

Chapitre 22

Polynômes (partie B)

Plan du chapitre

1	Divisibilité et division euclidienne de polynômes	1
1.1	Divisibilité dans $\mathbb{K}[X]$	1
1.2	Division euclidienne	3
1.3	Arithmétique de $\mathbb{K}[X]$	5
1.4	PGCD	6
1.5	Algorithme d'Euclide	8
1.6	Coefficients de Bézout, algorithme d'Euclide étendu	8
1.7	Théorèmes de Bézout et conséquences	9
1.8	PPCM	10
1.9	Extensions à plusieurs polynômes	11
2	Racines d'un polynôme	12
2.1	Racines et divisibilité	12
2.2	Multiplicité d'une racine	14
3	Méthodes pour les exercices.	18

Hypothèse

Dans tout ce chapitre, le corps \mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

1 Divisibilité et division euclidienne de polynômes

1.1 Divisibilité dans $\mathbb{K}[X]$

Définition 22.1

Soit $A, B \in \mathbb{K}[X]$. On dit que B divise A , et on note $B \mid A$, s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = BQ$.
On dit alors que B est un diviseur de A , et que A est un multiple de B .

Exemple 1. \circ $X^n - 1$ est divisible par $X - 1$ (dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$) car $X^n - 1 = \dots\dots\dots$

\circ $X^2 - 4$ est-il divisible par $5X + 10$ (dans $\mathbb{R}[X]$) ?

\circ $X^2 - 4$ est-il divisible par $X^2 + 1$ dans $\mathbb{R}[X]$?

- Soit $P \in \mathbb{K}[X]$. Alors $P \mid 0$ car $0 = 0 \cdot P$ et $1 \mid P$ car $P = 1 \cdot P$.
- Pour tous $\lambda, \mu \in \mathbb{K}^*$ et $P, Q \in \mathbb{K}[X]$, on a $P \mid Q$ si et seulement si $\lambda P \mid \mu Q$.

Théorème 22.2 – Division et degré

Soit $A, B \in \mathbb{K}[X]$ non nuls.

- Si $B \mid A$, alors $\deg B \leq \deg A$.
- Si $B \mid A$ et $\deg B = \deg A$, alors $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$.

Démonstration. • Montrons la première assertion.

- Montrons la seconde assertion.

□

Théorème 22.3

La relation “divise” sur $\mathbb{K}[X]$ est une relation binaire qui a les propriétés suivantes. Étant donné trois polynômes A, B, C :

- Réflexivité : on a $A \mid A$.
- Transitivité : si $A \mid B$ et $B \mid C$, alors $A \mid C$.
- Pour tous polynômes A et B :

$$(A \mid B \text{ et } B \mid A) \iff \dots\dots\dots$$

On dit alors que les polynômes A et B sont associés.

Remarque. La relation de divisibilité entre polynômes n’est ni symétrique, ni antisymétrique. Ce n’est donc pas une relation d’ordre, ni une relation d’équivalence.

Démonstration. La réflexivité et la transitivité sont évidentes. Montrons la dernière assertion.

1.2 Division euclidienne

Théorème 22.4 – division euclidienne dans $\mathbb{K}[X]$

Les polynômes Q et R sont appelés respectivement le quotient et le reste de la division euclidienne de A par B .

Démonstration. On montre séparément existence et unicité :

Existence : soit B un polynôme non nul. Pour tout $n \in \mathbb{N}$, on pose l'assertion :

$$\mathcal{P}_n : \quad \forall A \in \underbrace{\mathbb{K}_n[X]}_{\text{i.e. } \deg A \leq n} \quad \exists Q, R \in \mathbb{K}[X] \quad A = BQ + R \quad \text{et} \quad \deg R < \deg B$$

- Initialisation : montrons \mathcal{P}_0 . Soit $A \in \mathbb{K}_0[X]$: le polynôme A est constant.
 - Si $\deg B > \deg A$, le couple $(Q, R) = (0, A)$ convient.

