)^5) = 5 \neq -\infty = \deg(0)$ , ce qui est impossible. Donc  $\alpha_2 = 0$  et on en déduit  $\alpha_1 = 0$ . La famille  $(1, (X + 1)^5, (X - 2)^7)$  est donc libre dans  $\mathbb{R}[X]$ .

Remarque : cette méthode fonctionne pour toute famille de polynôme où les degrés sont tous distincts (on parle alors de famille échelonnée en degrés).

**Proposition** (Degré de la somme et du produit).

Soit  $P$  et  $Q$  deux polynômes de  $\mathbb{K}[X]$ , et  $\alpha \in \mathbb{K}^*$ . On a :

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

$$\deg(PQ) = \deg(P) + \deg(Q),$$

$$\deg(\alpha P) = \deg(P).$$

*Démonstration.* (démonstration à connaître) Si  $P(X) = 0$  ou  $Q(X) = 0$ , les résultats sont immédiats. Sinon, il existe des coefficients  $(\alpha_i) \in \mathbb{K}^{n+1}$  et  $(\beta_i) \in \mathbb{K}^{m+1}$ , avec  $\alpha_n \neq 0$  et  $\beta_m \neq 0$ , tels que  $P(X) = \sum_{k=0}^n \alpha_k X^k$  et  $Q(X) = \sum_{k=0}^m \beta_k X^k$ .

- Cas de la somme : on peut supposer que  $n \geq m$ . Alors  $(P + Q)(X) = \sum_{k=0}^m (\alpha_k + \beta_k) X^k + \sum_{k=m+1}^n \alpha_k X^k$ . Donc  $\deg(P + Q) \leq n = \max(\deg(P), \deg(Q))$ . Ce n'est pas une égalité, car si  $n = m$ , et qu'en plus  $\alpha_n + \beta_n = 0$ , le degré est plus petit.
- Cas du produit :  $PQ(X) = \left( \sum_{k=0}^n \alpha_k X^k \right) \left( \sum_{k=0}^m \beta_k X^k \right)$ . Or  $\alpha_n \beta_m \neq 0$  par produit de réels non nuls, donc  $\alpha_n \beta_m$  est le coefficient dominant de  $PQ$  et  $\deg(PQ) = n + m = \deg(P) + \deg(Q)$ .
- Cas de la multiplication par un scalaire :  $\alpha P(X) = \sum_{k=0}^n \alpha \alpha_k X^k$  a pour coefficient dominant  $\alpha \alpha_n \neq 0$  et  $\deg(\alpha P) = n = \deg(P)$ .

□

**Exemple 4.** Montrer que l'ensemble  $\mathbb{K}_n[X]$  des polynômes de degré au plus  $n$  est un  $\mathbb{K}$ -espace vectoriel. En déterminer une base.

- $\deg(0) = -\infty \leq n$ , donc  $0 \in \mathbb{K}_n[X]$  et l'ensemble n'est pas vide.
- Soit  $(P, Q) \in (\mathbb{K}_n[X])^2$  et  $\lambda \in \mathbb{K}$ . Alors  $\lambda P + Q \in \mathbb{K}[X]$ , et :

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

Or  $\deg(Q) \leq n$  et  $\deg(\lambda P) \leq \deg(P) \leq n$ . Donc  $\deg(\lambda P + Q) \leq n$  et  $\lambda P + Q \in \mathbb{K}_n[X]$ .  $\mathbb{K}_n[X]$  est un sous-espace vectoriel de  $\mathbb{K}[X]$ , c'est donc un  $\mathbb{K}$ -espace vectoriel.

Variante de ce raisonnement en utilisant les coefficients plutôt que le degré :

- $0 = \sum_{k=0}^n 0X^k$ , donc  $0 \in \mathbb{K}_n[X]$  et l'ensemble n'est pas vide.
- Soit  $(P, Q) \in (\mathbb{K}_n[X])^2$  et  $\lambda \in \mathbb{K}$ . Alors il existe  $(\alpha_k) \in \mathbb{K}^{n+1}$  et  $(\beta_k) \in \mathbb{K}^{n+1}$  tels que  $P(X) = \sum_{k=0}^n \alpha_k X^k$  et  $Q(X) = \sum_{k=0}^n \beta_k X^k$ . Donc

$$(\lambda P + Q)(X) = \sum_{k=0}^n (\lambda \alpha_k + \beta_k) X^k.$$

Donc  $\lambda P + Q \in \mathbb{K}_n[X]$ .

