3. Polynômes

Dans ce chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$, et $\mathbb{K}^{\mathbb{N}}$ représente l'ensemble des suites d'éléments dans $\mathbb{K}$.

3.1 Notions de base

Définition 3.1 Pour tout suite $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}^{\mathbb{N}}$, on appelle support de $(a_n)_{n\in\mathbb{N}}$ l'ensemble

$$J = \{n \in \mathbb{N},\ a_n \neq 0\}.$$

– Une suite $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}^{\mathbb{N}}$ est dite presque nulle lorsque son support J est fini.

– Les polynôme à coefficients dans $\mathbb{K}$ sont les suites presque nulles d'éléments dans $\mathbb{K}$, et leur ensemble est noté $\mathbb{K}^{(\mathbb{N})}$.

Propriétés 3.1 – L'ensemble $(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ est un espace vectoriel sur $\mathbb{K}$ pour les lois usuelles :

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}} \quad \text{et} \quad \lambda \cdot (a_n)_{n\in\mathbb{N}} = (\lambda\, a_n)_{n\in\mathbb{N}} \quad (\forall \lambda \in \mathbb{K}).$$

– L'ensemble $(\mathbb{K}^{(\mathbb{N})}, +, \cdot)$ est un anneau commutatif pour le produit suivant :

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}} \quad \text{tel que} \quad c_n = \sum_{k=0}^{n} a_k\, b_{n-k}.$$

Écritures d'un polynôme : Soient $(i, j) \in \mathbb{N}^2$, on définit le symbole de Kronecker δ_{ij} par

$$\delta_{ij} = \begin{cases} 1 & \text{si} \quad i = j, \\ 0 & \text{si} \quad i \neq j \end{cases}$$

Notons p_k la suite $(\delta_{kn})_{n\in\mathbb{N}}$ (1 en $k^{\text{ème}}$ position et 0 ailleurs). Pour tout $a \in \mathbb{K}^{(\mathbb{N})}$ de support J, on a

$$a = (a_k)_{k\in\mathbb{N}} = \sum_{k\in\mathbb{N}} a_k\, p_k = \sum_{k\in J} a_k\, p_k.$$

Notons $p_1 = (0,1,0,\dots)$ par X : c'est l'indéterminée de $\mathbb{K}^{(\mathbb{N})}$, et pour tout $n \in \mathbb{N}$, on a

$$\forall n \in \mathbb{N}^*, \quad p_n = X^n \quad \text{et par convention, on pose} \quad X^0 = 1.$$

Par conséquent, tout polynôme $a = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$ s'écrit

$$a = \sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\in J} a_n X^n.$$

Avec cette nouvelle écriture, l'ensemble $\mathbb{K}^{(\mathbb{N})}$ des polynôme à coefficient dans $\mathbb{K}$, se notera $\mathbb{K}[X]$.

Remarque Si $P = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{K}[X]$ est à support I vide, on dit que P est le polynôme nul, on a :

$$P = 0_{\mathbb{K}[X]} \iff \forall n \in \mathbb{N},\ a_n = 0 \iff I = \emptyset.$$

Définition 3.2 — Degré d'un polynôme. Soit $P = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{K}[X]$ un polynôme et I son support. Le degré de du polynôme P, noté $\deg(P)$, est l'élément de $\mathbb{N}\cup\{-\infty\}$ défini par :

- $\deg(P) = \sup(I)$ si $I \neq \emptyset$,
- $\deg(P) = -\infty$ si $I = \emptyset$, c'est-à-dire si $P = 0_{\mathbb{K}[X]}$.

Remarque Si le polynôme $P = \sum_{n\in\mathbb{N}} a_n X^n$ est non nul de degré p, alors le terme a_p est dit coefficient dominant de P, et le polynôme P est dit unitaire (ou normalisé) lorsque son coefficient dominant est

$$a_p = 1.$$

Propriétés 3.2 Deux polynômes P et Q sont égaux lorsque ils sont de même degré et leurs coefficients respectifs sont égaux et on écrit $P = Q$.

Proposition 3.1 Étant donné deux polynômes $P = \sum_{n\in\mathbb{N}} a_n X^n$ et $Q = \sum_{n\in\mathbb{N}} b_n X^n$, on a

$$\deg(P+Q) \leqslant \sup(\deg(P), \deg(Q)).$$

Preuve *On sait que $a_n + b_n = 0$ dès que on a : $a_n = 0$ et $b_n = 0$, et cela prouve que*

$$\deg(P+Q) \leqslant \sup(\deg(P), \deg(Q)).$$

■

Remarque Soit $p = \deg(P)$ et $q = \deg(Q)$ avec par exemple $p < q$. On a

$$\deg(P+Q) \leqslant \sup(\deg(P), \deg(Q)) = q.$$

D'autre part, $a_q = 0$ et $b_q \neq 0$, alors $a_q + b_q \neq 0$ et donc $\deg(P+Q) \geqslant q$. Ce qui montre

$$\deg(P) \neq \deg(Q) \implies \deg(P+Q) = \sup(\deg(P), \deg(Q)).$$

Corollaire 3.1 Pour tous $n \in \mathbb{N}$, l'ensemble des polynôme P tels que $\deg(P) \leqslant n$, noté $\mathbb{K}_n[X]$, est un sous-espace vectoriel de l'espace des polynômes $\mathbb{K}[X]$.

