Chapitre 23

Polynômes (partie B)

Plan du chapitre

Hypothèse

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

1 Divisibilité entre polynômes

1.1 Définition et généralités

Définition 23.1

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, ou encore que A est un multiple de B.

Exemple 1.
- $X^n - 1$ est divisible par $X - 1$ (dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$) car $X^n - 1 = \ldots\ldots\ldots\ldots$
- $X^2 - 4$ est-il divisible par $5X + 10$ (dans $\mathbb{R}[X]$) ?
- $X^2 - 4$ est-il divisible par $X^2 + 1$ dans $\mathbb{R}[X]$?

- Soit $P \in \mathbb{K}[X]$. Alors $P \mid 0$ car ..... et $1 \mid P$ car .....

Remarque. Pour tous $\lambda, \mu \in \mathbb{K}^*$ et $P, Q \in \mathbb{K}[X]$, on a $P \mid Q$ si et seulement si $\lambda P \mid \mu Q$.

Définition 23.2

Deux polynômes P et Q de $\mathbb{K}[X]$ sont dits associés s'il existe $\lambda \in \mathbb{K}^*$ tels que $P = \lambda Q$.
Il s'agit d'une relation d'équivalence sur $\mathbb{K}[X]$.

Par exemple, pour la symétrie : si $P = \lambda Q$ avec $\lambda \in \mathbb{K}^*$, alors $Q = \lambda' P$ avec $\lambda' = 1/\lambda \in \mathbb{K}^*$.

Théorème 23.3 – 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 et B sont associés, i.e. : .....

Démonstration.

- Montrons la première assertion.

- Montrons la seconde assertion.

□

Théorème 23.4

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 :

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

Remarque. Tout comme dans $\mathbb{Z}$, 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 : le sens réciproque est évident.

□

Théorème 23.5

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

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

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 $AU + BV$. □

Théorème 23.6

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

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

Démonstration.

Notation. On note $\text{div}(A)$ l'ensemble des polynômes diviseurs de A, càd : □

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

Lemme 23.7

Soit $A, B \in \mathbb{K}[X]$ deux polynômes **associés**. Alors $\text{div}(A) = \text{div}(B)$.

1.2 Division euclidienne

Théorème 23.8 – 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 :

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

- Initialisation : montrons H_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 H_n est vraie. Montrons que H_{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 H_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

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

    (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

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

    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

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

    On a donc

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

    Ainsi le couple $\left(\frac{a_{n+1}}{b_p}X^{n+1-p} + Q_0\ ,\ R\right)$ convient.
    D'où H_{n+1} est vraie.
- Finalement, pour tout $n \in \mathbb{N}$, H_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 23.9

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 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 $\mathbb{K}[X]$.

□

1.3 PGCD

Dans cette partie, on s'attache à montrer l'existence et l'unicité du PGCD de deux polynômes A et B tels que $(A,B) \neq (0,0)$. Dans un premier temps, on montre qu'il existe un "degré maximal" pour qu'un polynôme P puisse diviser à la fois A et B.

On pose

$$Y = \left\{ \deg P \;\middle|\; P \in \operatorname{div}(A) \cap \operatorname{div}(B) \right\}$$

On va montrer que Y est une partie non vide et majorée de $\mathbb{Z}$.

On a ainsi prouvé qu'il existe un degré maximal pour qu'un polynôme divise à la fois A et B.

Définition 23.10 – 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 $P \in \mathbb{K}[X]$

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

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.

Démonstration. On reprend l'ensemble Y défini ci-dessus et $m = \max(Y)$. Soit C un polynôme de $\operatorname{div}(A) \cap \operatorname{div}(B)$ tel que $\deg C = m$. On pose $\lambda = \operatorname{cd}(C)$ son coefficient dominant et $D = \dfrac{1}{\lambda} C$. On vérifie alors que D est aussi un diviseur commun à A et B, qu'il est de degré m (donc maximal) et unitaire. Ainsi, le PGCD de A et de B existe bien. La preuve de l'unicité sera vue ultérieurement. □

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 un polynôme W est un PGCD de A et de B si et seulement si W et $A \wedge B$ sont associés.

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.

Théorème 23.11

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 23.12

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 $\text{div}(D) = \text{div}(A) \cap \text{div}(B)$, càd que pour tout $P \in \mathbb{K}[X]$, on a

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

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

Ce théorème (qu'on ne démontrera pas) permet de prouver l'unicité de la Définition 23.10.

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 $\lambda, \mu \in \mathbb{K}^*$, $(\lambda A) \wedge (\mu B) = A \wedge B$.

1.4 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 $A \neq 0$ et $B \neq 0$ (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 $B, R_1, R_2, \cdots$ 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 $B = X^2 + 4X - 5$.

1.5 Coefficients de Bézout, algorithme d'Euclide étendu

Théorème 23.13 – 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 $A \wedge B = X - 1$.