On conclut ensuite de la même façon.

Il ne reste plus qu'à déterminer une base :

- Soit  $P(X) \in \mathbb{K}_n[X]$ , alors il existe des scalaires  $a_0, \dots, a_n$  tels que  $P(X) = \sum_{k=0}^n a_k X^k$ . Puisque pour tout  $k \in \llbracket 0, n \rrbracket$ ,  $X^k \in \mathbb{K}_n[X]$ ,  $(1, X, X^2, \dots, X^n)$  forme une famille génératrice de  $\mathbb{K}_n[X]$ .
- Soit  $(\lambda_k)_{k \in \llbracket 0, n \rrbracket} \in \mathbb{K}^{n+1}$ , on suppose que  $\sum_{k=0}^n \lambda_k X^k = 0$ . Il s'agit donc du polynôme nul, dont tous les coefficients sont nuls. Donc  $\lambda_0 = \lambda_1 = \dots = \lambda_n = 0$ . Donc la famille est libre.  $(1, X, X^2, \dots, X^n)$  est donc une base de  $\mathbb{K}_n[X]$ .

**Proposition.**

Soit  $P$  et  $Q$  deux éléments de  $\mathbb{K}[X]$ . Alors

$$(PQ)(X) = 0 \iff P(X) = 0 \text{ ou } Q(X) = 0.$$

*Démonstration.* La réciproque est évidente, il suffit donc de vérifier le sens direct.

On raisonne par contraposée : supposons que  $P(X) \neq 0$  et  $Q(X) \neq 0$ . Par passage au degré, on en déduit que  $\deg(P) \geq 0$  et  $\deg(Q) \geq 0$ . Or  $\deg(PQ) = \deg(P) + \deg(Q)$ . Donc  $\deg(PQ) \geq 0$ . Donc  $(PQ)(X) \neq 0$ , d'où le résultat.  $\square$

**Exemple 5.** Soit  $(\alpha, \beta) \in \mathbb{R}^2$ . On suppose que  $(\alpha X + \beta)(3X^2 + 6) = 0$ . Alors  $\alpha X + \beta = 0$  et donc  $\alpha = \beta = 0$ .

## 2 Polynôme dérivé

### 2.1 Définition

**Définition** (Polynôme dérivé).

Soit  $P(X) = \sum_{k=0}^n \alpha_k X^k \in \mathbb{K}[X]$  tel que  $\deg(P) \geq 1$ . Le polynôme  $P'(X) = \sum_{k=1}^n k\alpha_k X^{k-1}$  est appelé **polynôme dérivé** de  $P$  et a pour degré  $\deg(P) - 1$ .

Si  $P$  est un polynôme constant, alors son polynôme dérivé est le polynôme nul.

**Exemple 6.** Si  $P(X) = 4X^2 + 3X + 1$ ,  $P'(X) = 8X + 3$ .

**Remarque.** Attention, cette définition est cohérente avec la fonction dérivée d'une fonction polynomiale dans  $\mathbb{R}$  mais on n'a pas de notion de dérivation pour une fonction polynomiale à coefficients dans  $\mathbb{C}$ .

**Remarque.** Il n'y a pas de condition d'existence du polynôme dérivé, au contraire d'une fonction dérivée.

**Remarque.** On peut définir par récurrence des polynômes dérivés successifs : pour tout  $j \in \mathbb{N}^*$ ,

— si  $P^{(j)}$  est un polynôme non constant de  $\mathbb{K}[X]$ , alors  $P^{(j+1)}$  est le polynôme dérivé de  $P^{(j)}$ ,

— si  $P^{(j)}$  est un polynôme constant de  $\mathbb{K}[X]$  alors  $P^{(j+1)}$  est le polynôme nul,

avec la convention  $P^{(0)} = P$ .

**Proposition** (Expression des polynômes dérivés successifs).

Soit  $P(X) = \sum_{k=0}^n \alpha_k X^k$  un polynôme de  $\mathbb{K}[X]$  de degré  $n$ . Alors,  $\forall k \in \llbracket 0, n \rrbracket$ ,  $\deg P^{(k)} = n - k$ , et

$$P^{(k)}(X) = \sum_{i=k}^n \frac{i!}{(i-k)!} \alpha_i X^{i-k}.$$

Par ailleurs,  $\forall k \geq n + 1$ ,  $P^{(k)}(X) = 0$ .