Preuve *Ce sous-ensemble est non vide puisque il contient le polynôme nul. De plus, on a*

$$\forall P \in \mathbb{K}_n[X], \forall Q \in \mathbb{K}_n[X] : \ P+Q \in \mathbb{K}_n[X],$$

puisque

$$\deg(P+Q) \leqslant \sup(\deg(P), \deg(Q)) \leqslant n.$$

Et on a

$$\forall P \in \mathbb{K}_n[X], \forall \lambda \in \mathbb{K} : \ \lambda P \in \mathbb{K}_n[X],$$

puisque

$$\lambda P = 0_{\mathbb{K}[X]} \ \ si \ \ \lambda = 0 \quad et \quad \deg(\lambda P) = \deg(P) \ \ si \ \ \lambda \neq 0.$$

■

Proposition 3.2 Soient $P = \sum_{n\in\mathbb{N}} a_n X^n$ et $P = \sum_{n\in\mathbb{N}} b_n X^n$ deux polynômes de $\mathbb{K}[X]$, on a

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

Preuve *Supposons que* $P = \sum_{n=0}^{p} a_n X^n$ *et* $Q = \sum_{n=0}^{q} b_n X^n$ *sont non nuls, de degrés respectifs* p *et* q. *Le produit de* PQ *a pour coefficients*

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Si $n > p+q$ *et* $0 \leqslant k \leqslant n$, *on a :* $k > p$ *ou* $n-k > q$, *d'où* $a_k = 0$ *ou* $b_{n-k} = 0$, *et donc*

$$c_n = 0.$$

Si $n = p+q$ *et* $0 \leqslant k \leqslant n = p+q$, *on a :* $k > p$ *ou* $n-k > q$ *ou* $k = p$ *ou* $n-k = q$, *et donc*

$$c_n = c_{p+q} = a_p b_q \neq 0 \quad (car\ a_p \neq 0 \ \ et \ \ b_q \neq 0).$$

■

Corollaire 3.2 L'anneau $(\mathbb{K}[X], +, \cdot)$ est un anneau intègre puisque

$$PQ = 0 \implies P = 0 \ \text{ ou } \ Q = 0.$$

Les éléments inversibles de $\mathbb{K}[X]$ sont les scalaire non nuls, c'est-à-dire $\mathbb{K}^*$.

Preuve *Si* $P \in \mathbb{K}[X]$ *est inversible, alors il existe* $Q \in \mathbb{K}[X]$ *tel que* $PQ = 1$ *et donc*

$$\deg(PQ) = \deg(P) + \deg(Q) = 0.$$

Ainsi, on trouve

$$\deg(P) = \deg(Q) = 0.$$

Finalement, seul les polynômes constants et non nuls sont inversibles. ■

Propriétés 3.3 Soit $P=\sum_{k\in\mathbb{N}} a_k X^k$ et Q deux polynômes, on appelle polynôme composée de P et Q, le polynôme noté $P\circ Q$, et défini par $P=\sum_{k\in\mathbb{N}} a_k\, Q^k$. Si de plus, $Q\neq 0$, alors on a

$$\deg(P\circ Q)=\deg(P)\times\deg(Q).$$

Exercice 3.1 *Calculer* $P=\sum_{k=0}^{n} C_n^k\, X^k\,(1-X)^{n-k}$ *et* $Q=\sum_{k=0}^{n} k\, C_n^k\, X^k\,(1-X)^{n-k}$ *où* $n\in\mathbb{N}$ *fixé.*

Exercice 3.2 *Déterminer tous les polynômes* $P\in\mathbb{K}[X]$ *vérifiant :* $P(X^2)=(X^2+1)P(X)$.

3.2 Arithmétique dans $\mathbb{K}[X]$

Définition 3.3 Soient P et Q deux polynômes de $\mathbb{K}[X]$ avec $Q\neq 0$. On dit que Q divise P (ou encore : P est divisible par Q) lorsqu'il existe $T\in\mathbb{K}[X]$ tel que $P=QT$ et on écrit $Q\mid P$.

Exemple. On a $X^3-1=(X-1)(X^2+X+1)$, alors $(X-1)$ divise X^3-1 .

R On note que le polynôme nul $P=0$ est divisible par tous les polynômes et que le polynôme constant $Q=\lambda\in\mathbb{K}^*$ divise tous les polynômes non nuls de $\mathbb{K}[X]$.

Définition 3.4 Deux polynômes non nuls P et Q sont dits associés s'il existe $\lambda\in\mathbb{K}^*$ tels que

$$P=\lambda Q.$$

Exercice 3.3 *Soient* P *et* Q *deux polynômes non nuls. Montrer que*

$$Q\mid P\Rightarrow \deg(Q)\leqslant\deg(P)\ ;\ \ Q\mid P\ et\ R\mid Q\Rightarrow R\mid P\ ;\ \ Q\mid P\ et\ P\mid Q\Rightarrow\exists\lambda\in\mathbb{K}^*,\ P=\lambda Q.$$

Exercice 3.4 *Montrer que, pour tout* $P\in\mathbb{K}[X]$, *on a :* $P(X)-X$ *divise* $P[P(X)]-X$

Théorème 3.1 — Division euclidienne. Soient $A,B\in\mathbb{K}[X]$ deux polynômes avec $B\neq 0$. Il existe un unique couple (Q,R) de polynômes de $\mathbb{K}[X]$ vérifiant

$$A=BQ+R\quad\text{et}\quad\deg(R)<\deg(B).$$

On dit que Q est le quotient et R est le reste de la division euclidienne de A par B.