- Si $\deg B \leq \deg A$, alors comme B est non nul et $\deg A \leq 0$, on a nécessairement $\deg B = \deg A = 0$. Ainsi on peut poser $A = \lambda \in \mathbb{K}^*$ et $B = \mu \in \mathbb{K}^*$. On vérifie alors que le couple $(Q, R) = (\lambda \mu^{-1}, 0)$ convient.
- Hérédité : soit $n \in \mathbb{N}$. On suppose que \mathcal{P}_n est vraie. Montrons que \mathcal{P}_{n+1} est vraie. Soit $A \in \mathbb{K}_{n+1}[X]$.
 - Si $\deg A \leq n$, l'existence du couple (Q, R) découle directement de \mathcal{P}_n .
 - Si $\deg A < \deg B$, le couple $(Q, R) = (0, A)$ convient.
 - Il reste donc à traiter le cas où $\deg A = n + 1$ et $\deg B \leq \deg A$. On pose $p = \deg B \leq n + 1$ et

$$\begin{aligned} A &= a_{n+1}X^{n+1} + a_nX^n + \cdots + a_0 && \text{avec } a_{n+1} \neq 0 \\ B &= b_pX^p + b_{p-1}X^{p-1} + \cdots + b_0 && \text{avec } b_p \neq 0 \end{aligned}$$

(l'écriture normalisée de B a un sens car $B \neq 0$). On pose le polynôme

$$P := A - \frac{a_{n+1}}{b_p}X^{n+1-p}B$$

Par construction, on a

$$\deg P \leq \max(\deg A, \deg(X^{n+1-p}B)) = \max(n+1, n+1) = n+1$$

De plus, le coefficient de degré $n+1$ de P est

$$a_{n+1} - \frac{a_{n+1}}{b_p}b_p = 0$$

On en déduit que $\deg P \leq n$. Comme \mathcal{P}_n est vraie, il existe donc un couple (Q_0, R) de polynômes tel que

$$P = BQ_0 + R \quad \text{et} \quad \deg R < \deg B.$$

On a donc

$$A = B \left(\frac{a_{n+1}}{b_p}X^{n+1-p} + Q_0 \right) + R \quad \text{et} \quad \deg R < \deg B.$$

Ainsi le couple $\left(\frac{a_{n+1}}{b_p}X^{n+1-p} + Q_0, R \right)$ convient. D'où \mathcal{P}_{n+1} est vraie.

- Finalement, pour tout $n \in \mathbb{N}$, \mathcal{P}_n est vraie.

□

La démonstration de l'existence donne de plus une méthode algorithmique pour déterminer le couple (Q, R) de la division euclidienne de A par B . En pratique, le calcul se fait ainsi :

Exemple 2. Déterminer le quotient et le reste de la division euclidienne de A par B , dans chacun des cas suivants :

- $A = X^4 + 4X^3 + X + 1$ et $B = X + 1$.

- $A = X^4 + 2X^3 + 1$ et $B = X^2 - 1$.

- $A = X^3 + X + 1$ et $B = X^4$.

Remarque. Si on demande seulement le reste (sans le quotient) de la division euclidienne de A par B , il est possible de conclure sans effectuer la division euclidienne complète.

Exemple 3. Soit $n \in \mathbb{N}$. Déterminer le reste de la division euclidienne de $X^n - 2$ par $X + 1$.

Théorème 22.5

Soit $A, B \in \mathbb{K}[X]$, avec B non nul.
 B divise A si et seulement si le reste de la division euclidienne de A par B est nul.

Démonstration. Sens direct : supposons que B divise A : il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$, donc $A = BQ + 0$. Par unicité du couple “(quotient, reste)”, le reste de la division euclidienne de A par B est 0.

Sens réciproque : supposons que le reste de la division euclidienne de A par B est nul : il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ + 0$. Alors B divise A dans $\mathbb{K}[X]$. \square

1.3 Arithmétique de $\mathbb{K}[X]$

Théorème 22.6

Soit $A, B, D \in \mathbb{K}[X]$.

$$D \mid A \text{ et } D \mid B \implies \forall U, V \in \mathbb{K}[X] \quad D \mid AU + BV$$

Démonstration. Supposons que $D \mid A$ et $D \mid B$: il existe des polynômes Q_A et Q_B tels que $A = DQ_A$ et $B = DQ_B$. Alors, pour tous polynômes U et V ,

$$AU + BV = DQ_AU + DQ_BV = D(Q_AU + Q_BV),$$

donc D divise $AU + BV$. \square

Théorème 22.7

Pour tous polynômes A, B et C , avec A non nul, on a

$$AB \mid AC \iff B \mid C.$$

□

1.4 PGCD

Définition 22.8 – PGCD

Soit $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. Alors il existe un unique polynôme $D \in \mathbb{K}[X]$ qui vérifie les conditions suivantes :

1. D est un diviseur commun à A et B , i.e. $D \mid A$ et $D \mid B$.
2. D est de degré maximal parmi les diviseurs communs à A et B : pour tout $P \in \mathbb{K}[X]$

$$(P \mid A \text{ et } P \mid B) \implies \deg P \leq \deg D$$

3. D est **unitaire**.

D est appelé **le** PGCD de A et B . On note $D = A \wedge B$.