*Démonstration.* (démonstration à connaître) On montre la première partie par récurrence : soit  $k \in \llbracket 0, n \rrbracket$ , on pose

$$H(k) = \left\{ \deg P^{(k)} = n - k \text{ et } P^{(k)}(X) = \sum_{i=k}^n \frac{i!}{(i-k)!} \alpha_i X^{i-k} \right\}.$$

Initialisation : pour  $k = 0$ ,  $P^{(0)} = P$ , il est donc bien de degré  $n$  et  $H(0)$  est vraie.

Soit  $k \in \llbracket 0, n-1 \rrbracket$  un entier naturel fixé. Supposons que  $H(k)$  est vraie. Alors,  $\deg P^{(k)} = n - k \geq 1$  et on peut appliquer la formule de dérivation :

$$\begin{aligned} P^{(k+1)}(X) &= (P^{(k)}(X))' = \left( \sum_{i=k}^n \frac{i!}{(i-k)!} \alpha_i X^{i-k} \right)' \\ &= 0 + \sum_{i=k+1}^n \frac{i!}{(i-k)!} (i-k) \alpha_i X^{i-k-1} \\ &= \sum_{i=k+1}^n \frac{i!}{(i-(k+1))!} \alpha_i X^{i-(k+1)}. \end{aligned}$$

Par ailleurs,  $\deg P^{(k+1)} = n - (k+1)$  car  $\frac{n!}{(n-(k+1))!} \neq 0$ . Donc  $H(k+1)$  est vraie.

On a donc montré que  $\forall k \in \llbracket 0, n \rrbracket$ ,  $H(k)$  est vraie.

On en déduit en particulier que  $P^{(n)}(X) = n! \alpha_n$  est un polynôme constant. Donc  $\forall k \geq n+1$ ,  $P^{(k)}(X) = 0$ . □

## 2.2 Formule de Taylor

**Proposition** (Formule de Taylor).

Si  $P$  est un polynôme de degré  $n$ , alors on a :  $\forall a \in \mathbb{K}$ ,  $P(X) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X-a)^k$ .

*Démonstration.* On commence par le cas  $a = 0$ , pour lequel on déduit de la formule de dérivation que :  $\forall k \in \llbracket 0, n \rrbracket$ ,

$$P^{(k)}(0) = \frac{k!}{(0)!} \alpha_k 0^{k-k} = k! \alpha_k. \text{ On a donc bien } P(X) = \sum_{k=0}^n \frac{P^{(k)}(0)}{k!} X^k.$$

Pour le cas général d'un  $a$  quelconque, on applique ce résultat au polynôme  $Q(Y) = P(Y+a)$ , d'inconnue  $Y = X-a$  :

$$Q(Y) = \sum_{k=0}^n \frac{Q^{(k)}(0)}{k!} Y^k.$$

Dériver  $k$  fois la relation  $Q(Y) = P(Y+a)$  donne ensuite  $Q^{(k)}(Y) = P^{(k)}(Y+a)$  et en particulier  $Q^{(k)}(0) = P^{(k)}(a)$ .

On obtient donc :

$$P(X) = Q(Y) = \sum_{k=0}^n \frac{Q^{(k)}(0)}{k!} Y^k = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X-a)^k.$$

□

**Exemple 7.** Soit  $P(X) = X^2 + 3X + 5$ . Alors  $P'(X) = 2X + 3$ ,  $P''(X) = 2$  et pour  $a = 1$ , on obtient :

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

### 3 Division de polynômes

#### 3.1 Théorème de division euclidienne

##### Théorème (Division euclidienne).

Soit  $A$  et  $B$  deux polynômes de  $\mathbb{K}[X]$ , avec  $B$  non nul. Alors il existe un unique couple de polynômes  $(Q, R)$  de  $\mathbb{K}[X]$  qui vérifient :

$$A(X) = B(X).Q(X) + R(X),$$

avec  $\deg(R) < \deg(B)$ . On appelle  $Q$  le **quotient** et  $R$  le **reste** de la division euclidienne de  $A$  par  $B$ .

**Exemple 8.** On peut écrire la division euclidienne de  $X^2 + X + 1$  par  $X$  :

$$X^2 + X + 1 = X(X + 1) + 1,$$

le quotient est donc  $X + 1$  et le reste  $1$  est de degré  $0 < 1$ .

