Anneaux, Corps, Polynômes

Table des matières

1 Anneau, corps

1.1 Anneau

Définition 1.1

Soit $(A,+)$ un groupe commutatif (d'élément neutre 0_A) et $\times$ une loi de composition interne sur A. On dit que $(A,+,\times)$ est un *anneau* lorsque
- $\times$ est associatif,
- $\times$ admet un élément neutre 1_A,
- $\times$ est distributive par rapport à $+$

$$\forall a,b,c\in A,\qquad \begin{aligned} a\times(b+c)&=a\times b+a\times c,\\ (a+b)\times c&=a\times c+b\times c.\end{aligned}$$

Un élément $a\in A$ est dit *inversible* lorsqu'il est inversible pour la loi $\times$. Un anneau $(A,+,\times)$ est dit *commutatif* lorsque $\times$ est commutative.

Remarque

⇨ Si $a,b\in A$, on dit que a et b *commutent* lorsque $a\times b=b\times a$.

Exemples

⇨ $(\mathbb{C},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{Z},+,\times)$ sont des anneaux commutatifs.

⇨ Si $(A,+,\times)$ est un anneau et X est un ensemble, l'ensemble $\mathcal{F}(X,A)$ des fonctions de X dans A, muni des lois $+$ et $\times$ définies par

$$\forall f,g\in\mathcal{F}(X,A),\quad \forall x\in X,\quad \begin{aligned}(f+g)(x)&\coloneqq f(x)+g(x),\\ (f\times g)(x)&\coloneqq f(x)\times g(x)\end{aligned}$$

est un anneau dont l'élément neutre pour l'addition est la fonction $x\mapsto 0_A$ et l'élément neutre pour la multiplication est $x\mapsto 1_A$. Si A est commutatif, alors $\mathcal{F}(X,A)$ l'est aussi. En particulier, $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\times)$ et $(\mathbb{R}^{\mathbb{N}},+,\times)$ sont des anneaux commutatifs.

⇨ Si $n\in\mathbb{N}$, alors $(\mathcal{M}_n(\mathbb{R}),+,\times)$ est un anneau dont l'élément neutre pour la multiplication est la matrice I_n. Il est non commutatif dès que $n\geqslant 2$. Les éléments inversibles de $\mathcal{M}_n(\mathbb{R})$ sont les matrices inversibles.

⇨ Si E est un $\mathbb{K}$-espace vectoriel, alors $(\mathcal{L}(E),+,\circ)$ est un anneau dont l'élément neutre est Id. En général, il n'est pas commutatif. Les éléments inversibles de $\mathcal{L}(E)$ sont les isomorphismes.

⇨ Soit $\mathbb{F}_2$ l'ensemble à deux éléments $\{\bar{0}, \bar{1}\}$. On définit sur $\mathbb{F}_2$ les lois $+$ et $\times$ par

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Alors $(\mathbb{F}_2, +, \times)$ est un anneau commutatif.

Proposition 1.2

Soit $(A, +, \times)$ un anneau. Alors

$$\begin{aligned} \forall a \in A, \quad & 0_A \times a = 0_A \quad \text{et} \quad a \times 0_A = 0_A \\ \forall a, b \in A, \quad & a \times (-b) = (-a) \times b = -(a \times b) \\ \forall a, b \in A, \quad \forall n \in \mathbb{Z}, \quad & (n \cdot a) \times b = a \times (n \cdot b) = n \cdot (a \times b). \end{aligned}$$

Remarque

⇨ Soit $(A, +, \times)$ un anneau dans lequel $0_A = 1_A$. Alors $A = \{0_A\}$. Réciproquement, si A est un ensemble contenant un unique élément muni des seules lois de composition interne $+$ et $\times$ que l'on peut définir sur cet ensemble, alors $A = \{0_A\}$ et $(A, +, \times)$ est un anneau. On dit que cet anneau est l'anneau *trivial*.