Par convention, on pose $0 \wedge 0 = 0$, de sorte que $A \wedge B$ a un sens pour tous polynômes A et B .

Remarque. Si un polynôme W ne vérifie que les points 1 et 2, alors W est appelé **un** PGCD de A et de B . On verra qu'en fait W est un PGCD de A et de B si et seulement si $W = \lambda(A \wedge B)$ avec $\lambda \in \mathbb{K}^*$.

Exemple 4. Si $A = X(X + 1)$ et $B = -X^2$, alors $A \wedge B = X$: c'est **le** PGCD. Les polynômes $2X$ et $\frac{1}{2}X$ sont des diviseurs communs à A et B de degré maximal, mais n'étant pas unitaires, aucun d'eux n'est **le** PGCD. Ce sont **des** PGCD.

Démonstration. Justifions que cette définition a un sens. Pour tout $A \in \mathbb{K}[X]$, on note $\text{div}(A)$ l'ensemble des polynômes diviseurs de A , c'à d

$$\text{div}(A) = \{B \in \mathbb{K}[X] \mid B \mid A\}$$

Il est clair que $\text{div}(0) = \mathbb{K}[X]$. Toutefois, si $A \neq 0$, alors par la propriété 22.2, $\text{div}(A)$ contient des polynômes de degré inférieur ou égal à $\deg A$: autrement dit $\text{div}(A) \subset \mathbb{K}_{\deg A}[X]$.

Soit maintenant $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. Alors l'ensemble $X := \text{div}(A) \cap \text{div}(B)$ est exactement

l'ensemble des diviseurs communs à A et B . Comme A ou B est non nul, par le paragraphe précédent, il existe ¹ $n \in \mathbb{N}$ tel que $X \subset \mathbb{K}_n[X]$. On pose alors $m \in \llbracket 0, n \rrbracket$ la valeur maximale des degrés des polynômes de X , c'à d

$$m = \max \{ \deg P \mid P \in X \}$$

On peut vérifier que m a bien un sens ². Soit $C \in X$ tel que $\deg C = m$. On note $c_m \neq 0$ son coefficient de degré m . Ensuite, on pose $D = \frac{1}{c_m} C$. On vérifie alors que D est aussi un diviseur commun à A et B , qu'il est de degré m (donc maximal) et unitaire.

La preuve de l'unicité sera vue ultérieurement. □

Lemme 22.9

Soit $A, B, Q, R \in \mathbb{K}[X]$ tels que $A = BQ + R$. On a

$$\text{div}(A) \cap \text{div}(B) = \text{div}(B) \cap \text{div}(R)$$

Démonstration. Comme $R = A - BQ$, tout diviseur commun à A et B divise aussi R (ainsi que B naturellement). Cela donne l'inclusion du premier ensemble dans le second. L'inclusion réciproque se démontre de la même manière avec la relation $A = BQ + R$. □

Théorème 22.10

Soit $A, B \in \mathbb{K}[X]$ avec $(A, B) \neq (0, 0)$. Soit D un PGCD de A et de B . Alors on a $\text{div}(D) = \text{div}(A) \cap \text{div}(B)$, c'à d que pour tout $P \in \mathbb{K}[X]$, on a

$$(P \mid A \text{ et } P \mid B) \iff P \mid D$$

Autrement dit, les diviseurs communs à A et B sont exactement les diviseurs de D .

Cette propriété (qu'on ne démontrera pas) permet de terminer la "preuve" que la définition 22.8 est bien posée en montrant l'unicité d'un polynôme qui vérifie les assertions 1, 2 et 3. Soit D_1 et D_2 deux polynômes qui les vérifient. Montrons que $D_1 = D_2$. Comme D_2 est un PGCD et que $D_1 \mid A$ et $D_1 \mid B$, on a par la propriété ci-dessus que $D_1 \mid D_2$. De même on montre que $D_2 \mid D_1$.

Ainsi, D_1 et D_2 sont associés : il existe $\lambda \in \mathbb{K}^*$ tel que $D_1 = \lambda D_2$. Comme D_1 et D_2 sont unitaires, en égalisant les coefficients dominants dans la relation $D_1 = \lambda D_2$, on a $1 = \lambda \times 1$. Ainsi $\lambda = 1$ si bien que $D_1 = D_2$. Il y a donc bien unicité du PGCD.