*Démonstration.* On fait la preuve en deux temps :

- Preuve de l'existence. On pose  $B(X) = \sum_{k=0}^p b_k X^k$ , et  $A_n(X) = \sum_{k=0}^n a_k X^k$ . (On introduit l'indice  $n$  pour marquer la connaissance du degré, et on définit  $A_{-\infty}$  comme le polynôme nul). On va montrer par récurrence forte sur  $n \in \mathbb{N}$  la propriété suivante :

$$P(n) : \ll \exists (Q_n, R_n) \in \mathbb{K}[X]^2 \text{ tels que } A_n = Q_n B + R_n \text{ et } \deg(R_n) < \deg(B) \gg.$$

Initialisation : pour tout  $n < \deg(B)$ , (il existe au moins un tel  $n$  car  $B$  est non nul),  $A_n = 0B + A_n$  et  $Q_n = 0$  et  $R_n = A_n$  satisfont les conditions du théorème. Donc  $P(n)$  est vraie.

Soit  $n \geq \deg(B) - 1$  un entier naturel fixé, on suppose que  $P(k)$  est vraie pour tout  $k \leq n$ . Soit  $A_{n+1}$  un polynôme de degré  $n + 1$ . On considère le polynôme

$$S_n(X) = A_{n+1}(X) - \frac{a_{n+1}}{b_p} B(X) X^{n+1-p}.$$

Ce polynôme est de degré inférieur ou égal à  $n$  par construction (le coefficient  $\frac{a_{n+1}}{b_p}$  a été choisi pour que les termes en  $X^{n+1}$  s'annulent). Il existe donc, par hypothèse de récurrence, des polynômes  $Q$  et  $R$  tels que  $S_n(X) = Q(X)B(X) + R(X)$  et  $\deg(R) < \deg(B)$ . On a alors :

$$\begin{aligned} A_{n+1}(X) &= \frac{a_{n+1}}{b_p} B(X) X^{n+1-p} + Q(X)B(X) + R(X) \\ &= \left( \frac{a_{n+1}}{b_p} X^{n+1-p} + Q(X) \right) B(X) + R(X). \end{aligned}$$

Choisir  $Q_{n+1}(X) = \frac{a_{n+1}}{b_p} X^{n+1-p} + Q(X)$  et  $R_{n+1}(X) = R(X)$  montre alors  $P(n + 1)$ .

Cela termine la preuve de l'existence.

- Preuve de l'unicité. Supposons que  $(Q_1, R_1)$  et  $(Q_2, R_2)$  soient deux couples convenant :  $A = BQ_1 + R_1$  et  $A = BQ_2 + R_2$ , avec  $\deg(R_1) < \deg(B)$  et  $\deg(R_2) < \deg(B)$ . On trouve par soustraction :

$$B(Q_1 - Q_2) = R_2 - R_1.$$

Par propriétés du degré, on obtient alors :

$$\deg(B) + \deg(Q_1 - Q_2) = \deg(B(Q_1 - Q_2)) = \deg(R_2 - R_1) \leq \max(\deg(R_1), \deg(R_2)) < \deg(B).$$

Or le degré est à valeurs dans  $\mathbb{N} \cup \{-\infty\}$ . Donc  $\deg(Q_1 - Q_2) = -\infty$  et  $Q_1 = Q_2$ . Donc  $R_1 = R_2$ , ce qui termine la preuve de l'unicité.

□

**Exemple 9.** De manière générale, pour effectuer une division de polynôme, on peut poser le calcul. Si on veut par exemple diviser  $X^4 + 3X^3 + 3X + 2$  par  $X^2 + 1$ , cela donne :

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

Le quotient est donc  $X^2 + 3X - 1$ , et le reste  $3$  vérifie  $\deg(3) = 0 < 2 = \deg(X^2 + 1)$ .

**Proposition** (Degré du quotient).

Dans la division euclidienne de  $A$  par  $B$ , si  $\deg(A) \geq \deg(B)$ , alors

$$\deg(Q) = \deg(A) - \deg(B).$$

*Démonstration.* Par théorème de division euclidienne, on a  $A = BQ + R$ , avec  $\deg(A) \geq \deg(B) > \deg(R)$ . Donc  $BQ = A - R$  et par propriétés du degré  $\deg(B) + \deg(Q) = \deg(BQ) = \deg(A - R) = \deg(A)$ , où la dernière égalité découle de la condition  $\deg(A) > \deg(R)$ . Ce qui termine la preuve. □