Proposition 1.3

Soit $(A, +, \times)$ un anneau et $a, b \in A$ tels que $a \times b = b \times a$. Alors, pour tout $n \in \mathbb{N}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot \left(a^{n-k} \times b^k\right) \qquad \text{et} \qquad a^n - b^n = (a-b) \times \left[\sum_{k=0}^{n-1} a^{(n-1)-k} \times b^k\right].$$

Remarques

⇨ Ces relations peuvent être fausses lorsque a et b ne commutent pas. Par exemple, si a et b sont deux éléments d'un anneau, alors

$$(a+b)^2 = a^2 + 2 \cdot a \times b + b^2 \quad \Longleftrightarrow \quad a \times b = b \times a.$$

⇨ Remarquons que si $a \in A$, alors a commute avec 1_A, donc ces formules sont valables pour développer $(1_A + a)^n$ et factoriser $a^n - 1_A$.

Définition 1.4

On dit qu'un élément $a \in A$ est nilpotent lorsqu'il existe $n \in \mathbb{N}$ tel que $a^n = 0_A$.

Exercice 1

⇨ Montrer que si x est nilpotent, alors $1_A - x$ est inversible.

Définition 1.5

Soit $(A, +, \times)$ un anneau. L'ensemble U_A des éléments inversibles de A est un groupe pour la multiplication.

Remarque

⇨ L'ensemble U_A des inversibles de A est parfois noté $A^\times$. Il est important de ne pas confondre cet ensemble avec $A^* := A \setminus \{0_A\}$.

Exemples

⇨ Le groupe des inversibles de $\mathbb{Z}$ est $(\{-1, 1\}, \times)$.

⇨ Le groupe des inversibles de $\mathcal{M}_n(\mathbb{R})$ est $(\mathrm{GL}_n(\mathbb{R}), \times)$. Le groupe des inversibles de $\mathcal{L}(E)$ est $(\mathrm{GL}(E), \circ)$.

Définition 1.6

On dit qu'un anneau $(A, +, \times)$ est *intègre* lorsque
- $1_A \neq 0_A$
- $\times$ est commutative
- $\forall a, b \in A, \quad a \times b = 0_A \Longrightarrow [a = 0_A \quad \text{ou} \quad b = 0_A]$.

Remarque

⇨ Si $(A, +, \times)$ est intègre, tout élément non nul $a \in A^*$ est régulier pour $\times$:

$$\forall b, c \in A, \quad a \times b = a \times c \quad \Longrightarrow \quad b = c.$$

Exercice 2

⇨ L'anneau $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\times)$ est-il intègre ?

Dans la suite, lorsqu'il n'y a pas de confusion possible, les éléments 0_A et 1_A seront le plus souvent notés 0 et 1.

Définition 1.7

Soit $(A,+,\times)$ un anneau et B une partie de A. On dit que B est un *sous-anneau* de A lorsque
- $0 \in B$ et $1 \in B$
- $\forall b_1, b_2 \in B, \quad b_1 + b_2 \in B, \quad -b_1 \in B$ et $b_1 \times b_2 \in B$.

Si tel est le cas, $(B,+,\times)$ est un anneau.

Remarques

⇨ Si B est un sous-anneau de $(A,+,\times)$, B est un sous-groupe de $(A,+)$.

⇨ Si B est un sous-anneau de $\mathbb{C}$, alors $\mathbb{Z} \subset B$.

Exercice 3

⇨ Montrer que $\mathbb{Z}[\mathrm{i}] \coloneqq \{a + \mathrm{i}b : a,b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$.