Quelques propriétés classiques sur le PGCD (on suppose $(A, B) \neq (0, 0)$) :

- $A \wedge B \neq 0$
- $A \wedge B = B \wedge A$
- $A \wedge B = B$ ssi $B \mid A$ et B est unitaire.
- Si A est unitaire : $A \wedge 0 = A$
- Pour tout $\lambda \in \mathbb{K}^*$: $A \wedge \lambda = 1$.
- Si $A \neq 0 \neq B$: $\deg(A \wedge B) \leq \min(\deg A, \deg B)$.
- Pour tous $\lambda, \mu \in \mathbb{K}^*$, $(\lambda A) \wedge (\mu B) = A \wedge B$.

1. Plus exactement on peut poser $n = \max(\deg A, \deg B)$, qui est un entier naturel car $\deg A$ ou $\deg B$ l'est.

2. En effet, si on pose $Y = \{ \deg P \mid P \in X \setminus \{0\} \}$ alors Y est une partie non vide (car $1 \in X$ et donc $0 \in Y$) et majorée (par n) de \mathbb{Z} . Ainsi, Y possède un maximum.

1.5 Algorithme d'Euclide

L'algorithme d'Euclide vu dans \mathbb{Z} peut être adapté à $\mathbb{K}[X]$ pour calculer le PGCD de deux polynômes.

Méthode – Algorithme d'Euclide

Soit $A, B \in \mathbb{K}[X]$ tels que A, B soient non nuls (sinon $A \wedge B$ est évident). Quitte à échanger A et B , on suppose que $\deg B \leq \deg A$.

1. On fait la division euclidienne de A par B : on trouve un reste R_1 .
2. On fait la division euclidienne de B par R_1 : on trouve un reste R_2 .
3. On fait la division euclidienne de R_1 par R_2 : on trouve un reste R_3 , etc.
4. On s'arrête dès qu'on trouve un reste nul $R_k = 0$ avec $k \geq 1$.
5. On considère le dernier reste non nul, à savoir $D := R_{k-1}$. **Attention** : D n'est pas forcément le PGCD : il vérifie $\text{div}(D) = \text{div}(A) \cap \text{div}(B)$ mais il peut ne pas être unitaire.
6. Pour obtenir le PGCD, il faut alors diviser D par son coefficient dominant.

Par ailleurs, à chaque étape, on peut rendre B, R_1, R_2, \dots unitaire avant de faire la division euclidienne, ce qui peut simplifier les calculs.

Exemple 5. Calculer le PGCD de $A = X^3 - X^2 + 2X - 2$ et $B = X^2 + 4X - 5$.

1.6 Coefficients de Bézout, algorithme d'Euclide étendu

Théorème 22.11 – Théorème de Bézout-Bachet (ou relation de Bézout)

Soit $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. Il existe un couple $(U, V) \in \mathbb{K}[X]^2$ tel que

$$AU + BV = A \wedge B$$

Le couple (U, V) est appelé un **couple de coefficients de Bézout** de A et B .

Méthode – Algorithme d'Euclide étendu

On peut calculer un couple de coefficients de Bézout par l'algorithme d'Euclide étendu, cf ci-dessous. Attention à ne pas oublier si nécessaire de rendre le polynôme final unitaire pour avoir **le** PGCD.

Exemple 6. Trouver un couple de coefficients de Bézout pour les polynômes $A = X^3 - X^2 + 2X - 2$ et $B = X^2 + 4X - 5$.

On a vu que $A \wedge B = X - 1$.

1.7 Théorèmes de Bézout et conséquences

Définition 22.12

Soit $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. On dit que A et B sont **premiers entre eux** si $A \wedge B = 1$. Cela revient à dire que les seuls diviseurs communs à A et B sont les polynômes constants non nuls.

Théorème 22.13 – Théorème de Bézout

Soit $A, B \in \mathbb{K}[X]$. Alors les polynômes A et B sont premiers entre eux si et seulement s'il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Démonstration. Le sens direct est évident par le théorème de Bézout-Bachet. Pour le sens réciproque, si $AU + BV = 1$, alors $(A, B) \neq (0, 0)$ et on peut poser $D = A \wedge B$. Alors, $D \mid A$ et $D \mid B$ donc $D \mid AU + BV$ càd $D \mid 1$. Comme D est unitaire, on en déduit que $D = 1$. □

Théorème 22.14 – Se ramener à des polynômes premiers entre eux

Soit $A, B \in \mathbb{K}[X]$ tels que $(A, B) \neq (0, 0)$. On pose $D = A \wedge B$. Alors, il existe A_1, B_1 tels que

$$A = DA_1 \quad B = DB_1 \quad A_1 \wedge B_1 = 1$$

En particulier, $\frac{A}{A \wedge B}$ et $\frac{B}{A \wedge B}$ sont premiers entre eux.