## 3.2 Multiples et diviseurs

**Définition** (Multiple, diviseur).

Soit  $A$  et  $B$  deux polynômes de  $\mathbb{K}[X]$ , avec  $B$  non nul. On dit que le polynôme  $B$  est un **diviseur** du polynôme  $A$ , ou le polynôme  $A$  est un **multiple** du polynôme  $B$ , lorsqu'il existe un polynôme  $Q$  de  $\mathbb{K}[X]$  tel que

$$A(X) = B(X).Q(X).$$

**Exemple 10.**  $(X + 1)$  et  $(X - 1)$  sont des diviseurs de  $X^2 - 1$ .

**Remarque.** Autrement dit,  $B$  est un diviseur de  $A$  lorsque le reste de la division de  $A$  par  $B$  est le polynôme nul.

## 4 Racines d'un polynôme

### 4.1 Définition

**Définition** (Racine d'un polynôme).

Soit  $P$  un polynôme de  $\mathbb{K}[X]$  et  $r \in \mathbb{K}$  un scalaire. On dit que  $r$  est une **racine** du polynôme  $P$  si

$$P(r) = 0.$$

**Remarque.** Le polynôme nul a donc une infinité de racines.



## 4.2 Racines et divisibilité

### Théorème (Racines et divisibilité).

Soit  $P$  un polynôme de  $\mathbb{K}[X]$  et  $r \in \mathbb{K}$ . Le scalaire  $r$  est racine du polynôme  $P$  si et seulement si

$$X - r \text{ divise } P.$$

**Exemple 11.** 1 est racine de  $X^2 - 1$ , et donc  $X - 1$  divise  $X^2 - 1$ .

*Démonstration.* (démonstration à connaître) Si  $P(X) = 0$ , c'est immédiat.

Si  $P(X) \neq 0$ , on note  $n$  le degré de  $P$  et on applique la formule de Taylor en  $r$  :

$$\begin{aligned} P(X) &= P(r) + P'(r)(X - r) + \frac{P''(r)}{2!}(X - r)^2 + \dots + \frac{P^{(n)}(r)}{n!}(X - r)^n \\ &= P(r) + (X - r) \left( P'(r) + \frac{P''(r)}{2!}(X - r) + \dots + \frac{P^{(n)}(r)}{n!}(X - r)^{n-1} \right). \end{aligned}$$

- Si  $r$  est racine de  $P$ , alors  $P(r) = 0$  et l'expression précédente donne directement que  $X - r$  divise  $P$ .
- Réciproquement, on suppose que  $X - r$  divise  $P$ . L'expression précédente donne la division euclidienne de  $P$  par  $X - r$  puisque  $\deg(P(r)) \leq 0 < 1 = \deg(X - r)$ . La divisibilité assure donc que le reste (en l'occurrence  $P(r)$ ) est nul. Donc  $r$  est racine de  $P$ .

D'où le résultat. □

### Corollaire.

Soit  $P(X)$  un polynôme de  $\mathbb{K}[X]$  et  $r_1, r_2, \dots, r_m$  des éléments deux à deux distincts de  $\mathbb{K}$ . Le polynôme  $(X - r_1)(X - r_2) \dots (X - r_m)$  divise  $P$  si et seulement si  $r_1, r_2, \dots, r_m$  sont des racines de  $P$ .

*Démonstration.* L'implication directe est évidente, il suffit donc de montrer la réciproque. On suppose que  $r_1, r_2, \dots, r_m$  sont des racines de  $P$ , et on pose  $\forall k \in \llbracket 1, m \rrbracket$ ,

$$H(k) = \langle (X - r_1)(X - r_2) \dots (X - r_k) \text{ divise } P \rangle$$

L'initialisation de la récurrence est directe par la propriété précédente :  $H(1)$  est vraie.

Soit  $k \in \llbracket 1, m - 1 \rrbracket$  un entier naturel fixé, on suppose que  $H(k)$  est vraie : il existe  $A \in \mathbb{K}[X]$  tel que

$$P(X) = (X - r_1)(X - r_2) \dots (X - r_k)A(X).$$

Comme  $k + 1 \leq m$ , alors  $r_{k+1}$  est racine de  $P$  et  $P(r_{k+1}) = 0$ . Mais comme les  $r_i$  sont supposés distincts deux à deux  $(r_{k+1} - r_1)(r_{k+1} - r_2) \dots (r_{k+1} - r_k) \neq 0$ . Donc nécessairement  $A(r_{k+1}) = 0$  et  $r_{k+1}$  est racine de  $A$ . Par la proposition précédente, il existe alors  $C \in \mathbb{K}[X]$  tel que  $A(X) = (X - r_{k+1})C(X)$ . Donc

$$P(X) = (X - r_1)(X - r_2) \dots (X - r_k)(X - r_{k+1})C(X).$$

Ce qui montre  $H(k + 1)$ .