Définition 1.8

Soit $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. On dit qu'une application φ de A dans B est un *morphisme d'anneau* lorsque

$$\begin{aligned} &\forall a_1, a_2 \in A, \quad && \varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \\ &\forall a_1, a_2 \in A, \quad && \varphi(a_1 \times a_2) = \varphi(a_1) \times \varphi(a_2) \\ & && \varphi(1_A) = 1_B. \end{aligned}$$

Proposition 1.9

Soit φ un morphisme d'anneau de $(A,+,\times)$ dans $(B,+,\times)$. Alors

$$\begin{aligned} &\forall a \in A, \quad \forall n \in \mathbb{Z}, \quad && \varphi(n \cdot a) = n \cdot \varphi(a) \\ &\forall a \in A, \quad \forall n \in \mathbb{N}, \quad && \varphi(a^n) = [\varphi(a)]^n. \end{aligned}$$

De plus, si $a \in A$ est inversible, il en est de même pour $\varphi(a)$ et

$$\forall n \in \mathbb{Z}, \quad \varphi(a^n) = [\varphi(a)]^n.$$

Proposition 1.10

- La composée de deux morphismes d'anneaux est un morphisme d'anneau.
- La bijection réciproque d'un isomorphisme est un isomorphisme.

Proposition 1.11

Soit φ un isomorphisme de l'anneau $(A,+,\times)$ dans l'anneau $(B,+,\times)$. Alors

$$\forall x \in A, \quad x \in U_A \iff \varphi(x) \in U_B.$$

De plus φ induit un isomorphisme du groupe $(U_A,\times)$ dans le groupe $(U_B,\times)$.

Définition 1.12

On dit qu'une partie $\mathcal{I}$ d'un anneau commutatif $(A,+,\times)$ est un *idéal* de A lorsque
- $0 \in \mathcal{I}$
- $\forall x, y \in \mathcal{I}, \quad \forall a, b \in A, \quad ax + by \in \mathcal{I}$

Proposition 1.13

Soit $(A,+,\times)$ un anneau commutatif et $x \in A$. Alors

$$xA \coloneqq \{ax : a \in A\}$$

est un idéal de A. Un tel idéal est appelé idéal *principal*.

Remarque

⇨ Soit $\mathcal{I}$ un idéal de $\mathbb{Z}$. Alors, il existe un unique $n \in \mathbb{N}$ tel que $\mathcal{I} = n\mathbb{Z}$. Dans $\mathbb{Z}$, tout idéal est donc principal.

1.2 Corps

Définition 1.14

On dit qu'un anneau $(\mathbb{K}, +, \times)$ est un *corps* lorsque
- $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$
- $\times$ est commutative
- Tout élément non nul de $\mathbb{K}$ admet un inverse pour la loi $\times$.

Exemples

⇨ Muni des lois usuelles d'addition et de multiplication, $\mathbb{C}$ est un corps.

⇨ $(\mathbb{F}_2, +, \times)$ est un corps.

Remarque

⇨ Si $\mathbb{K}$ est un corps, l'ensemble des inversibles de $\mathbb{K}$ est $\mathbb{K}^* := \mathbb{K} \setminus \{0_{\mathbb{K}}\}$. Autrement dit, $\mathbb{K}^\times = \mathbb{K}^*$.

Proposition 1.15

Un corps est intègre.

Exercice 4

⇨ Résoudre l'équation $x^2 = 1$ sur le corps $\mathbb{K}$.

Définition 1.16

Soit $(\mathbb{L}, +, \times)$ un corps et $\mathbb{K}$ une partie de $\mathbb{L}$. On dit que $\mathbb{K}$ est un *sous-corps* de $\mathbb{L}$ lorsque
- $\mathbb{K}$ est un sous-anneau de $\mathbb{L}$
- $\forall x \in \mathbb{K} \setminus \{0\}, \quad x^{-1} \in \mathbb{K}$.

Si tel est le cas, $(\mathbb{K}, +, \times)$ est un corps.

Remarque

⇨ $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-corps de $\mathbb{C}$.

⇨ Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, alors $\mathbb{Q} \subset \mathbb{K}$.