Théorème 22.15 – Lemme de Gauss

Soit $A, B, C \in \mathbb{K}[X]$. Si $A \mid BC$ et $A \wedge B = 1$, alors $A \mid C$.

Théorème 22.16

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

$$\begin{cases} A \mid C \\ B \mid C \\ A \wedge B = 1 \end{cases} \implies AB \mid C$$

Théorème 22.17

Soit $A_1, A_2, B \in \mathbb{K}[X]$.

$$\begin{cases} A_1 \wedge B = 1 \\ A_2 \wedge B = 1 \end{cases} \implies (A_1 A_2) \wedge B = 1$$

1.8 PPCM

Soit $A \in \mathbb{K}[X]$. L'ensemble des polynômes multiples de A s'écrit

$$A\mathbb{K}[X] = \{AP \mid P \in \mathbb{K}[X]\}$$

Il est clair que $0\mathbb{K}[X] = \{0\}$. Si par contre $A \neq 0$, alors $A\mathbb{K}[X]$ contient des polynômes de degré aussi grand que l'on souhaite. Soit A, B deux polynômes non nuls. Alors l'ensemble $X := A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est exactement l'ensemble de tous les multiples communs à A et B . On peut montrer que X possède un unique polynôme non nul de degré minimal et unitaire.

Définition 22.18 – PPCM

Soit A, B deux polynômes non nuls. Il existe un unique polynôme $M \in \mathbb{K}[X]$ non nul tel que :

1. M est un multiple commun à A et B , i.e. $A \mid M$ et $B \mid M$.
2. M est de degré minimal parmi les multiples **non nuls** communs à A et B : pour tout $P \in \mathbb{K}[X] \setminus \{0\}$

$$(A \mid P \text{ et } B \mid P) \implies \deg M \leq \deg P$$

3. M est **unitaire**.

M est appelé le **PPCM** de A et B . On note $M = A \vee B$.

Par convention, on pose $0 \vee 0 = 0$ et pour tout polynôme A non nul, on pose $A \vee 0 = \frac{1}{\lambda}A$ avec λ le coefficient dominant de A , de sorte que $\frac{1}{\lambda}A$ soit unitaire.

Théorème 22.19

Soit A, B deux polynômes non nuls et $M = A \vee B$. Alors on a $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$, càd que pour tout $P \in \mathbb{K}[X]$, on a

$$(A \mid P \text{ et } B \mid P) \iff M \mid P$$

Autrement dit, les multiples communs à A et B sont exactement les multiples de $A \vee B$.

Quelques propriétés classiques sur le PPCM (on suppose A, B non nuls) :

- $A \vee B \neq 0$
- $A \vee B = B \vee A$
- $A \vee B = A$ ssi $B \mid A$ et A est unitaire.
- $\deg(A \vee B) \geq \max(\deg A, \deg B)$.

Théorème 22.20

Soit A, B deux polynômes non nuls. Alors AB et $(A \wedge B)(A \vee B)$ sont associés.

Ce théorème permet de calculer le PPCM, à partir du PGCD.

Exemple 7. Calculer le PPCM des polynômes $A = X^3 - X^2 + 2X - 2$ et $B = X^2 + 4X - 5$.

1.9 Extensions à plusieurs polynômes

Définition 22.21

Soit $r \in \mathbb{N}^*$ et A_1, \dots, A_r des polynômes non tous nuls, càd $(A_1, \dots, A_r) \neq (0, \dots, 0)$. Alors il existe un unique polynôme **unitaire** D tel que $\text{div}(A_1) \cap \dots \cap \text{div}(A_r) = \text{div}(D)$.

On appelle D le PGCD de A_1, \dots, A_r et on note

$$D = A_1 \wedge \dots \wedge A_r = \bigwedge_{i=1}^r A_i$$

Autrement dit les diviseurs communs à A_1, \dots, A_r sont exactement les diviseurs de D .

