Chapitre 12.B
Polynômes (Partie B)

Plan du chapitre

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

3 Divisibilité et division euclidienne de polynômes

(cf Chapitre 12.A pour le début)

3.3 PGCD

Notation : pour tout $A \in \mathbb{K}[X]$, on note $\mathcal{D}(A)$ l'ensemble des diviseurs de A, càd

$$\mathcal{D}(A) = \{B \in \mathbb{K}[X] \mid \exists Q \in \mathbb{K}[X] \quad A = BQ\}$$

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

Soit maintenant $A,B \in \mathbb{K}[X]$ tels que $(A,B) \neq (0,0)$. Alors l'ensemble $X := \mathcal{D}(A) \cap \mathcal{D}(B)$ est exactement l'ensemble des diviseurs communs à A et B. On peut montrer que $X = \mathcal{D}(D)$, où $D \neq 0$ est un diviseur commun à A et B (de degré maximal).

Définition 15 : PGCD

Soit $A,B \in \mathbb{K}[X]$ tels que $(A,B) \neq (0,0)$. Alors il existe un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que

$$\mathcal{D}(D) = \mathcal{D}(A) \cap \mathcal{D}(B)$$

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

$D = A \wedge B$ est un diviseur commun de degré maximal : si U est un diviseur commun à A et B , alors $\deg U \leq \deg D$.

Remarque : Si $A,B \in \mathbb{K}[X]$ et $(A,B) \neq (0,0)$, alors en posant $D = A \wedge B$, l'égalité $\mathcal{D}(D) = \mathcal{D}(A) \cap \mathcal{D}(B)$ signifie exactement :

$$\forall P \in \mathbb{K}[X] \qquad (P \mid A \quad \text{et} \quad P \mid B) \iff P \mid D$$

Autrement dit, tout diviseur commun à A et B est aussi un diviseur de $A \wedge B$ et inversement.

Remarque importante : Si $D = A \wedge B$, alors tout polynôme $D_\lambda := \lambda D$ avec $\lambda \in \mathbb{K}^*$ vérifie aussi l'équivalence ci-dessus [1]. Ce sont aussi des diviseurs communs à A et B de degré maximal, mais $D_1 = D = A \wedge B$ est le seul d'entre eux à être unitaire. C'est lui qu'on appelle le PGCD.

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

3.4 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 22 : 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 $D := R_{k-1}$. (Si $k = 1$, alors $D = R_0 := B$).

D n'est pas forcément le PGCD : il vérifie $\mathcal{D}(D) = \mathcal{D}(A) \cap \mathcal{D}(B)$ mais il peut ne pas être unitaire.

6. Pour obtenir le PGCD, il faut alors diviser D par son coefficient dominant :

$$D = \sum_{j=0}^{n} a_j X^j \qquad \text{avec } a_n \neq 0 \qquad \text{entraine que} \qquad A \wedge B = \frac{1}{a_n} D$$

Exemple 2 : Calculer le PGCD de $A = X^3 + X^2 - X - 1$ et $B = X^3 - X^2 - 2X$.

1. On dit parfois que ces polynômes sont des PGCD de A et B.

3.5 Coefficients de Bézout, algorithme d'Euclide étendu

Théorème 23 : Théorème de Bézout-Bachet

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 24 : 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 une ligne supplémentaire pour passer du CDDM au PGCD (si nécessaire).

Exemple 3 : Trouver un couple de coefficients de Bézout pour $A = X^3 + X^2 - X - 1$ et $B = X^3 - X^2 - 2X$.

3.6 Polynômes premiers entre eux

Définition 16

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 $A \wedge B = 1$.
Autrement dit, les seuls diviseurs communs à A et B sont les polynômes constants non nuls.

Theorème 25 : Théorème de Bézout

Soit $A,B \in \mathbb{K}[X]$. Alors A,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 $D = 1$.

Propriété 26 : 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.

Propriété 27 : Lemme de Gauss

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

Propriété 28

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

$$\Big(A \mid C \quad \text{et} \quad B \mid C \quad \text{et} \quad A \wedge B = 1\Big) \implies AB \mid C$$

3.7 PPCM

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

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

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 $X = M\mathbb{K}[X]$, où $M \neq 0$ est un multiple commun à A et B (de degré minimal).

Propriété 29

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

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$$

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

$M = A \vee B$ est un multiple commun de degré minimal : si N est un multiple *non nul* commun à A et B, alors $\deg M \leq \deg N$.