Donc  $\forall k \in \llbracket 1, m \rrbracket$ ,  $H(k)$  est vraie. En particulier  $H(m)$  est vraie, ce qui termine la preuve. □

### Proposition.

Un polynôme de degré inférieur ou égal à  $n$  et qui possède au moins  $n + 1$  racines distinctes est le polynôme nul.

**Remarque.** Par contraposée, tout polynôme non nul de degré  $n$  admet au plus  $n$  racines.

**Remarque.** En particulier, tout polynôme qui admet une infinité de racines est le polynôme nul.

*Démonstration.* Soit  $P$  un polynôme de degré inférieur ou égal à  $n$ . Si  $P$  admet  $r_1, r_2, \dots, r_{n+1}$  comme racines distinctes, le corollaire précédent donne l'existence d'un polynôme  $Q$  tel que :

$$P(X) = (X - r_1)(X - r_2) \dots (X - r_{n+1})Q(X).$$

Par propriétés du degré, cela donne  $\deg(P) = n + 1 + \deg(Q)$ . Comme par hypothèse,  $\deg(P) \leq n$ , cela implique que  $Q = 0$ , et donc  $P = 0$ . □

### 4.3 Ordre de multiplicité d'une racine

**Définition** (Ordre de multiplicité).

Soit  $P$  un polynôme de  $\mathbb{K}[X]$ ,  $p$  un entier naturel non nul et  $r \in \mathbb{K}$  un scalaire. On dit que  $r$  est une racine d'ordre de multiplicité  $p$  du polynôme  $P$  lorsque

$$(X - r)^p \text{ divise } P \quad \text{et} \quad (X - r)^{p+1} \text{ ne divise pas } P.$$

**Remarque.** Autrement dit,  $r$  est une racine d'ordre de multiplicité  $p$  du polynôme  $P$  lorsqu'il existe un polynôme  $Q$  de  $\mathbb{K}[X]$  tel que

$$P(X) = (X - r)^p Q(X) \text{ et } Q(r) \neq 0.$$

**Remarque.** Attention! Pour montrer que  $r$  est une racine d'ordre  $p$  de  $P$ , il faut penser à vérifier la deuxième condition : que  $(X - r)^{p+1}$  ne divise pas  $P$ .

**Théorème** (Lien avec les dérivées successives).

Soit  $P$  un polynôme de  $\mathbb{K}[X]$ ,  $r \in \mathbb{K}$  et  $p$  un entier naturel non nul. Le scalaire  $r$  est une racine d'ordre  $p$  du polynôme  $P$  si et seulement si

$$\forall k \in \llbracket 0, p-1 \rrbracket, P^{(k)}(r) = 0 \text{ et } P^{(p)}(r) \neq 0.$$

*Démonstration.* Soit  $P$  un polynôme de degré  $n$ . On applique la formule de Taylor en  $r$  :

$$P(X) = P(r) + P'(r)(X - r) + \frac{P''(r)}{2!}(X - r)^2 + \dots + \frac{P^{(n)}(r)}{n!}(X - r)^n.$$

— On suppose que  $\forall k \in \llbracket 0, p-1 \rrbracket, P^{(k)}(r) = 0$  et  $P^{(p)}(r) \neq 0$ . Alors

$$P(X) = (X - r)^p \underbrace{\left( \frac{P^{(p)}(r)}{p!} + \frac{P^{(p+1)}(r)}{(p+1)!}(X - r) + \dots + \frac{P^{(n)}(r)}{n!}(X - r)^{n-p} \right)}_{Q(X)},$$

donc  $(X - r)^p$  divise  $P(X)$ . De plus,  $\frac{P^{(p)}(r)}{p!} \neq 0$ . Comme il s'agit du reste dans la division euclidienne de  $Q(X)$  par  $(X - r)$  (par unicité de la division euclidienne et car  $\deg(\frac{P^{(p)}(r)}{p!}) = 0 < 1 = \deg(X - r)$ ), cela signifie que  $X - r$  ne divise pas  $Q(X)$ . Donc  $(X - r)^{p+1}$  ne divise pas  $P(X)$ . Donc  $r$  est une racine d'ordre  $p$  de  $P(X)$ .