Remarque. L'écriture $A_1 \wedge \dots \wedge A_r$ est non-ambiguë car on peut montrer que \wedge est associative. On peut donc mettre des parenthèses où l'on souhaite. Ainsi, pour calculer $A \wedge B \wedge C$, on peut calculer $B \wedge C$ puis $A \wedge (B \wedge C)$. Idem avec $A_1 \wedge \dots \wedge A_r$.

Théorème 22.22 – Théorèmes de Bézout-Bachet et de Bézout généralisés

Soit $r \in \mathbb{N}^*$ et A_1, \dots, A_r des polynômes non tous nuls.

- Il existe des polynômes U_1, \dots, U_r tel que $A_1U_1 + \dots + A_rU_r = \bigwedge_{i=1}^r A_i$.
- On a l'équivalence suivante :

$$\left(\exists U_1, \dots, U_r \in \mathbb{K}[X] \quad A_1U_1 + \dots + A_rU_r = 1 \right) \iff \bigwedge_{i=1}^r A_i = 1$$

Définition 22.23

Soit $r \in \mathbb{N}^*$ et A_1, \dots, A_r des polynômes non tous nuls.

- On dit que A_1, \dots, A_r sont premiers entre eux dans leur ensemble si $\bigwedge_{i=1}^r A_i = 1$.
- On dit que A_1, \dots, A_r sont premiers entre eux deux à deux si pour tous $i, j \in \llbracket 1, r \rrbracket$ tels que $i \neq j$, alors $A_i \wedge A_j = 1$.

Exemple 8. Soit $A_1 = (X + 1)(X + 2)$, $A_2 = (X + 2)(X + 3)$ et $A_3 = (X + 3)(X + 1)$. Alors A_1, A_2, A_3 sont premiers entre eux dans leur ensemble mais ils ne sont pas premiers entre eux à deux : il n'y a même aucun couple d'entiers (i, j) distincts pour lequel $A_i \wedge A_j = 1$ (à défaut que ce soit vrai pour tous).

2 Racines d'un polynôme

2.1 Racines et divisibilité

Définition 22.24

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

Exemple 9. ◦ Tout polynôme de degré 1 a exactement une racine. Plus précisément, pour tous $a \in \mathbb{K}^*$, $b \in \mathbb{K}$, l'unique racine de $aX + b$ est

- Tous les éléments de \mathbb{K} sont racines du polynôme nul.
- Si $\deg P = 2$, alors le nombre de racines de P dépend de \mathbb{K} .
 - Si $\mathbb{K} = \mathbb{R}$, alors P admet zéro, une ou deux racines réelles.
 - Si $\mathbb{K} = \mathbb{C}$, alors P admet deux racines, ou une racine "double".

Théorème 22.25

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors $P(\alpha) = 0 \iff X - \alpha \mid P$.

Démonstration. On réalise la division euclidienne de P par $X - \alpha$: il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

On a $\deg(X - \alpha) = 1$ donc $\deg R \leq 0$: le polynôme R est donc De plus, $P(\alpha) = Q(\alpha)(\alpha - \alpha) + R(\alpha) = R(\alpha)$. En conséquence :

$$P(\alpha) = 0 \iff R(\alpha) = 0 \iff R = 0 \iff X - \alpha \mid P$$

(La dernière équivalence découle du théorème 22.5). □

Méthode

Si α est une racine d'un polynôme P , on peut **factoriser** P par $(X - \alpha)$: il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)Q$. Pour trouver Q , on peut :

- Rechercher les coefficients restants par identification (le degré de Q étant clair). Il est possible de le faire "de tête" en partant des coefficients de plus haut (et/ou de plus bas degré) et en calculant les coefficients de degré décroissant (et/ou croissant).
- Faire la division euclidienne de P par $X - \alpha$: le reste doit être nul et Q sera le quotient.

Cette méthode s'applique également pour une factorisation de P par tout autre polynôme qui le divise.

Exemple 10. Soit $P = X^3 - 6X^2 + 5$. On constate que 1 est une racine évidente de P , donc il existe un polynôme Q tel que $P = (X - 1)Q$. Pour déterminer Q , on va suivre la première méthode :

Théorème 22.26

Pour tout $P \in \mathbb{K}[X]$, pour tous éléments $\alpha_1, \alpha_2, \dots, \alpha_n$ de \mathbb{K} deux à deux distincts :

$$\alpha_1, \alpha_2, \dots, \alpha_n \text{ sont des racines de } P \text{ si et seulement si } (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) \text{ divise } P.$$

Démonstration. On procède par double implication.