Remarque : Par définition, si A,$B \in \mathbb{K}[X]$ sont non nuls et qu'on pose $M = A \vee B$, alors

$$\forall P \in \mathbb{K}[X] \qquad (A \mid P \quad \text{et} \quad B \mid P) \iff M \mid P$$

Autrement dit, tout multiple commun à A et B est aussi un multiple de $A \vee B$ et inversement.

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

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

Propriété 30

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 4 : Calculer le PPCM $A = X^3 + X^2 - X - 1$ et $B = 2X^3 - 2X^2 - 4X$.

2

3.8 Extensions à plusieurs polynômes

Définition 17

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 $\mathcal{D}(A_1) \cap \dots \cap \mathcal{D}(A_r) = \mathcal{D}(D)$.

Autrement dit les diviseurs communs à $A_1,\dots,A_r$ sont exactement les diviseurs de D. On appelle D **le PGCD** de $A_1,\dots,A_r$ et on note

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

Calcul pratique du PGCD : L'écriture $A_1 \wedge \dots \wedge A_r$ est cohérente car $\wedge$ 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 $A_1 \wedge \dots \wedge A_r$.

Theorème 31 : 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 $A_1U_1 + \dots + A_rU_r = \bigwedge_{i=1}^{r} A_i$.
- $$\left(\exists U_1,\dots,U_r \in \mathbb{K}[X] \quad A_1U_1 + \dots + A_rU_r = 1\right) \iff \bigwedge_{i=1}^{r} A_i = 1$$

Définition 18

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 $i,j \in [\![1,r]\!]$ tels que $i \neq j$, alors $A_i \wedge A_j = 1$.

4 Racines d'un polynôme

4.1 Racines et divisibilité

Définition 19

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 5 :

- 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 peut admettre zéro, une ou deux racines réelles.

— Si $\mathbb{K} = \mathbb{C}$, alors P admet deux racines, ou une racine "double".

Propriété 32

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 de polynômes (Q, R) tel que

On a $\deg(X - \alpha) =$ donc $\deg R \leqslant$: le polynôme R est
De plus, $P(\alpha) =$ En conséquence :

(La dernière équivalence découle de la propriété **??**). □

Conséquence immédiate : Si α est une racine d'un polynôme P, on peut **factoriser** P par $(X - \alpha)$.

Exemple 6 : 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 $P = (X - 1)Q$. De plus $\deg P = 1 + \deg Q$, donc Q est de degré 2. Pour déterminer Q, on peut au choix :

- noter $Q = aX^2 + bX + c$, écrire $X^3 - 6X^2 + 5 = (X - 1)(aX^2 + bX + c)$ et déterminer a,b,c en identifiant (on peut le faire de tête si c'est simple).
- ou effectuer la division euclidienne de P par $X - 1$.

Propriété 33

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

$$\alpha_1, \alpha_2, \ldots, \alpha_n \text{ sont des racines de } P \quad \text{ssi} \quad (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n) \text{ divise } P.$$

Démonstration

► **Sens réciproque :** Comme $\prod_{k=1}^{n}(X - \alpha_k)$ divise P, il existe $Q \in \mathbb{K}[X]$ tel que $P = Q\prod_{k=1}^{n}(X - \alpha_k)$.
Pour tout $i \in [\![1, n]\!]$,

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

donc α_i est une racine de P.

► **Sens direct :** On ne fait la preuve que pour $n = 2$, le reste se déduit par récurrence. On suppose donc $P(\alpha_1) = P(\alpha_2) = 0$. On sait qu'alors $X - \alpha_1 \mid P$ et $X - \alpha_2 \mid P$.

De plus, comme $\alpha_1 \neq \alpha_2$, on montre facilement que $(X-\alpha_1) \wedge (X-\alpha_2) = 1$. Alors, par la propriété 28, $(X-\alpha_1)(X-\alpha_2) \mid P$. D'où le résultat.

Cette propriété a les conséquences essentielles suivantes :

Theorème 34

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

2. Si $P \in \mathbb{K}_n[X]$ admet $n+1$ racines, alors P est le polynôme nul.

3. Si $P \in \mathbb{K}[X]$ admet une infinité de racines distinctes, alors $P = 0$.

Démonstration

Soit $P \in \mathbb{K}[X]$ tel que $\deg P = n \in \mathbb{N}$. Supposons par l'absurde que P possède (au moins) $n+1$ racines distinctes $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$, alors d'après la propriété précédente, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_{n+1})Q$. Alors $\deg P = n = n+1+\deg Q$.
Ainsi, $\deg Q = -1 \notin \mathbb{N} \cup \{-\infty\}$. Contradiction.