1.6 Théorèmes de Bézout et conséquences

Définition 23.14

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 23.15 – 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 23.16 – 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

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

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

Théorème 23.17 – 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 23.18

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 23.19

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

$$\begin{cases} A_1 \wedge B = 1 \\ A_2 \wedge B = 1 \end{cases} \implies (A_1A_2) \wedge B = 1$$

1.7 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 $Y := A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est exactement l'ensemble de tous les multiples communs à A et B. On peut montrer que Y possède un unique polynôme non nul de degré minimal et unitaire.

Définition 23.20 – 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 $P \in \mathbb{K}[X] \setminus \{0\}$

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

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 $A \vee 0 = \dfrac{1}{\lambda}A$ avec λ le coefficient dominant de A, de sorte que $\dfrac{1}{\lambda}A$ soit unitaire.

Théorème 23.21

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

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

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 23.22

Soit A et B deux polynômes non nuls. Alors les polynômes 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 $B = X^2 + 4X - 5$.

1.8 Extensions à plusieurs polynômes

Définition 23.23

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

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

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

Remarque. L'écriture $A_1 \wedge \cdots \wedge A_r$ 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 $A_1 \wedge \cdots \wedge A_r$.

Théorème 23.24 – Théorèmes de Bézout-Bachet et de Bézout généralisés

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

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

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

Définition 23.25

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

- On dit que $A_1, \cdots, A_r$ sont premiers entre eux dans leur ensemble si $\bigwedge_{i=1}^{r} A_i = 1$.
- On dit que $A_1, \cdots, A_r$ sont premiers entre eux deux à deux si pour tous $i, j \in [\![1, r]\!]$ 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 23.26

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 23.27

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

$$P = Q(X - \alpha) + R \qquad \text{et} \qquad \deg R < \deg(X - \alpha)$$

Démonstration. 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 23.9). □

□

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 est évident, puis on peut calculer les coefficients de Q de tête.
- 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 :

Lemme 23.28

Soit $\alpha,\beta \in \mathbb{K}$ avec $\alpha \neq \beta$. Alors $(X-\alpha)\wedge(X-\beta)=1$.

Démonstration.

□

Théorème 23.29

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

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

Démonstration. On procède par double implication.

- Sens direct : par le Théorème 23.27, on a $X-\alpha_1 \mid P$, $X-\alpha_2 \mid P$, …, $X-\alpha_n \mid P$. Or, comme $\alpha_1 \neq \alpha_2$, on a $(X-\alpha_1)\wedge(X-\alpha_2)=1$. Par un corollaire du théorème de Bézout, on a donc $(X-\alpha_1)(X-\alpha_2) \mid P$.
  De plus, $\begin{cases}(X-\alpha_1)\wedge(X-\alpha_3)=1\\(X-\alpha_2)\wedge(X-\alpha_3)=1\end{cases}$ donc par un autre corollaire, $((X-\alpha_1)(X-\alpha_2))\wedge(X-\alpha_3)=1$. Comme $(X-\alpha_1)(X-\alpha_2) \mid P$ et $X-\alpha_3 \mid P$, on en déduit que $(X-\alpha_1)(X-\alpha_2)(X-\alpha_3) \mid P$. Par récurrence, on obtient $(X-\alpha_1)\cdots(X-\alpha_n) \mid P$.
- Sens réciproque : comme $(X-\alpha_1)\cdots(X-\alpha_n) \mid P$, il existe $Q \in \mathbb{K}[X]$ tel que $P=(X-\alpha_1)\cdots(X-\alpha_n)Q$. Il est alors clair que $P(\alpha_1)=0$ et $P(\alpha_2)=0$ et … et $P(\alpha_n)=0$. Donc $X-\alpha_1 \mid P$ et $X-\alpha_2 \mid P$ et … et $X-\alpha_n \mid P$.

□

Cette propriété a les conséquences essentielles suivantes :

Théorème 23.30 – Degré et nombre de racines

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

1.
2.
3.

Démonstration.

□

2.2 Multiplicité d'une racine

Hypothèse

Dans cette section, on considère que $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}$.

Définition 23.31 – Multiplicité exacte

On dit que α est une racine de P de multiplicité **(exactement)** m si

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

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

- α est appelée une racine simple si sa multiplicité vaut 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).
- Le cas $m = 0$ est possible dans cette définition et résulte d'une convention. Plus précisément :

$$m = 0 \iff X-\alpha \nmid P \iff P(\alpha) \neq 0$$

Ainsi, on peut que α est "racine de multiplicité 0" de P si α n'est, en réalité, pas une racine de P.

Théorème 23.32 – Caractérisations : multiplicité exacte

Les assertions suivantes sont équivalentes :

1. α est racine de P de multiplicité *(exactement)* m.
2.
3.
4.

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').