Preuve *Soit* $A=BQ+R=BQ'+R'$ *avec* $\deg(R)<\deg(B)$ *et* $\deg(R')<\deg(B)$, *on a*

$$B(Q-Q')=R'-R,$$

et par suite, il vient

$$\deg(B)+\deg(Q-Q')=\deg(R'-R).$$

Or $\deg(R'-R) \leqslant \sup(\deg(R'),\deg(R)) < \deg(B)$, *alors*

$$\deg(B)+\deg(Q-Q') < \deg(B).$$

Par suite, on obtient $\deg(Q-Q') = -\infty$, *c'est-à-dire*

$$Q-Q' = 0 \quad d'où \quad R-R' = 0.$$

Ainsi, la partie unicité est établie. Pour l'existence, soit B un polynôme de degré p et de coefficient dominant b_p, *alors :*

$-$ *si* $A = 0$ *ou* $A \neq 0$ *avec* $\deg(A) < p$, *on a*

$$A = 0\cdot B + A \quad et\ donc \quad Q = 0 \ \ et \ \ R = A.$$

$-$ *supposons établit, l'existence du quotient et reste dans la division par B de tout polynôme de degré inférieur ou égal à n. Soit A un polynôme de degré* $n+1$ *et de coefficient dominant* a_{n+1}, *posons*

$$A_1 = A - \frac{a_{n+1}}{b_p} X^{n+1-p} B.$$

On a : $\deg(A_1) \leqslant n$, *et par hypothèse de récurrence, il existe* Q_1 *et* R_1 *tels que*

$$A_1 = BQ_1 + R_1 \quad et \quad \deg(R_1) < \deg(B).$$

d'où

$$A = B\left(Q_1 + \frac{a_{n+1}}{b_p} X^{n+1-p}\right) + R_1 \quad et \quad \deg(R_1) < \deg(B).$$

Les polynômes $R = R_1$ *et* $Q = Q_1 + \frac{a_{n+1}}{b_p} X^{n+1-p}$ *vérifie la relation voulue, et donc la partie existence est établie par récurrence sur* $n = \deg(A)$.

■

Exemple. Effectuons la division euclidienne de $A = 6X^3 - 2X^2 + 6X + 3$ par $B = X^2 - X + 1$

$$\begin{array}{rl|l}
 & 6X^3 - 2X^2 + \ X + 3 & X^2 - \ X + 1 \\
\hline
- & 6X^3 - 6X^2 + 6X & Q = 6X + 4 \\
\hline
 & \quad 4X^2 - 5X + 3 & \\
- & \quad 4X^2 - 4X + 4 & \\
\hline
 & \quad R = -X - 1 &
\end{array}$$

Remarque $B \mid A$ si et seulement si le reste de la division euclidienne de A par B est nul.

Exercice 3.5 *Effectuer la division euclidienne de* $A = X^5 + 2X^3 - 2X - 2$ *par* $B = X^2 + 1$.

Exercice 3.6 *Exprimer le reste de la division euclidienne de* $P \in \mathbb{K}[X]$ *par* $(X-a)(X-b)$ *où* $a \neq b \in \mathbb{K}$, *en fonction de* $P(a)$ *et* $P(b)$.

Exercice 3.7 *Soient $A_1 = BQ_1 + R_1$ et $A_2 = BQ_2 + R_2$ les divisions euclidiennes respectives de A_1 par B et de A_2 par B. Quel est le reste R de la division euclidienne de de $A_1 + A_2$ par B ? A-t-on un résultat similaire pour la division euclidienne dans $\mathbb{N}$.*

Le résultat suivant, qui est une conséquence de $A = BQ + R$ et $R = A - BQ$, est la base de l'algorithme d'Euclide qui permet de déterminer le plus grand diviseur commun de deux polynômes.

Proposition 3.3 — Algorithme d'Euclide. Soient A et B deux polynômes de $\mathbb{K}[X]$ avec $B \neq 0$. Si Q et R sont le quotient et le reste de la division euclidienne de A par B, alors les diviseurs communs à A et B sont les mêmes que les diviseurs communs à B et R.

Théorème 3.2 Soient A et B deux polynômes de $\mathbb{K}[X]$. Il existe un unique polynôme nul ou unitaire $D \in \mathbb{K}[X]$ dont les diviseurs sont les diviseurs communs de A et B, c-à-dire

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

Le polynôme D est dit le plus grand commun diviseur de A et B et on écrit $D = \operatorname{pgcd}(A,B)$.

Remarque On note que

$$\operatorname{pgcd}(A,B) = 0 \iff A = B = 0 \ ; \quad B \mid A \iff \operatorname{pgcd}(A,B) = B \text{ normalisé.}$$

Et que le $\operatorname{pgcd}(A,B)$ est le dernier reste non nul et normalisé de l'algorithme d'Euclide.