Les assertions 2 et 3 découlent directement de la première. □

4.2 Multiplicité d'une racine

Définition 20

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

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

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

- Une **racine simple** de P est une racine de multiplicité 1 de P.
- Une **racine multiple** de P est une racine de multiplicité 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 $P(\alpha) \neq 0$.

Remarque : Cela justifie les termes employés pour les racines d'un polynôme de degré 2. Par exemple :

- Avec $P = X^2 - 2X + 1$,
- Avec $P = X^2 - 3X + 2$,

Propriété 35

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

$$(X-\alpha)^m \mid P \text{ et } (X-\alpha)^{m+1} \nmid P \iff \exists Q \in \mathbb{K}[X], P = (X-\alpha)^m Q \text{ et } Q(\alpha) \neq 0.$$

Démonstration

On a les équivalences suivantes :

$$\begin{aligned}(X-\alpha)^m \mid P \text{ et } (X-\alpha)^{m+1} \nmid P &\iff \exists Q \in \mathbb{K}[X] \quad P = (X-\alpha)^m Q \text{ et } (X-\alpha)^{m+1} \nmid (X-\alpha)^m Q \\ &\iff \exists Q \in \mathbb{K}[X] \quad P = (X-\alpha)^m Q \text{ et } X-\alpha \nmid Q.\end{aligned}$$

(En effet, d'après la propriété **??**, pour A non nul, $AB \nmid AC \iff B \nmid C$.) D'après la propriété 32, cela donne

$$(X-\alpha)^m \mid P \text{ et } (X-\alpha)^{m+1} \nmid P \iff \exists Q \in \mathbb{K}[X], P = (X-\alpha)^m Q \text{ et } Q(\alpha) \neq 0.$$ □

Propriété 36

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

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

Démonstration

► **Sens direct :** Supposons que $(X-\alpha)^r$ divise P : il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^r Q$.
Soit $n \in [\![0, r-1]\!]$. Montrons que $P^{(n)}(\alpha) = 0$. D'après la formule de Leibniz,

$$\begin{aligned} P^{(n)}(X) &= \sum_{k=0}^{n} \binom{n}{k} \left((X-\alpha)^r\right)^{(k)} Q^{(n-k)}(X) \\ &= \sum_{k=0}^{n} \binom{n}{k} r(r-1)\ldots(r-k+1)(X-\alpha)^{r-k} Q^{(n-k)}(X) \qquad \text{car } k \leq r \\ P^{(n)}(\alpha) &= \sum_{k=0}^{n} \binom{n}{k} r(r-1)\ldots(r-k+1) \underbrace{(\alpha-\alpha)^{r-k}}_{=0 \text{ car } r-k \geq 1} Q^{(n-k)}(\alpha) = 0 \end{aligned}$$

► **Réciproque :** Supposons que $P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$. D'après la formule de Taylor,

$$\begin{aligned} P(X) &= \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= \sum_{k=r}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= \sum_{k=0}^{n-r} \frac{P^{(k+r)}(\alpha)}{(k+r)!}(X-\alpha)^{k+r} \\ &= (X-\alpha)^r Q \qquad \text{avec } Q = \sum_{k=0}^{n-r} \frac{P^{(k+r)}(\alpha)}{(k+r)!}(X-\alpha)^k. \end{aligned}$$

Ainsi $(X-\alpha)^r$ divise P. □

Corollaire 37

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. $P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0$ 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 n'est pas racine de P').

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

Corollaire 38

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

Exemple 7 : Soit $P = X^4 - 2X^3 + 2X - 1$. Trouver une racine évidente de P et déterminer sa multiplicité. En déduire une factorisation de P.

Ainsi 1 est une racine de P de multiplicité . Donc il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-1)^{\cdots}Q$ et $Q(1) \neq 0$.

Propriété 39

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

1. $\forall k \in [\![1, p]\!]$, α_k est une racine de P de multiplicité au moins r_k.

2. $(X-\alpha_1)^{r_1}(X-\alpha_2)^{r_2}\ldots(X-\alpha_p)^{r_p} \mid P$.