— On suppose maintenant que  $r$  est une racine d'ordre  $p$  de  $P(X)$ . Alors  $(X-r)^p$  divise  $P(X)$ . Donc le reste  $R(X)$  de la division euclidienne de  $P(X)$  par  $(X-r)^p$  est nul. Il faut donc déterminer ce reste. Par la formule de Taylor et l'unicité de la division euclidienne  $R(X) = P(r) + P'(r)(X-r) + \frac{P''(r)}{2!}(X-r)^2 + \dots + \frac{P^{(p-1)}(r)}{(p-1)!}(X-r)^{p-1}$  (qui est bien de degré strictement inférieur à  $p = \deg((X-r)^p)$ ). Donc

$$P(r) + P'(r)(X-r) + \frac{P''(r)}{2!}(X-r)^2 + \dots + \frac{P^{(p-1)}(r)}{(p-1)!}(X-r)^{p-1} = 0.$$

La famille  $(1, (X-r), (X-r)^2, \dots, (X-r)^{p-1})$  étant échelonnée en degré et donc libre dans  $\mathbb{K}[X]$ , les coefficients de cette relation sont tous nuls et  $\forall k \in \llbracket 0, p-1 \rrbracket, P^{(k)}(r) = 0$ .

Il ne reste plus qu'à montrer que  $P^{(p)}(r) \neq 0$ . On le montre par l'absurde : supposons  $P^{(p)}(r) = 0$ . Les calculs précédents nous donnent qu'alors  $(X-r)^{p+1}$  divise  $P$ , et donc  $r$  est une racine d'ordre au moins  $p+1$  : absurde. Donc  $P^{(p)}(r) \neq 0$ .

D'où le résultat. □

**Exemple 12.** On considère  $P(X) = X^4 - 2X^3 + 3X^2 - 4X + 2$ . Est-ce que 1 est racine, et si oui avec quelle multiplicité ?  $P(1) = 1 - 2 + 3 - 4 + 2 = 0$ , donc 1 est racine. On calcule la dérivée :

$$P'(X) = 4X^3 - 6X^2 + 6X - 4.$$

$P'(1) = 4 - 6 + 6 - 4 = 0$ , donc 1 est racine d'ordre au moins 2. On calcule la dérivée seconde :

$$P''(X) = 12X^2 - 12X + 6.$$

$P''(1) = 12 - 12 + 6 = 6 \neq 0$ . Donc 1 est racine d'ordre 2 de  $P$ . Si on avait continué le calcul,

$$P^{(3)}(X) = 24X - 12, \quad P^{(4)}(X) = 24 \text{ et } P^{(5)}(X) = 0.$$

Donc  $P^{(5)}(1) = 0$ , mais ce n'est pas pour autant que 1 est d'ordre de multiplicité 5.

### Corollaire.

Si  $r$  est une racine d'ordre  $p \geq 1$  du polynôme  $P$ , alors

- $r$  est une racine d'ordre  $p-1$  de  $P'$ ,
- pour tout  $j \in \llbracket 0, p-1 \rrbracket, r$  est une racine d'ordre  $p-j$  de  $P^{(j)}$ .

### Proposition.

Un polynôme  $P \in \mathbb{K}[X]$  non nul et de degré  $n$  admet au plus  $n$  racines, comptées avec leurs ordres de multiplicité.

## 5 Factorisation

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

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

Tout polynôme de  $\mathbb{C}[X]$  non constant (donc de degré supérieur ou égal à un) admet au moins une racine dans  $\mathbb{C}$ .

**Proposition.**

Tout polynôme  $P \in \mathbb{C}[X]$  de degré  $n$  et de coefficient dominant  $\alpha_n$  peut être écrit sous la forme

$$P(X) = \alpha_n \prod_{k=1}^m (X - r_k)^{p_k}$$

avec  $r_k \in \mathbb{C}$  des racines distinctes de  $P$ ,  $p_k \in \mathbb{N}$  leurs ordres de multiplicité, et  $\sum_{k=1}^m p_k = n$ .

*Démonstration.* Soit  $n \in \mathbb{N}$ , on pose

$$H(n) = \ll \text{Si } \deg(P) = n, \quad P(X) = \alpha_n \prod_{k=1}^m (X - r_k)^{p_k} \text{ avec } \sum_{k=1}^m p_k = n \gg.$$

Initialisation : soit  $P(X)$  un polynôme de degré 0. Alors  $P(X) = a \in \mathbb{C}$  et  $H(0)$  est vraie.