Théorème 3.3 — d'Euclide. Si les A, B, Q et $R \in \mathbb{K}[X]$ non nuls vérifient $A = BQ + R$, alors

$$\operatorname{pgcd}(A,B) = \operatorname{pgcd}(B,R).$$

Exemple. Calculons $\operatorname{pgcd}(A,B)$ pour $A = X^3 + 2X^2 - X - 2$ et $B = X^2 + 4X + 3$. On a

$$\begin{array}{r|l} X^3+2X^2-X-2 & X^2+4X+3 \\ \hline X^3+4X^2+3X & X-2 \\ \hline -2X^2-4X-2 & \\ -2X^2-8X-6 & \\ \hline R_0 = 4X+4 & \end{array} \quad \text{et} \quad \begin{array}{r|l} X^2+4X+3 & 4X+4 \\ \hline X^2+X & (1/4)X+(3/4) \\ \hline 3X+3 & \\ 3X+3 & \\ \hline 0 & \end{array}$$

alors

$$\operatorname{pgcd}(A,B) = \operatorname{pgcd}(B,R_0) = \frac{1}{4}(4X+4) = X+1.$$

Exercice 3.8 *Calculer :* $\operatorname{pgcd}(X^5 - 4X^4 + 6X^3 - 6X^2 + 5X - 2; X^4 + X^3 + 2X^2 + X + 1)$

Exercice 3.9 *Soient $n, m \in \mathbb{N}^*$ et $\delta = \operatorname{pgcd}(n,m)$. Montrer que*

$$\operatorname{pgcd}(X^n - 1, X^m - 1) = X^\delta - 1.$$

Théorème 3.4 Soient A et B deux polynômes tels que $D = \text{pgcd}(A,B)$, alors

$$\exists\, U, V \in \mathbb{K}[X], \quad AU + BV = D.$$

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

Propriétés 3.4 Si Δ divise A et divise B, alors Δ divise $D = \text{pgcd}(A,B)$.

Preuve *On sait qu'il existe U et V tels que $D = UA + VB$. Comme Δ divise A et B, alors*

$$\Delta \mid UA + VB = D.$$

■

Propriétés 3.5 Soient A, B et C trois polynômes non nuls tels que C est unitaire, alors on a

$$\text{pgcd}(AC, BC) = \text{pgcd}(A,B)C.$$

Définition 3.5 Deux polynômes non nuls A et B sont dits premiers entre eux lorsque

$$\text{pgcd}(A,B) = 1.$$

Exemple. Soient $A = X - a$ et $B = X - b$ avec $a \neq b$. Le reste de la division euclidienne de $X - a$ par $X - b$ est $R = b - q \neq 0$, alors d'après l'algorithme d'Euclide, on a

$$\text{pgcd}(A,B) = 1 \text{ et donc } A \text{ et } B \text{ sont premiers entre eux.}$$

Théorème 3.5 — de Bezout. A et B non nuls, sont premiers entre eux si et seulement si

$$\exists U, V \in \mathbb{K}[X], \quad AU + BV = 1.$$

Preuve *($\Rightarrow$) : si A et B sont premiers entre eux,* $\text{pgcd}(A,B) = 1$ *et donc il existe U et V tels que*

$$AU + BV = 1.$$

($\Leftarrow$) : inversement, s'il existe U et V tels que $AU + BV = 1$, alors 1 est un diviseur commun à A et B, et par suite il est le polynôme unitaire de degré minimal qui divise A et B. C'est donc le pgcd *de A et B, et alors A et B sont premiers entre eux.*

■

Exemple. En remontant l'algorithme d'Euclide, on peut alors trouver un couple de coefficients de Bézout. Considérons par exemple $A = X^4 + 3X^3 - 2X^2 - X - 1$ et $B = -X^3 + 2X^2 - 4X + 3$, alors

$$\begin{array}{r|l}
X^4 + 3X^3 - 2X^2 - X - 1 & -X^3 + 2X^2 - 4X + 3 \\
\cline{2-2}
- \; X^4 - 2X^3 + 4X^2 - 3X & -X - 5 \\
\cline{1-1}
5X^3 - 6X^2 + 2X - 1 & \\
- \; 5X^3 - 10X^2 + 20X - 15 & \\
\cline{1-1}
R_0 = 4X^2 - 18X + 14 &
\end{array}$$

$$\begin{array}{r|l} -X^3+2X^2-4X+3 & 4X^2-18X+14 \\ \cline{2-2} -X^3+\frac{9}{2}X^2-\frac{7}{2}X & -\frac{1}{4}X-\frac{5}{8} \\ \cline{1-1} -\frac{5}{2}X^2-\frac{1}{2}X+3 & \\ -\frac{5}{2}X^2+\frac{45}{4}X-\frac{35}{4} & \\ \cline{1-1} R_1=-\frac{47}{4}X+\frac{47}{4} & \end{array}$$

$$\begin{array}{r|l} 4X^2-18X+14 & -\frac{47}{4}(X-1) \\ \cline{2-2} 4X^2-4X & -\frac{4}{47}(4X-14) \\ \cline{1-1} -14X+14 & \\ -14X+14 & \\ \cline{1-1} R_2=0 & \end{array}$$

d'où $D=\text{pgcd}(A,B)=R_1$ normalisée $=X-1$. De plus, on a

$$A=B\,(-X-5)+R_0 \qquad \text{et} \qquad B=R_0\,(-\frac{1}{4}X-\frac{5}{8})+R_1\,.$$

alors

$$\begin{aligned} R_1 &= B-R_0\,(-\frac{1}{4}X-\frac{5}{8}) \\ &= B-\underbrace{\big[A-B\,(-X-5)\big]}_{R_0}\,(-\frac{1}{4}X-\frac{5}{8}) \\ &= (-\frac{1}{4}X-\frac{5}{8})\,A+\big[\frac{1}{4}X^2+\frac{15}{4}X+\frac{33}{8}X\big]\,B. \end{aligned}$$