La démonstration de cette propriété est similaire à celle de la propriété 33 :

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

4.3 Factorisation de polynômes

Corollaire 40

Soit P un polynôme non nul. Si P admet r racines distinctes $\alpha_1, \alpha_2, \ldots, \alpha_r$ de multiplicités respectives $m_1, m_2, \ldots, m_r$, alors :

- On a $\sum_{k=1}^{r} m_k \leqslant \deg P$ et
$$\exists Q \in \mathbb{K}[X] \qquad P = Q\prod_{k=1}^{r}(X-\alpha_k)^{m_k}$$
- Si $\sum_{k=1}^{r} m_k = \deg P$, alors
$$\exists \lambda \in \mathbb{K}^* \qquad P = \lambda\prod_{k=1}^{r}(X-\alpha_k)^{m_k} = \lambda(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\ldots(X-\alpha_p)^{m_r}$$

Démonstration

Pour la première assertion, la factorisation de P découle immédiatement de la propriété 39. De plus,

$$\deg P = \deg Q + \sum_{i=1}^{r}\deg\left((X-\alpha_i)^{m_i}\right) = \deg Q + \sum_{i=1}^{r} m_i$$

d'où l'inégalité $\sum_{k=1}^{r} m_k \leqslant \deg P$ (si on avait $\deg Q = -\infty$, on aurait $Q = 0$ donc $P = 0$, absurde).

Pour la seconde assertion, si $\sum_{k=1}^{r} m_k = \deg P$, alors $\deg Q = 0$, donc $Q = \lambda \in \mathbb{K}^*$. On en déduit la seconde assertion. □

Remarque : En particulier, si un polynôme P de degré n admet n racines distinctes $\alpha_1, \alpha_2, \ldots, \alpha_n$, alors il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda\prod_{k=1}^{n}(X-\alpha_k)$.

Exemple 8 : Soit $n \in \mathbb{N}^*$. Donner une forme factorisée du polynôme $X^n - 1$ dans $\mathbb{C}[X]$ **(à connaître)**.

4.4 Polynômes scindés

Définition 21 : Polynôme scindé

Soit $P \in \mathbb{K}[X]$. On dit que P est **scindé sur** $\mathbb{K}$ s'il peut s'écrire comme un produit de polynômes de degré 1 : il existe $n \in \mathbb{N}$, $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$ (pas nécessairement distincts) et $\lambda \in \mathbb{K}^*$ tels que

$$P = \lambda \prod_{k=1}^{n} (X - \alpha_k) = \lambda (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n)$$

Si de plus cette écriture est valable avec $\alpha_1, \alpha_2, \ldots, \alpha_n$ deux à deux distincts, on dit que P est **scindé à racines simples**.

Remarque importante : En regroupant les α_k qui apparaissent plusieurs fois, quitte à les re-numéroter, cela revient à dire qu'il existe $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{K}$ deux à deux distincts, et $m_1, m_2, \ldots, m_r \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{m_r} = \lambda (X - \alpha_1)^{m_1} (X - \alpha_2)^{m_2} \ldots (X - \alpha_r)^{m_r} \qquad (*)$$

Sous forme $(*)$, P est scindé à racines simples si et seulement si toutes les multiplicités $m_1, \ldots, m_r$ valent 1.

Corollaire 41

P est scindé si et seulement si $P \neq 0$ et P admet autant de racines que son degré *comptées avec leurs multiplicités.*

Comptage de racines avec multiplicité : Par exemple, si P est sous la forme $(*)$, alors P admet $m_1 + m_2 + \cdots + m_r$ racines : chaque racine α_k est comptée autant de fois que sa multiplicité. Le corollaire ci-dessus dit ainsi que si $\sum_{k=1}^{r} m_k = \deg P$, alors P est scindé : c'est le résultat du corollaire 40.

Exemple 9 :

- Tout polynôme de degré 1 est scindé (à racines simples) : si $P = aX + b$ avec $a \in \mathbb{K}^*$, $b \in \mathbb{K}$, alors $P = a\,(X - \alpha)$ avec $\alpha =$
- Le polynôme $P = 3X^3 - X^2$
- Pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 1$
- Le polynôme $Q = X^2 + 1$

Remarque : quand on affirme qu'un polynôme est scindé, il est essentiel de préciser « sur $\mathbb{R}$ » ou « sur $\mathbb{C}$. »

Rappel : Pour tous $a, b, c \in \mathbb{C}$ tels que $a \neq 0$, pour tous $z_1, z_2 \in \mathbb{C}$:

$$z_1 \text{ et } z_2 \text{ sont les racines de } aX^2+bX+c \quad \iff \quad z_1+z_2 = \frac{-b}{a} \text{ et } z_1 z_2 = \frac{c}{a}.$$

Pour un polynôme scindé, on peut généraliser ces relations entre coefficients et racines :

Propriété 42 : Relations coefficients-racines (ou formules de Viète)

Soit $P = \sum_{k=0}^{n} b_k X^k$ un polynôme de degré $n \in \mathbb{N}^*$ scindé : $P = \lambda(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n)$, avec $\lambda \in \mathbb{K}^*$, et $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{K}$ (pas nécessairement distincts). Alors :

$$\sum_{k=1}^{n} \alpha_k = -\frac{b_{n-1}}{b_n} \qquad \text{et} \qquad \prod_{k=1}^{n} \alpha_k = (-1)^n \frac{b_0}{b_n} \qquad (b_n = \lambda \neq 0).$$

Ces relations donnent la somme et le produit des racines *comptées autant de fois que leur multiplicité*. Elles se montrent par identification.