Soit  $n \in \mathbb{N}$  fixé, on suppose que  $H(n)$  est vrai. Soit  $P$  un polynôme de  $\mathbb{C}[X]$  de degré  $n + 1$ . Par le théorème de d'Alembert,  $P$  admet une racine  $r$ , et est donc divisible par  $(X - r)$  : on peut écrire  $P(X) = (X - r)Q(X)$ , avec  $\deg(Q) = n$ . Il suffit d'appliquer  $H(n)$  à  $Q$  et d'observer que  $P$  et  $Q$  ont le même coefficient dominant pour conclure que  $H(n + 1)$  est vrai.

Cela termine la preuve. □

**Exemple 13.** Factoriser dans  $\mathbb{C}$  le polynôme  $P(X) = X^3 + X$ .

On a par factorisation directe :

$$P(X) = X(X^2 + 1) = X(X - i)(X + i).$$

## 5.2 Factorisations dans $\mathbb{R}[X]$

**Proposition (Racines conjuguées).**

Soit  $z$  un nombre complexe, et  $P$  un polynôme de  $\mathbb{R}[X]$ . Si  $z$  est racine du polynôme  $P$ , alors  $\bar{z}$  est également racine de  $P$ , avec le même ordre de multiplicité.

*Démonstration.* Soit  $P(X) = \sum_{k=0}^n \alpha_k X^k$  avec  $\forall k \in \llbracket 0, n \rrbracket$ ,  $\alpha_k \in \mathbb{R}$ . Par hypothèse  $z$  est racine de  $P$ , donc

$$0 = \sum_{k=0}^n \alpha_k z^k.$$

Par passage au conjugué, comme  $\alpha_k = \overline{\alpha_k}$  on obtient :

$$0 = \sum_{k=0}^n \overline{\alpha_k} \cdot \bar{z}^k = \sum_{k=0}^n \alpha_k \bar{z}^k = P(\bar{z}).$$

Donc  $\bar{z}$  est également racine de  $P$ . Pour conclure en ce qui concerne l'ordre de multiplicité, il suffit de refaire la même opération sur les dérivées de  $P$ , qui sont également des polynômes à coefficients réels. □

**Proposition.**

Tout polynôme de  $\mathbb{R}[X]$  peut s'écrire comme produit d'un réel, de polynômes à coefficients réels de degré 1 et de polynômes à coefficients réels de degré 2 n'ayant pas de racine réelle.

*Démonstration.* On utilise la décomposition de  $P$  dans  $\mathbb{C}[X]$  :

$$P(X) = \alpha_n \prod_{k=1}^n (X - r_k),$$

où les  $r_k$  sont des racines réelles ou complexes de  $P$ . Comme  $P \in \mathbb{R}[X]$ , on a  $\alpha_n \in \mathbb{R}$ . Si les  $r_k$  sont tous réels, la décomposition est encore valable dans  $\mathbb{R}[X]$ . Il reste donc à traiter le cas où l'on rencontre  $r_{k_0} \in \mathbb{C} \setminus \mathbb{R}$ . Dans ce cas, par la proposition précédente,  $\overline{r_{k_0}}$  est également racine de  $P$ , avec le même ordre de multiplicité  $j$ . On simplifie alors tous les termes contenant ces deux racines :

$$\begin{aligned} (X - r_{k_0})^j (X - \overline{r_{k_0}})^j &= ((X - r_{k_0})(X - \overline{r_{k_0}}))^j \\ &= (X^2 - X(r_{k_0} + \overline{r_{k_0}}) + r_{k_0} \overline{r_{k_0}})^j \\ &= (X^2 - 2 \operatorname{Re}(r_{k_0})X + |r_{k_0}|^2)^j \end{aligned}$$

qui est bien dans  $\mathbb{R}[X]$  et sans racine réelle. On procède de même pour toutes les racines complexes, ce qui permet de conclure.  $\square$

**Exemple 14.** Factoriser dans  $\mathbb{R}$  le polynôme  $P(X) = X^3 + X$ .

On a par factorisation immédiate :

$$P(X) = X(X^2 + 1).$$

$X^2 + 1$  a pour discriminant  $\Delta = -4 < 0$ ,  $X^2 + 1$  n'a donc pas de racine réelle et la factorisation est terminée.