Définition 1.17

Si $(\mathbb{K}, +, \times)$ et $(\mathbb{L}, +, \times)$ sont deux corps, on appelle morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$ tout morphisme d'anneau pour les structures sous-jacentes.

Remarques

⇨ Si φ est un morphisme d'un sous-corps $\mathbb{K}$ de $\mathbb{C}$ dans un sous-corps $\mathbb{L}$ de $\mathbb{C}$, alors

$$\forall r \in \mathbb{Q}, \quad \forall x \in \mathbb{K}, \quad \varphi(rx) = r\varphi(x).$$

⇨ Si φ est un morphisme de corps, alors φ est injective.

Exercice 5

⇨ Déterminer les morphismes de corps φ de $\mathbb{C}$ dans $\mathbb{C}$ tels que : $\forall x \in \mathbb{R}, \quad \varphi(x) = x$.

Définition 1.18

Soit $\mathbb{K}$ un corps. Alors, l'application

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & \mathbb{K} \\ & k & \longmapsto & k \cdot 1_{\mathbb{K}} \end{array}$$

est un morphisme du groupe $(\mathbb{Z}, +)$ dans $(\mathbb{K}, +)$. Il existe donc un unique $p \in \mathbb{N}$ tel que $\operatorname{Ker} \varphi = p\mathbb{Z}$. L'entier p est soit nul soit un nombre premier et est appelé *caractéristique* de $\mathbb{K}$.

Remarques

⇨ Les sous-corps de $\mathbb{C}$ sont de caractéristique nulle. Le corps $\mathbb{F}_2$ est de caractéristique 2.

⇨ Lorsque $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, pour tout $k \in \mathbb{Z}$, on a $k \cdot 1_{\mathbb{K}} = k$. Si $\mathbb{K}$ est un corps quelconque, on confondra le plus souvent $k \cdot 1_{\mathbb{K}}$ et k.

2 Espace vectoriel, algèbre

2.1 Espace vectoriel

Définition 2.1

Soit $\mathbb{K}$ un corps, $(E, +)$ un groupe commutatif d'élément neutre 0_E et $\cdot$ une loi de composition externe.

$$\begin{array}{rccc} \cdot : & \mathbb{K} \times E & \longrightarrow & E \\ & (\lambda, x) & \longmapsto & \lambda \cdot x \end{array}$$

On dit que $(E, +, \cdot)$ est un $\mathbb{K}$-*espace vectoriel* lorsque

$$\begin{array}{lll} \forall x, y \in E, & \forall \lambda \in \mathbb{K}, & \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y \\ \forall x \in E, & \forall \lambda, \mu \in \mathbb{K}, & (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x \\ \forall x \in E, & \forall \lambda, \mu \in \mathbb{K}, & \lambda \cdot (\mu \cdot x) = (\lambda \mu) \cdot x \\ & \forall x \in E, & 1 \cdot x = x. \end{array}$$

Les éléments de $\mathbb{K}$ sont appelés *scalaires*, ceux de E, *vecteurs*.

Remarque

⇨ L'ensemble du cours sur les espaces vectoriels reste valide pour un corps quelconque, excepté le paragraphe sur les symétries qui n'est vrai que pour les corps de caractéristique différente de 2.

Proposition 2.2

Soit $(E, +, \cdot)$ un $\mathbb{L}$-espace vectoriel et $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Alors $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel. En particulier $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.

Remarques

⇨ $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel.

⇨ Muni des lois usuelles, $\mathcal{F}(\mathbb{R}, \mathbb{C})$ est un $\mathbb{C}$-espace vectoriel. Comme $\mathbb{R}$ est un sous-corps de $\mathbb{C}$, $\mathcal{F}(\mathbb{R}, \mathbb{C})$ est aussi un $\mathbb{R}$-espace vectoriel.