Suite de l'exemple 8 : Soit $n \in \mathbb{N}^*$. Retrouver le produit et la somme des racines n-èmes de l'unité.

5 Décomposition en produit de facteurs irréductibles

5.1 Polynômes irréductibles

Définition 22

Soit $P \in \mathbb{K}[X]$. On dit que P est **irréductible sur** $\mathbb{K}$ si

- $\deg P \geqslant 1$ et...
- ... les seuls diviseurs de P dans $\mathbb{K}[X]$ sont :
  - — les polynômes constants (de degré 0),
  - — les polynômes de même degré que P (donc associés à P : de la forme λP, avec $\lambda \in \mathbb{K}^*$).

Propriété 43

1. Tout polynôme de degré 1 est irréductible.

2. Si $\deg P \geq 2$ et que P admet une racine dans $\mathbb{K}$, alors P n'est pas irréductible sur $\mathbb{K}$.

Démonstration

1. Soit $P \in \mathbb{K}[X]$ de degré 1. Soit $A \in \mathbb{K}[X]$ un diviseur de P : il existe $Q \in \mathbb{K}[X]$ tel que $P = AQ$. Alors

2. Si $\alpha \in \mathbb{K}$ est une racine de P, alors $X - \alpha \mid P$. Donc P admet un diviseur de degré 1 (différent de 0 et de $\deg P \geq 2$), donc P n'est pas irréductible. □

Exemple 10 : Les polynômes suivants sont-ils irréductibles ?

$$P = X^3 - X^2 + X - 1 \qquad Q = X^2 + 1.$$

Remarque : Les polynômes irréductibles dans $\mathbb{K}[X]$ jouent un rôle similaire aux nombres premiers dans $\mathbb{N}$. De même que tout nombre entier se décompose de manière unique en produit de facteurs premiers, on va montrer que **tout polynôme de $\mathbb{K}[X]$ peut se décomposer comme un produit de polynômes irréductibles de $\mathbb{K}[X]$**.

5.2 Décomposition des polynômes dans $\mathbb{C}[X]$

Theorème 44 : Théorème de d'Alembert-Gauss (admis)

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.
On dit que $\mathbb{C}$ est **algébriquement clos**.

Ce théorème a la conséquence essentielle suivante :

Theorème 45

Tout polynôme non nul de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Démonstration

On raisonne par récurrence sur le degré. Par convention, tout polynôme de degré zéro est scindé. Pour tout $n \in \mathbb{N}^*$, notons $\mathcal{P}_n$ le prédicat : « tout polynôme de degré n est scindé sur $\mathbb{C}$. »

- **Initialisation :** $n = 1$. D'après l'exemple 9, tout polynôme de degré 1 est scindé sur $\mathbb{C}$.
- **Hérédité :** Soit $n \in \mathbb{N}^*$ tel que $\mathcal{P}_n$ est vraie. Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n+1$.
  D'après le théorème de d'Alembert-Gauss, P admet une racine $\alpha \in \mathbb{C}$. Donc $X - \alpha$ divise P : il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - \alpha)Q$.
  On montre alors facilement que $\deg Q = \deg P - 1 = n$. Par hypothèse de récurrence, Q est scindé sur $\mathbb{C}$: il existe $\lambda \in \mathbb{K}^*$, $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tels que $Q = \lambda \prod_{k=1}^{n} (X - \alpha_k)$.
  Ainsi $P = \lambda \prod_{k=1}^{n+1} (X - \alpha_k)$, avec $\alpha_{n+1} = \alpha$. Donc P est scindé et $\mathcal{P}_{n+1}$ est vraie.