Et donc

$$D=\ -\frac{4}{47}\,R_1=\underbrace{\big[\frac{1}{47}X+\frac{5}{94}\big]}_{U}\,A+\underbrace{\big[\frac{-1}{47}X^2-\frac{15}{47}X-\frac{33}{94}X\big]}_{V}\,B\,.$$

Exercice 3.10 *Soit A et B tels que* $\text{pgcd}(A,B)=1$. *Montrer que si C divise A, alors*

$$\text{pgcd}(C,B)=1.$$

Remarque Soit D normalisé, un diviseur commun de A et B, c-à-dire $A=DA_1$ et $B=DB_1$, on a

$$\text{pgcd}(A,B)=D \iff \text{pgcd}(A_1,B_1)=1.$$

Propriétés 3.6 Soient A, B et C des polynômes, alors on a :

$$\text{pgcd}(A,BC)=1 \iff [\text{pgcd}(A,B)=1 \ \text{ et } \ \text{pgcd}(A,C)=1].$$

Preuve *($\Rightarrow$) : supposons* $\text{pgcd}(A,BC)=1$*, il existe U et V tels que* $UA+VBC=1$*. En utilisant*

$$UA+(VB)C=1 \ \text{ et } \ UA+(VC)B=1,$$

il vient que

$$\text{pgcd}(A,B)=1 \ \text{ et } \ \text{pgcd}(A,C)=1.$$

($\Leftarrow$) : supposons $\text{pgcd}(A,B)=1$ *et* $\text{pgcd}(A,C)=1$*, il existe U, V, S et T tels que*

$$UA+VB=1 \ \text{ et } \ SA+TC=1.$$

Multiplions les deux égalités, membre par membre, on obtient

$$(UAS+VBS+UTC)A+(VT)BC=1.$$

Ce qui montre que $\text{pgcd}(A,BC)=1$.

■

Corollaire 3.3 A est premier avec un produit $\prod_{i=1}^{n} B_i = B_1B_2\cdots B_n$ si et seulement si

$$\forall i=1,..,n: \quad \text{pgcd}(A,B_i)=1.$$

Corollaire 3.4 Soient A et B des polynômes non nuls, alors, pour tous n et p dans $\mathbb{N}^*$, on a :

$$\text{pgcd}(A,B)=1 \iff \text{pgcd}(A^n,B^p)=1.$$

Théorème 3.6 — de Gauss. Si $\text{pgcd}(A,B)=1$ et si A divise BC, alors A divise C.

Preuve *On déduit de* $\text{pgcd}(A,B)=1$ *qu'il existe U et V tels que* $UA+VB=1$*, et donc*

$$UAC+VBC=C.$$

Or A divise UAC et divise VBC, alors il divise également C.

■

Propriétés 3.7 Si $\text{pgcd}(A,B)=1$ alors $\text{pgcd}(A,BC)=\text{pgcd}(A,C)$.

Preuve *Si D divise A et C, il divise A et BC. Soit D un diviseur commun de A et BC, de* $D \mid A$ *et* $\text{pgcd}(A,B)=1$*, il vient* $\text{pgcd}(D,B)=1$ *et donc, d'après le théorème de Gauss,* $D \mid C$*. Puisque, les diviseurs communs à A et C sont les mêmes que les diviseurs communs à A et BC, il vient*

$$\text{pgcd}(A,C)=\text{pgcd}(A,BC).$$

■

Propriétés 3.8 Si A_1 divise B, A_2 divise B et $\text{pgcd}(A_1,A_2)=1$, alors

$$A_1A_2 \ \text{ divise } \ B.$$

Preuve *On a* A_1 *divise B, soit* $B=A_1Q$*, et puisque* $A_2 \mid B$*, on trouve*

$$A_2 \mid B=A_1Q.$$

Or $\text{pgcd}(A_1,A_2)=1$*, donc d'après le théorème de Gauss,* $A_2 \mid Q$*, soit* $Q=A_2S$*. Ainsi, il vient*

$$B=A_1A_2S.$$

■

Corollaire 3.5 Si $A_1, \cdots, A_n$ sont deux à deux premiers entre eux et si tout les A_i divise B, alors

$$\prod_{i=1}^{n} A_i = A_1 A_2 \cdots A_n \text{ divise } B.$$

Exercice 3.11 *Soient A et $B \in \mathbb{K}[X]^*$, montrer que*

$$\text{pgcd}(A,B) = 1 \iff \text{pgcd}(A+B, AB) = 1.$$

3.3 Fonctions polynomiales et divisibilité

La fonction polynomiale associée à $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ est l'application, notée $\tilde{P}$ ou P, suivante :

$$\begin{array}{rccc} \tilde{P}: & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & \sum_{k=0}^{n} a_k x^k \end{array}$$

Définition 3.6 On dit qu'un élément $\alpha \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$ lorsque $\tilde{P}(\alpha) = 0$.