2.2 Algèbre

Définition 2.3

On dit qu'un anneau $(A, +, \times)$ muni d'une loi de composition externe $\cdot$ sur un corps $\mathbb{K}$ est une $\mathbb{K}$-algèbre lorsque
- $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel
- $\times$ est compatible avec la loi de composition externe

$$\forall x, y \in A, \quad \forall \lambda \in \mathbb{K}, \quad (\lambda \cdot x) \times y = x \times (\lambda \cdot y) = \lambda \cdot (x \times y)$$

On dit que l'algèbre $(A, +, \cdot, \times)$ est commutative lorsque $\times$ est commutatif.

Exemples

⇨ $\mathbb{K}$ est une $\mathbb{K}$-algèbre.

⇨ Soit X un ensemble. Alors $(\mathcal{F}(X, \mathbb{K}), +, \cdot, \times)$ est une $\mathbb{K}$-algèbre commutative. En particulier, l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ est une $\mathbb{R}$-algèbre commutative et l'ensemble des suites réelles est une $\mathbb{R}$-algèbre commutative.

Définition 2.4

Soit $(A, +, \cdot, \times)$ une $\mathbb{K}$-algèbre et B une partie de A. On dit que B est une *sous-algèbre* de A lorsque
- $0 \in B$ et $1 \in B$
- $\forall x, y \in B, \quad \forall \lambda, \mu \in \mathbb{K}, \quad \lambda x + \mu y \in B$
- $\forall x, y \in B, \quad x \times y \in B$

Si tel est le cas, $(B, +, \cdot, \times)$ est une $\mathbb{K}$-algèbre.

Remarque

⇨ Une sous-algèbre n'est rien d'autre qu'un sous-espace vectoriel qui est aussi un sous-anneau.

Définition 2.5

Soit $(A,+,\cdot,\times)$ et $(B,+,\cdot,\times)$ deux $\mathbb{K}$-algèbre. On dit qu'une application φ de A dans B est un morphisme d'algèbre lorsque c'est un morphisme d'anneau et une application linéaire, c'est-à-dire lorsque

$$\begin{aligned} \forall x,y\in A,\quad \forall \lambda,\mu\in\mathbb{K},\quad & \varphi\left(\lambda x+\mu y\right)=\lambda\varphi(x)+\mu\varphi(y)\\ \forall x,y\in A,\quad & \varphi\left(xy\right)=\varphi(x)\varphi(y)\\ & \varphi(1_A)=1_B. \end{aligned}$$

Proposition 2.6

Soit E un $\mathbb{K}$-espace vectoriel. Alors $\left(\mathcal{L}\left(E\right),+,\cdot,\circ\right)$ est une $\mathbb{K}$-algèbre.

Proposition 2.7

Soit $\mathbb{K}$ un corps et $n\in\mathbb{N}$. Alors $\left(\mathcal{M}_n\left(\mathbb{K}\right),+,\cdot,\times\right)$ est une $\mathbb{K}$-algèbre.

3 L'algèbre $\mathbb{K}[X]$

3.1 Définition

Définition 3.1

Soit $\mathbb{K}$ un corps. Alors il existe une unique algèbre commutative $\mathbb{K}[X]$ ainsi qu'un élément $X\in\mathbb{K}[X]$, appelé *indéterminée*, tels que

— Pour tout $P\in\mathbb{K}[X]$, il existe $n\in\mathbb{N}$ et $a_0,\dots,a_n\in\mathbb{K}$ tels que

$$P=a_0+a_1X+\cdots+a_nX^n$$

où, par abus de notation, $a_0=a_0\cdot 1_{\mathbb{K}[X]}=a_0X^0$.

— Pour tout $n\in\mathbb{N}$ et $a_0,\dots,a_n\in\mathbb{K}$

$$a_0+a_1X+\cdots+a_nX^n=0\quad\Longrightarrow\quad a_0=\cdots=a_n=0.$$

On l'appelle *algèbre des polynômes à coefficients dans* $\mathbb{K}$.