- Sens direct : on procède par récurrence. Pour $n = 1$, le résultat découle de la propriété 22.25. Supposons la propriété vraie pour un $n \in \mathbb{N}^*$ fixé. Montrons-là au rang $n + 1$. Soit $\alpha_1, \dots, \alpha_{n+1}$ des racines distinctes de P . Par hypothèse de récurrence, on a $Q \mid P$ avec :

$$Q := (X - \alpha_1) \cdots (X - \alpha_n)$$

De plus, $Q(\alpha_{n+1}) \neq 0$ donc $X - \alpha_{n+1} \nmid Q$. Par ailleurs $Q \nmid X - \alpha_{n+1}$. Alors, par la propriété 22.16, $Q(X - \alpha_{n+1}) \mid P$. D'où le résultat.

- Sens réciproque : comme $\prod_{k=1}^n (X - \alpha_k)$ divise P , il existe $R \in \mathbb{K}[X]$ tel que $P = R \prod_{k=1}^n (X - \alpha_k)$.
Pour tout $i \in \llbracket 1, n \rrbracket$,

$$P(\alpha_i) = R(\alpha_i) \prod_{k=1}^n (\alpha_i - \alpha_k) = R(\alpha_i) (\alpha_i - \alpha_i) \prod_{\substack{k=1 \\ k \neq i}}^n (\alpha_i - \alpha_k) = 0$$

donc α_i est une racine de P .

□

Cette propriété a les conséquences essentielles suivantes :

Théorème 22.27 – Degré et nombre de racines

Un polynôme non nul ne peut avoir plus de racines que son degré. Par conséquent :

1. Tout polynôme de degré $n \in \mathbb{N}$ admet au plus n racines distinctes.
2. Si $P \in \mathbb{K}_n[X]$ admet (au moins) $n + 1$ racines, alors P est le polynôme nul.
3. Si $P \in \mathbb{K}[X]$ admet une infinité de racines distinctes, alors $P = 0$.

□

2.2 Multiplicité d'une racine

Définition 22.28 – Multiplicité – Division

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On dit que α est une racine de P de multiplicité m si

$$(X - \alpha)^m \mid P \quad \text{et} \quad (X - \alpha)^{m+1} \nmid P$$

Cela revient à dire que m est le plus grand entier k tel que $(X - \alpha)^k$ divise P .

- α est appelée une racine simple si c'est une racine de multiplicité 1.
- α est appelée une racine multiple de P si sa multiplicité est supérieure ou égale à 2. On parle notamment de racine double (ou triple) pour une racine de multiplicité 2 (ou 3).
- Par extension, on dit que α est "racine d'ordre 0" si $P(\alpha) \neq 0$.

Théorème 22.29 – Multiplicité – Factorisation

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}$. α est racine de P de multiplicité m si et seulement si

$$\exists Q \in \mathbb{K}[X] \quad P = (X - \alpha)^m Q \quad \text{et} \quad Q(\alpha) \neq 0$$

Remarque. α est racine de multiplicité *au moins* $r \in \mathbb{N}$ si $(X - \alpha)^r \mid P$.

Dans les deux propriétés précédentes, les conditions “ $(X - \alpha)^{m+1} \mid P$ ” et “ $Q(\alpha) \neq 0$ ” des propriétés ci-dessus permettent d’affirmer que la multiplicité est *exactement* m .

Théorème 22.30 – Multiplicité minorée et dérivation

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $r \in \mathbb{N}^*$.

$$(X - \alpha)^r \mid P \quad \Longleftrightarrow \quad P(\alpha) = P'(\alpha) = \dots = P^{(r-1)}(\alpha) = 0.$$

Démonstration. On procède par double implication.

Corollaire 22.31 – Caractérisations : multiplicité exacte

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :

1. α est racine de P de multiplicité (*exactement*) m .
2. $(X - \alpha)^m \mid P$ et $(X - \alpha)^{m+1} \nmid P$.
3. $\exists Q \in \mathbb{K}[X] \quad P = (X - \alpha)^m Q$ et $Q(\alpha) \neq 0$.
4. $P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

En particulier, la dernière ligne montre que si α est racine de P de multiplicité $m \in \mathbb{N}^*$, alors α est racine de P' de multiplicité $m - 1$ (si $m = 1$, alors α est racine de P' de multiplicité 0, donc n'est pas racine de P').

Exemple 11. α est une racine double de P si et seulement si $P(\alpha) = P'(\alpha) = 0$ et $P''(\alpha) \neq 0$.