Exemple. Soit $P = X^{n+1} + X^n - 2X^{n-1} + nX - n$ où $n \in \mathbb{N}^*$ un polynôme de $\mathbb{R}[X]$. On a

$$P(1) = 1 + 1 - 2 + n - n = 0 \text{ et alors } \alpha = 1 \text{ est une racine de } P.$$

Théorème 3.7 Un polynôme est divisible par $X - \alpha$ si et seulement si α est racine de P.

Preuve *Dans la division euclidienne de P par $X - \alpha$, le reste est un polynôme constant*

$$P = (X - \alpha)Q + r \text{ avec } r \in \mathbb{K}.$$

Par conséquent, on obtient $P(\alpha) = r$, d'où le résultat voulu.

■

Corollaire 3.6 Si un polynôme P admet n racines $\alpha_1, \alpha_2, \ldots, \alpha_n$ deux à deux distincts, alors

$$(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n) \text{ divise } P.$$

Preuve *On procède par récurrence sur n. La propriété est vraie pour $n = 1$, supposons-la vraie pour $n \in \mathbb{N}^*$ et soit $P \in \mathbb{K}[X]$ admettant $n+1$ racines distincts $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$. D'après le théorème précédent, P est divisible par $X - \alpha_{n+1}$, donc*

$$P(X) = (X - \alpha_{n+1})\, Q(X).$$

Comme $\alpha_1, \ldots, \alpha_n$ sont des racines de Q, l'hypothèse de récurrence implique que

$$(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n) \text{ divise } Q,$$

donc il existe $R \in \mathbb{K}[X]$ tel que $Q(X) = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)R(X)$. Finalement, on a

$$P(X) = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)(X - \alpha_{n+1})\, R(X).$$

Ce qui prouve que la la propriété est récurrente.

■

Théorème 3.8 Si $P \in \mathbb{K}_n[X]$ admet au moins $n+1$ racines distincts, alors P est nul.

Preuve *D'après le corollaire précédent, il existe* $R \in \mathbb{K}[X]$ *tel que*

$$P(X) = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)(X-\alpha_{n+1})R(X).$$

Pour $R \neq 0$, *on a* $\deg(P) \geqslant n+1$, *ce qui est contraire à l'hypothèse, donc*

$$R = 0 \ \text{ et puis } \ P = 0.$$

■

Remarque Pour démontrer qu'un polynôme est nul, on utilise souvent :

- si $P \in \mathbb{K}[X]$ admet une infinité de racines dans $\mathbb{K}$, alors $P = 0$.
- si $P \in \mathbb{K}_n[X]$ admet plus que n racines distincts dans $\mathbb{K}$, alors $P = 0$.

Exemple. Soit $n \in \mathbb{N}$, on sait qu'il existe un polynôme P tel que

$$\forall x \in \mathbb{R} \ : \ P(\cos x) = \cos(nx).$$

Montrons l'unicité du polynôme P, supposons qu'il en existe deux, soit P et Q, alors

$$\forall x \in \mathbb{R} \ : \ (P-Q)(\cos x) = 0.$$

Comme la fonction cosinus a pour image [-1,1], alors

$$\forall u \in [-1,1], \quad (P-Q)(u) = 0.$$

Donc le polynôme $P-Q$ possède une infinité de racines, et par suite

$$P = Q.$$

Exercice 3.12 *Montrer que si P est de degré n admettant n racines distincts* $\alpha_1, \cdots, \alpha_n$, *alors*

$$P = c_n \prod_{i=1}^{n} (X-\alpha_i) \quad \text{où } c_n \text{ est le coefficient dominant de } P.$$

3.4 Dérivation des polynômes - Ordre de multiplicité d'une racine

Définition 3.7 Le polynôme dérivé de $P = \sum_{k=0}^{n} a_k X^k$ est le polynôme

$$P' = \sum_{k=0}^{n} (k+1)\, a_{k+1} X^k.$$

On définit les dérivées successives de $P \in \mathbb{K}[X]$, par les relations suivantes :

$$P^{(0)} = P\,, \quad P^{(1)} = P' \quad \text{et} \quad \forall k \geqslant 2\,, \ P^{(k)} = \left(P^{(k-1)}\right)'.$$

Proposition 3.4 Soit $P=\sum_{k=0}^{n} a_k X^k$ un polynôme de degré $n>0$, alors

$$\begin{cases} P^{(j)}=\sum_{k=j}^{n} k(k-1)\cdots(k-j+1)\, a_k\, X^{k-j} & \text{si} \quad j\leqslant n \\ P^{(j)}=0 \quad \text{si} \quad j>n. \end{cases}$$

Remarque Les règles sur la dérivation des polynômes sont identiques à celles des fonctions. On a

$$(P+Q)'=P'+Q' \; ; \; (\lambda P)'=\lambda P' \; ; \; (PQ)'=PQ'+P'Q,$$

$$(PQ)^{(n)}=\sum_{k=0}^{n} C_n^k\, P^{(k)}\, Q^{(n-k)} \quad \text{(formule de Leibnitz)}.$$

Exercice 3.13 1. *Soient $n\in\mathbb{N}$ et $a\in\mathbb{R}$. Démontrer que pour tout entier $j\in[\![1,n]\!]$, on a*

$$((X-a)^n)^{(j)}=n(n-1)\cdots(n-j+1)(X-a)^{n-j}=j!C_n^j(X-a)^{n-j}.$$

2. *En utilisant la formule de Leibnitz, calculer la dérivée $n^{ème}$ en 1 de $P=(X^2-1)^n$.*