► **Conclusion :** Pour tout $n \in \mathbb{N}^*$, $\mathcal{P}_n$ est vraie. □

Corollaire 46 : Polynômes irréductibles et décomposition sur $\mathbb{C}[X]$

1. Les polynômes irréductibles sur $\mathbb{C}$ sont les polynômes de degré 1 (et ce sont les seuls).

2. Tout polynôme non nul de $\mathbb{C}[X]$ peut se décomposer en produit de polynômes irréductibles (donc de degré 1) sous la forme :

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

avec $\lambda \in \mathbb{C}^*$, $r \in \mathbb{N}$, $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ les racines deux à deux distinctes de P, et $m_1, \dots, m_r \in \mathbb{N}^*$ leurs multiplicités respectives.
Cette décomposition est unique à l'ordre des facteurs près.

Lorsque P est décomposé, on peut "lire" ses racines et leurs multiplicités (si $r = 0$, P est constant non nul).

Démonstration

1. On a vu précédemment que tous les polynômes de degré 1 sont irréductibles. De plus, tout polynôme de degré supérieur ou égal à 2 est scindé sur $\mathbb{C}$, donc admet une racine et par conséquent n'est pas irréductible.

2. La décomposition résulte directement du fait que tout polynôme non constant de $\mathbb{C}[X]$ est scindé. □

Exemple 11 : Factoriser le polynôme $X^4 + 1$ dans $\mathbb{C}[X]$.

5.3 Décomposition des polynômes dans $\mathbb{R}[X]$

Propriété 47

Soit P un polynôme à coefficients réels. Si α est une racine complexe de $\mathbb{C}$, alors $\overline{\alpha}$ est aussi une racine de P, de même multiplicité que α.

Démonstration

Tout d'abord, pour tout $Q \in \mathbb{R}[X]$, pour tout $\alpha \in \mathbb{C}$, $Q(\overline{\alpha}) = \overline{Q(\alpha)}$. En effet, si $Q = \sum_{k=0}^{n} a_k X^k$, alors

$$\overline{Q(\alpha)} = \sum_{k=0}^{n} \overline{(a_k \alpha^k)} = \sum_{k=0}^{n} \overline{a_k}\, \overline{\alpha}^k = \sum_{k=0}^{n} a_k\, \overline{\alpha}^k = Q(\overline{\alpha}),$$

car $a_0, a_1, \dots, a_n \in \mathbb{R}$.
En conséquence, comme P et ses dérivées successives sont à coefficients réels, pour tout $\alpha \in \mathbb{C}$:

$$\begin{aligned}
\alpha \text{ est racine de } P \text{ de multiplicité } m \quad &\iff \quad P(\alpha) = P'(\alpha) = \dots = P^{(m-1)}(\alpha) = 0 \text{ et } P^{(m)}(\alpha) \neq 0 \\
&\iff \quad \overline{P(\alpha)} = \overline{P'(\alpha)} = \dots = \overline{P^{(m-1)}(\alpha)} = 0 \text{ et } \overline{P^{(m)}(\alpha)} \neq 0 \\
&\iff \quad P(\overline{\alpha}) = P'(\overline{\alpha}) = \dots = P^{(m-1)}(\overline{\alpha}) = 0 \text{ et } P^{(m)}(\overline{\alpha}) \neq 0 \\
&\iff \quad \overline{\alpha} \text{ est une racine de } P \text{ de multiplicité } m.
\end{aligned}$$

□

Théorème 48 : Polynômes irréductibles et factorisation sur $\mathbb{R}[X]$

1. Les polynômes irréductibles sur $\mathbb{R}$ sont les polynômes de degré 1, et les polynômes de degré 2 de discriminant strictement négatif (et ce sont les seuls).

2. Tout polynôme non nul de $\mathbb{R}[X]$ se factorise en produit de polynômes irréductibles sous la forme

$$P = \lambda \left(\prod_{k=1}^{r} (X - \alpha_k)^{m_k} \right) \prod_{j=1}^{s} Q_j^{p_j}$$

avec $\lambda \in \mathbb{R}^*$, $r \in \mathbb{N}$, $s \in \mathbb{N}$ et :

- $\alpha_1, \dots, \alpha_r \in \mathbb{R}$ les racines réelles de P, deux à deux distinctes,
- $m_1, \dots, m_r \in \mathbb{N}^*$ leurs multiplicités respectives,
- $Q_1, \dots, Q_s \in \mathbb{R}[X]$ des polynômes unitaires distincts de degré 2 à discriminant strictement négatif.
- $p_1, \dots, p_s \in \mathbb{N}^*$ jouent le rôle de "multiplicités" des $Q_1, \dots, Q_s$.

Cette décomposition est unique à l'ordre des facteurs près.

Dans la factorisation ci-dessus, on peut avoir $r = 0$ ou $s = 0$ (dans ce cas le produit correspondant vaut 1 car on somme sur le vide). Si $r = s = 0$, alors P est constant non nul. De plus, λ est le coefficient dominant de P.