Corollaire 22.32 – Caractérisations : multiplicité minorée

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :

1. α est racine de P de multiplicité *au moins* m .
2. $(X - \alpha)^m \mid P$.
3. $\exists Q \in \mathbb{K}[X] \quad P = (X - \alpha)^m Q$.
4. $P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$.

Exemple 12. Soit $P = X^4 - 2X^3 + 2X - 1$. Trouver une racine évidente de P et déterminer sa multiplicité. En déduire une factorisation de P .

Théorème 22.33

Pour tout $P \in \mathbb{K}[X]$, pour tous éléments $\alpha_1, \alpha_2, \dots, \alpha_p$ de \mathbb{K} deux à deux distincts, et pour tous $r_1, r_2, \dots, r_p \in \mathbb{N}$, on a équivalence entre les propriétés suivantes :

1. $\forall k \in \llbracket 1, p \rrbracket, \alpha_k$ est une racine de P de multiplicité au moins r_k .
2. $(X - \alpha_1)^{r_1} (X - \alpha_2)^{r_2} \dots (X - \alpha_p)^{r_p} \mid P$.

Démonstration. La démonstration de cette propriété est similaire à celle de la propriété 22.26 :

- L'implication (2) \Rightarrow (1) découle du corollaire précédent.
- L'implication (1) \Rightarrow (2) se démontre par récurrence sur p .

□

Si on note $\alpha_1, \dots, \alpha_r$ les racines de P de multiplicités respectives $m_1, \dots, m_r \in \mathbb{N}^*$, alors on dit que P possède un total de $m_1 + \dots + m_r$ racines *comptées avec multiplicité*. Autrement dit, une racine double ($m_i = 2$) compte double, une racine triple ($m_i = 3$) compte triple, etc.

Théorème 22.34 – Degré et nombre de racines comptées avec multiplicité

Un polynôme non nul ne peut pas admettre plus de racines *comptées avec multiplicité* que son degré. Par conséquent :

1. Si $\deg P = n \in \mathbb{N}$, alors P admet au plus n racines *comptées avec multiplicité*.
2. Si $P \in \mathbb{K}_n[X]$ et que P admet au moins $n + 1$ racines *comptées avec multiplicité*, alors P est le polynôme nul.

Démonstration. La démonstration de cette propriété est similaire à celle du théorème 22.27, en utilisant cette fois le théorème 22.33. □

3 Méthodes pour les exercices

Méthode

Pour factoriser un polynôme P par un polynôme $X - \alpha$, on peut :

- Chercher un polynôme Q vérifiant $P = (X - \alpha)Q$ par identification (le degré de Q étant clair).
- Calculer le quotient de la division euclidienne de P par $X - \alpha$. Le quotient sera le polynôme Q tel que $P = (X - \alpha)Q$.

Cette méthode s'applique également pour une factorisation de P par tout autre polynôme qui le divise, pas seulement ceux de la forme $X - \alpha$.

Méthode

Pour montrer que α est une racine de multiplicité **exactement** $k \in \mathbb{N}^*$ de P , on peut :

- Montrer que $P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0$ et que $P^{(k)}(\alpha) \neq 0$.
- Montrer que $(X - \alpha)^k$ divise P et que $(X - \alpha)^{k+1}$ ne divise pas P .
- Montrer qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^k Q$ avec $Q(\alpha) \neq 0$.

Méthode

Pour montrer que α est une racine de multiplicité **au moins** $k \in \mathbb{N}^*$ de P , on peut :

- Montrer que $P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0$.
- Montrer que $(X - \alpha)^k$ divise P .
- Montrer qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^k Q$.

Méthode

Pour montrer qu'un polynôme P est nul, on peut :

- Montrer que P admet strictement plus de racines comptées avec multiplicité que son degré.
- Montrer que P admet une infinité de racines.

On peut montrer que deux polynômes P et Q sont égaux en montrant que $P - Q$ est nul par cette méthode.

Méthode

Pour prouver que deux polynômes A et B sont premiers entre eux, on peut :

- Calculer $A \wedge B$ par l'algorithme d'Euclide.
- Trouver $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$ et invoquer le théorème de Bézout.
- Montrer que A et B n'ont pas de racine commune dans \mathbb{C} (vu ultérieurement).
- Constater que les décompositions de A et de B en produit de polynômes irréductibles n'ont aucun polynôme irréductible en commun (vu ultérieurement).