Par un raisonnement par récurrence sur le degré d'un polynôme P, on obtient

Théorème 3.9 — Formule de Taylor. Soient $P\in\mathbb{K}[X]$ un polynôme de degré n et $a\in\mathbb{K}$, alors

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

Remarque — Formule de Mac Laurin. Dans le cas particulier où $a=0$, on a

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

Exercice 3.14 *Trouver tout $P\in\mathbb{K}[X]$ unitaires non constants divisibles par P'.*

Exercice 3.15 *Déterminer tous les polynômes $P\in\mathbb{C}[X]$ vérifiant : $(X^2+1)P''-6P=0$.*

Exercice 3.16 *Déterminer les polynômes $P\in\mathbb{K}[X]$ qui vérifie*

$$P(2)=6\,,\;\; P'(2)=1\,,\;\; P''(2)=4 \;\; et \;\; (\forall n\geqslant 3)\,,\; P^{(n)}(2)=0\,.$$

Définition 3.8 — ordre de multiplicité d'une racine. Soit $\alpha\in\mathbb{K}$ une racine de P, on dit que α est d'ordre de multiplicité $k\in\mathbb{N}^*$ lorsque

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

Autrement dit, la racine α est d'ordre de multiplicité k si et seulement si

$$P = (X-\alpha)^k Q + R \text{ avec } R(\alpha) \neq 0.$$

Exemple. Le polynôme $P = (X-1)(X+1)^2(X-2)^3$ possède les trois racines :

- $\alpha_1 = 1$: racine d'ordre de multiplicité 1 (racine simple).
- $\alpha_2 = -1$: racine d'ordre de multiplicité 2 (racine double).
- $\alpha_3 = 2$: racine d'ordre de multiplicité 3 (racine triple).

Proposition 3.5 Une racine α de P est d'ordre de multiplicité k si et seulement si

$$P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \quad \text{et} \quad P^{(k)}(\alpha) \neq 0.$$

Preuve *En écrivant la formule de Taylor, on obtient*

$$\begin{aligned} P(X) &= \sum_{n\in\mathbb{N}} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n \\ &= \left[\sum_{n>k} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^{n-k} + \frac{P^{(k)}(\alpha)}{k!}\right](X-\alpha)^k + \sum_{n=0}^{k-1} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n. \end{aligned}$$

C'est la division euclidienne de P par $(X-\alpha)^k$:

$$P = (X-\alpha)^k Q + R \text{ avec } \deg(R) < k.$$

Par suite, on trouve

- *Si α est d'ordre de multiplicité k, P est divisible par $(X-\alpha)^k$ et donc $R = 0$, d'où*

  $$P^{(n)}(\alpha) = 0 \text{ pour tout } n = 0, \ldots, k-1.$$

  De plus, P n'est pas divisible par $(X-\alpha)^{k+1}$, alors Q n'est pas divisible par $X-\alpha$ d'où

  $$Q(\alpha) \neq 0.$$

  Puis, en utilisant $Q(\alpha) = \dfrac{P^{(k)}(\alpha)}{k!}$, il vient que

  $$P^{(k)}(\alpha) \neq 0.$$

- *Inversement, $P^{(n)}(\alpha) = 0$ pour tout $n = 0, \ldots, k-1$ et $P^{(k)}(\alpha) \neq 0$ implique que R est nul et donc P est divisible par $(X-\alpha)^k$ et non divisible par $(X-\alpha)^{k+1}$ (puisque Q n'est pas divisible par $X-\alpha$). Ainsi, α est une racine d'ordre de multiplicité k, du polynôme P.*

■

Proposition 3.6 Si P est un polynôme non nul, admettant p racines distincts $\alpha_1, \cdots, \alpha_p$ d'ordre de multiplicité respectives $k_1, \cdots, k_p$, alors P est divisible par

$$\prod_{i=1}^{p} (X-\alpha_i)^{k_i} = (X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\cdots(X-\alpha_p)^{k_p}.$$

Corollaire 3.7 Si P est un polynôme non nul de degré n, admettant p racines distincts $\alpha_1, \cdots, \alpha_p$ d'ordre de multiplicité respectives $k_1, \cdots, k_p$ telles que $k_1 + \cdots + k_p = n$, alors

$$P = c_n \prod_{i=1}^{p} (X - a_i)^{k_i} \quad \text{où } c_n \text{ est le coefficient dominant de } P.$$

Exercice 3.17 *Soit $n \in \mathbb{N}^* \setminus \{1\}$.*

1. *Montrer que $P = (X-2)^{2n} + (X-1)^n - 1$ est divisible par $X^2 - 3X + 2$.*
2. *Déterminer les réels a et b pour que $P = aX^{n+1} + bX^n + 1$ soit divisible par $(X-1)^2$.*
3. *Montrer que $(X-1)^3 \mid P = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$. A-t-on $(X-1)^4 \mid P$?*

Exercice 3.18 *Soient P un polynôme de $\mathbb{R}[X]$ et $\alpha \in \mathbb{C}$. Démontrer que si α si est une racine de P, alors $\overline{\alpha}$ est également une racine de P (les racines complexes d'un polynôme à coefficients réels sont deux à deux conjugués).*

3.5 Polynômes irréductibles - Factorisation des polynômes

Définition 3.9 Un polynôme P de $\mathbb{K}[X]$ est dit irréductible lorsque $\deg(P) \geqslant 1$ et les seuls diviseurs de P sont les polynômes constants et les polynômes associés à P.