On peut obtenir la décomposition de P sur $\mathbb{C}$ en décomposant chaque Q_j comme $(X - \beta_j)(X - \bar{\beta_j})$, avec $\beta_j \in \mathbb{C} \setminus \mathbb{R}$. L'entier p_j correspond alors à la multiplicité de β_j et de $\bar{\beta_j}$ dans cette décomposition.

Comme sur $\mathbb{C}$, on peut lire les racines réelles de P sur sa factorisation dans $\mathbb{R}[X]$. Les Q_j n'ont pas de racine réelle donc il suffit de regarder le premier produit.

Démonstration

On ne montre que la deuxième assertion. Soit $P \in \mathbb{R}[X]$. On note :

- λ le coefficient dominant de P.
- $\alpha_1, \dots, \alpha_r$ les racines réelles de P (deux à deux distinctes).
- $m_1, \dots, m_r$ les multiplicités respectives de $\alpha_1, \dots, \alpha_r$.
- $\beta_1, \overline{\beta_1}, \dots, \beta_q, \overline{\beta_s}$ les racines complexes non réelles de P (deux à deux distinctes).
- $n_1, \dots, n_s$ les multiplicités respectives de $\beta_1, \dots, \beta_s$ (ce sont aussi les multiplicités de $\overline{\beta_1}, \dots, \overline{\beta_s}$).

D'après la factorisation de P en produit de facteurs irréductibles dans $\mathbb{C}[X]$, on a

$$\begin{aligned} P &= \lambda \left(\prod_{k=1}^{r} (X - \alpha_k)^{m_k} \right) \left(\prod_{k=1}^{s} (X - \beta_k)^{n_k} \right) \left(\prod_{k=1}^{s} (X - \overline{\beta_k})^{n_k} \right) \\ &= \lambda \left(\prod_{k=1}^{r} (X - \alpha_k)^{m_k} \right) \left(\prod_{k=1}^{s} \left[(X - \beta_k)(X - \overline{\beta_k}) \right]^{n_k} \right). \end{aligned}$$

Or, pour tout $k \in [\![1, s]\!]$,

$$(X - \beta_k)(X - \overline{\beta_k}) = X^2 - (\beta_k + \overline{\beta_k})X + \beta_k \overline{\beta_k} = X^2 - 2\,\mathrm{Re}(\beta_k)X + |\beta_k|^2,$$

ce qui donne un polynôme à coefficients réels, de discriminant négatif. D'où la décomposition annoncée. □

Pour factoriser un polynôme sur $\mathbb{R}$, on peut factoriser sur $\mathbb{C}$, puis regrouper les termes complexes conjuguées. Attention : un polynôme qui n'a pas de racines réelle n'est pas nécessairement irréductible, cf exemple ci-dessous.

Exemple 12 : Décomposer $X^4 + 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

5.4 Décomposition, PGCD, PPCM

Soit $A,B \in \mathbb{K}[X]$ non constants. Soit $P_1,\dots,P_r$ des polynômes irréductibles sur $\mathbb{K}$ qui permettent de décomposer A et B, càd tels que

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r} \qquad \text{et} \qquad B = \mu P_1^{\beta_1} P_2^{\beta_2} \dots P_r^{\beta_r}$$

avec $\lambda,\mu \in \mathbb{K}^*$ et $\alpha_1,\beta_1,\dots,\alpha_r,\beta_r \in \mathbb{N}$.

Dans ce cas, on peut déduire le PGCD et le PPCM de A et B :

$$A \wedge B = \prod_{k=1}^{r} P_k^{\min(\alpha_k,\beta_k)} \qquad \text{et} \qquad A \vee B = \prod_{k=1}^{r} P_k^{\max(\alpha_k,\beta_k)}$$

Exemple 13 : Si $A = 2(X-1)X^2$ et $B = (X-1)^2X(X+1)$ alors

$$A \wedge B = (X-1)X \qquad \text{et} \qquad A \vee B = (X-1)^2X^2(X+1)$$

Comme tout polynôme irréductible sur $\mathbb{C}$ admet une racine, on en déduit le résultat suivant :

Propriété 49

Si $P,Q \in \mathbb{C}[X]$, alors $P \wedge Q = 1$ si et seulement si P et Q n'ont pas de racine commune dans $\mathbb{C}$.