Démonstration. On utilise le Théorème 23.34 : pour chacune des assertions 2, 3 et 4, la première partie permet d'assurer que la multiplicité de α vaut au moins m. La seconde partie permet d'assurer que la multiplicité de α n'est pas supérieure ou égale à $m+1$. □

Exemple 11. Montrer que 1 est racine triple de $P(X) = X^5 - 5X^4 + 7X^3 - 3X^2 + 2X - 2$.

Définition 23.33 – Multiplicité minorée

On dit que α est une racine de P de multiplicité **au moins** m si

$$(X-\alpha)^m \mid P$$

Théorème 23.34

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. $P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0$

Démonstration. L'équivalence entre 1 et 2 vient de la définition, celle entre 2 et 3 est évidente. Il reste à démontrer que

$$(X-\alpha)^m \mid P \qquad \Longleftrightarrow \qquad P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0$$

□

Exemple 12. Factoriser le polynôme $P(X) = X^5 - 5X^4 + 7X^3 - 3X^2 + 2X - 2$ sachant que 1 est racine triple.

2.3 Comptage de racines avec multiplicité

Théorème 23.35

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

1. $\forall k \in [\![1, p]\!]$, α_k est une racine de P de multiplicité **au moins** m_k.
2. $(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\dots(X-\alpha_p)^{m_p} \mid P$.

Démonstration. La démonstration est similaire à celle du Théorème 23.29 :

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

□

Si on note $\alpha_1, \cdots, \alpha_r$ les racines de P de multiplicités (exactes) respectives $m_1, \cdots, m_r \in \mathbb{N}^*$, 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 23.36 – 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, pour tout $n \in \mathbb{N}$:

1. Si $\deg P = n$, alors P admet au plus n racines *comptées avec multiplicité*.
2. Si $\deg P \leq n$ et que P admet au moins $n+1$ racines *comptées avec multiplicité*, alors P est le polynôme nul.

Démonstration. La démonstration est similaire à celle du Théorème 23.30, en utilisant cette fois le Théorème 23.35. □

3 Polynômes d'interpolation de Lagrange

Soit $n \in \mathbb{N}^*$. Soit $x_1, \dots, x_n \in \mathbb{K}$ des scalaires tous distincts. Pour cette partie, on pose

$$\forall i \in [\![1, n]\!] \qquad L_i(X) := \prod_{\substack{1 \leq k \leq n \\ k \neq i}} \frac{X - x_k}{x_i - x_k} \in \mathbb{K}_{n-1}[X]$$

Théorème 23.37

Pour tous $i, j \in [\![1, n]\!]$, on a

$$L_i(x_j) = \delta_{ij} := \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Démonstration.

□

Théorème 23.38 – Polynôme de Lagrange

Soit $n \in \mathbb{N}^*$.

- Soit $x_1, \cdots, x_n \in \mathbb{K}$ distincts deux à deux.
- Soit $y_1, \cdots, y_n \in \mathbb{K}$ quelconques.

Alors il existe un unique polynôme $P \in \mathbb{K}_{n-1}\left[X\right]$ (i.e. de degré au plus $n-1$) dont la fonction polynômiale passe par les points $(x_1, y_1), \cdots, (x_n, y_n)$, càd tel que

$$P(x_1) = y_1, \quad P(x_2) = y_2, \quad \ldots \quad P(x_n) = y_n$$

Ce polynôme P est donné par :

$$P(X) = \sum_{i=1}^{n} y_i L_i(X) = \sum_{i=1}^{n} y_i \prod_{\substack{1 \leq k \leq n \\ k \neq i}} \frac{X - x_k}{x_i - x_k}$$

P est appelé le polynôme d'interpolation de Lagrange associé aux points $(x_1, y_1), \cdots, (x_n, y_n)$.

Démonstration.

□

Exemple 13. Le polynôme d'interpolation de Lagrange qui passe par les points $(1,2)$ et $(3,5)$ est dans $\mathbb{K}_1\left[X\right]$, donc de la forme $aX + b$. Il s'agit en fait de la droite affine qui passe par ces deux points.

Exemple 14. Soit $a, b, c \in \mathbb{R}$. Déterminer un polynôme de degré au plus 2 qui passe par les trois points suivants :

$$(x_1, y_1) = (-1, a) \qquad (x_2, y_2) = (0, b) \qquad (x_3, y_3) = (1, c)$$

4 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 déterminer la multiplicité **exacte** d'une racine α, on peut :

- Vérifier que $P(\alpha)=0$, puis continuer avec $P'(\alpha)$, $P''(\alpha)$, etc. jusqu'à trouver un résultat non nul.
- Vérifier que $X-\alpha$ divise P, puis continuer avec $(X-\alpha)^2$, $(X-\alpha)^3$, etc. jusqu'à trouver une puissance de $X-\alpha$ qui ne divise pas P.

Cette méthode peut s'adapter pour montrer qu'une racine α est de multiplicité **au moins** égale à une valeur donnée.

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.

Notamment, 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).