Autrement dit, P est irréductible s'il n'est pas constant et si pour tout $A, B \in \mathbb{K}[X]$, on a

$$P = AB \implies \deg(A) = 0 \text{ ou } \deg(B) = 0.$$

Remarques. *− L'irréductibilité dépend de l'ensemble $\mathbb{K}$. Par exemple, $P = X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ et il est réductible dans $\mathbb{C}[X]$ puisque $(X + i) \mid P$.*

− Tout polynôme de degré 1 est irréductible dans $\mathbb{K}[X]$. Et tout polynôme irréductible possédant une racine de $\mathbb{K}$ est nécessairement de degré 1.

− Un polynôme qui n'a pas de racine, n'est pas nécessairement irréductible, par l'exemple

$$P = (X^2 + 1)^2 \text{ dans } \mathbb{R}[X].$$

− Un polynôme degré 2 ou 3 qui n'admet pas de racine dans $\mathbb{K}$ est irréductible.

− Un polynôme de degré 2 est irréductible dans $\mathbb{R}[X]$ lorsque son discriminant est strictement négatif (polynôme sans racines réelles).

Théorème 3.10 — Théorème de D'Alembert-Gauss.

- Tout polynôme non constant dans $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.
- Tout polynôme non constant de $\mathbb{C}[X]$ de degré n admet exactement n racines dans $\mathbb{C}$.

Ce théorème assure que les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Proposition 3.7 — Factorisation dans $\mathbb{C}[X]$. Tout polynôme non nul $P \in \mathbb{C}[X]$ de degré n admettant p racines complexes distincts $\alpha_1, \cdots, \alpha_p$ d'ordre de multiplicités respectives $k_1, \cdots, k_p$ et de coefficient dominant c_n, s'écrit sous la forme

$$P = c_n \prod_{i=1}^{p} (X - \alpha_i)^{k_i} \qquad (P \text{ est dit un polynôme scindé}).$$

Exemple. Les racines du polynôme $P = X^4 + 1$ dans $\mathbb{C}$ sont

$$e^{i\frac{\pi}{4}} = \frac{1+i}{\sqrt{2}} \; ; \; e^{i\frac{3\pi}{4}} = \frac{-1+i}{\sqrt{2}} \; ; \; e^{i\frac{5\pi}{4}} = \frac{-1-i}{\sqrt{2}} \; ; \; e^{i\frac{7\pi}{4}} = \frac{1-i}{\sqrt{2}}.$$

Alors, la factorisation du polynôme P dans $\mathbb{C}[X]$ est

$$P = \left(X - e^{i\frac{\pi}{4}}\right)\left(X - e^{i\frac{3\pi}{4}}\right)\left(X - e^{i\frac{5\pi}{4}}\right)\left(X - e^{i\frac{7\pi}{4}}\right).$$

Exercice 3.19 *Factoriser en produit de polynômes irréductibles dans $\mathbb{C}[X]$, les polynômes*

$$P = X^4 + X^2 + 1 \; , \; R = X^5 - 1 \; , \; Q = X^5 + 1 \; , \; S = X^6 + 1 \; \textit{et} \; T = X^6 - 1.$$

Étant donné que les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réel (c'est-à-dire de discriminant strictement négatif), alors

Proposition 3.8 — Factorisation dans $\mathbb{R}[X]$. Tout polynôme $P \in \mathbb{R}[X]$ de degré n et de coefficient dominant c_n s'écrit sous la forme

$$P = c_n \prod_{i=1}^{p} (X - \alpha_i)^{k_i} \prod_{j=1}^{q} (X^2 + \beta_j X + \gamma_j)^{s_j}.$$

où
- α_i les racines réelles de P d'ordre de multiplicité k_i,
- $X^2 + \beta_j X + \gamma_j$ des polynômes de $\mathbb{R}[X]$ de discriminant strictement négatif,
- s_j sont des entiers naturels.

Remarque En calculant le produit des termes à racines conjuguées dans la factorisation de P dans $\mathbb{C}[X]$, on obtient une factorisation de P dans $\mathbb{R}[X]$. Par exemple, $P = X^4 + 1$ s'écrit dans $\mathbb{C}[X]$:

$$P = \left(X - e^{i\frac{\pi}{4}}\right)\left(X - e^{i\frac{7\pi}{4}}\right)\left(X - e^{i\frac{3\pi}{4}}\right)\left(X - e^{i\frac{5\pi}{4}}\right).$$

En calculant le produit des termes à racines conjuguées, on obtient la factorisation de P dans $\mathbb{R}[X]$:

$$P = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

Exercice 3.20 *Factoriser dans* $\mathbb{R}[X]$ *les polynômes suivants*

$$P = X^4 + X^2 - 6\,,\quad Q = X^4 - 2X^2 + 9\,,\quad S = X^6 + 9X^3 + 8\,,\quad \textit{et}\quad T = X^8 + X^4 + 1\,.$$

Exercice 3.21 *Factoriser dans* $\mathbb{C}[X]$, *puis dans* $\mathbb{R}[X]$ *:* $P = (X^2 - 4X + 1)^2 - (3X - 5)^2$.