Pour appliquer ce résultat, il faut absolument regarder s'il y a une racine *complexe* commune : $P = (X^2+1)$ et $Q = (X^2+1)^2$ n'ont pas de racine commune dans $\mathbb{R}$, mais on voit facilement que P et Q ne sont pas premiers entre eux (car $P \mid Q$). C'est cohérent avec la propriété ci-dessus, puisque P et Q ont au moins une racine commune dans $\mathbb{C}$ (à savoir i et $-i$).

6 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

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

Propriété 50

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

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

$\delta_{i,j}$ est appelé **symbole de Kronecker**.

Démonstration

Si $j=i$, alors $L_i(x_i)=\prod_{\substack{1\leq k\leq n\\ k\neq i}}\frac{x_i-x_k}{x_i-x_k}=\prod_{\substack{1\leq k\leq n\\ k\neq i}}1=1.$

Si $j\neq i$, alors $L_i(x_j)=\prod_{\substack{1\leq k\leq n\\ k\neq i}}\frac{x_j-x_k}{x_i-x_k}=\underbrace{\frac{x_j-x_j}{x_i-x_j}}_{=0}\prod_{\substack{1\leq k\leq n\\ k\neq i,\,k\neq j}}\frac{x_j-x_k}{x_i-x_k}=0.$

Définition 23 : Polynôme de Lagrange

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

- Soit $x_1,\dots,x_n\in\mathbb{K}$ des scalaires tous distincts.
- Soit $y_1,\dots,y_n\in\mathbb{K}$ des scalaires quelconques.

Alors il existe un unique polynôme $P\in\mathbb{K}_{n-1}[X]$ qui passe par les points $(x_1,y_1),\dots,(x_n,y_n)$, càd tel que pour tout j, on a $P(x_j)=y_j$. Il est donné par :

$$P(X)=\sum_{i=1}^{n}y_iL_i(X)=\sum_{i=1}^{n}y_i\prod_{\substack{1\leq k\leq n\\ k\neq i}}\frac{X-x_k}{x_i-x_k}\quad\in\mathbb{K}_{n-1}[X]$$

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

Démonstration

Existence : Soit P le polynôme défini ci-dessus. Comme $y_iL_i\in\mathbb{K}_{n-1}[X]$, par somme $P\in\mathbb{K}_{n-1}[X]$. De plus,

$$P(x_j)=\sum_{i=1}^{n}y_iL_i(x_j)=\sum_{i=1}^{n}y_i\delta_{i,j}=y_j$$

Unicité : Soit $P_1,P_2\in\mathbb{K}_{n-1}[X]$ tels que pour tout $j\in[\![1,n]\!]$ on a $P_1(x_j)=P_2(x_j)=y_j$. Alors $(P_1-P_2)(x_j)=0$. Le polynôme P_1-P_2 admet donc n racines $x_1,\dots,x_n$ et comme ce polynôme est de degré au plus $n-1$, il s'agit du polynôme nul : $P_1-P_2=0$. Donc $P_1=P_2$ et il y a unicité.

Exemple 14 : Le polynôme d'interpolation de Lagrange qui passe par les points (1,2) et (3,5) est dans $\mathbb{K}_1[X]$, donc de la forme $aX+b$. Il s'agit en fait de la droite affine qui passe par ces deux points.

Exemple 15 : On cherche le polynôme d'interpolation de Lagrange qui passe par les points

$$(x_1,y_1)=(0,-1)\qquad(x_2,y_2)=(1,4)\qquad(x_3,y_3)=(-2,1)$$

On détermine d'abord les polynômes L_i :

$$L_1(X)=\prod_{k=2}^{3}\frac{X-x_k}{x_1-x_k}=\frac{X-x_2}{x_1-x_2}\cdot\frac{X-x_3}{x_1-x_3}=\frac{X-1}{0-1}\cdot\frac{X-(-2)}{0-(-2)}=-\frac{1}{2}(X-1)(X+2)$$

$$L_2(X)=\prod_{\substack{k=1\\ k\neq 2}}^{3}\frac{X-x_k}{x_2-x_k}=\frac{X-x_1}{x_2-x_1}\cdot\frac{X-x_3}{x_2-x_3}=\frac{X-0}{1-0}\cdot\frac{X-(-2)}{1-(-2)}=\frac{1}{3}X(X+2)$$

et de même $L_3(X)=\frac{1}{6}X(X-1)$. Ensuite, on peut déterminer P :

$$P=\sum_{i=1}^{3}y_iL_i=-L_1+4L_2+L_3=\quad(\dots)\quad=2X^2-3X+1$$

On peut vérifier qu'effectivement $P(0)=-1$, $P(1)=4$ et $P(-2)=1$.