Remarque

⇨ Soit $P\in\mathbb{K}[X]$ et $a_0,\dots,a_n\in\mathbb{K}$ tels que $P=a_0+a_1X+\cdots+a_nX^n$. Il est d'usage de définir a_k pour tout $k>n$ en posant $a_k\coloneqq 0$. Alors, quel que soit $q\geqslant n$

$$P=\sum_{k=0}^{q}a_kX^k.$$

D'autre part, si $b_0,\dots,b_m\in\mathbb{K}$ sont tels que $P=b_0+b_1X+\cdots+b_mX^m$, en définissant $b_k\coloneqq 0$ pour tout $k>m$, on a

$$\forall k\in\mathbb{N},\quad a_k=b_k.$$

Aurement dit, la suite (a_k) est unique ; on l'appelle famille des *coefficients de* P.

Proposition 3.2: Produit de Cauchy

Soit $P,Q\in\mathbb{K}[X]$ deux polynômes dont les coefficients sont respectivement (a_k) et (b_k). Alors, si on note (c_k) la famille des coefficients du produit PQ, on a

$$\forall k\in\mathbb{N},\quad c_k=\sum_{l=0}^{k}a_{k-l}b_l.$$

Remarque

⇨ On a donc

$$\left(\sum_{k=0}^{n} a_k X^k\right)\left(\sum_{k=0}^{m} b_k X^k\right) = \sum_{k=0}^{n+m}\left(\sum_{l=0}^{k} a_{k-l} b_l\right) X^k$$

si on utilise la convention $a_k \coloneqq 0$ pour $k > n$ et $b_k \coloneqq 0$ pour $k > m$.

Exercice 6

⇨ Soit $n \in \mathbb{N}$. Montrer que

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

en calculant $(1+X)^{2n}$ de deux manières différentes.

3.2 Substitution

Définition 3.3

Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre, $x \in \mathcal{A}$ et $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$. On définit $P(x)$ par

$$P(x) \coloneqq a_0 1_{\mathcal{A}} + a_1 x + \cdots + a_n x^n \in \mathcal{A}.$$

On dit que l'on a substitué l'élément $x \in \mathcal{A}$ à l'indéterminée X.

Remarques

⇨ Si $\mathcal{A}$ une $\mathbb{K}$-algèbre et $x \in \mathcal{A}$, l'application φ de $\mathbb{K}[X]$ dans $\mathcal{A}$ qui à P associe $P(x)$ est un morphisme d'algèbre. Autrement dit

$$\begin{aligned} \forall P, Q \in \mathbb{K}[X], \quad \forall \lambda, \mu \in \mathbb{K}, \qquad & (\lambda P + \mu Q)(x) = \lambda P(x) + \mu Q(x) \\ \forall P, Q \in \mathbb{K}[X], \qquad & (PQ)(x) = P(x)Q(x) \\ & 1_{\mathbb{K}[X]}(x) = 1_{\mathcal{A}}. \end{aligned}$$

⇨ On dit qu'un polynôme P est un polynôme annulateur de $x \in \mathcal{A}$ lorsque $P(x) = 0$. Par exemple, si $\mathbb{K} = \mathbb{R}$ et $\mathcal{A} = \mathbb{C}$, $P \coloneqq X^2 + 1$ est un polynôme annulateur de i. Si E est un $\mathbb{K}$-espace vectoriel et si $s \in \mathcal{L}(E)$ est une symétrie, alors $P \coloneqq X^2 - 1$ est un polynôme annulateur de s.

⇨ On dit qu'un élément $z \in \mathbb{C}$ est algébrique lorsqu'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(z) = 0$. Par exemple $z_1 = \left(1+\sqrt{5}\right)/2$ est algébrique car $P_1 \coloneqq X^2 - X - 1 \in \mathbb{Q}[X]$ est un polynôme annulateur de z_1. De même, j est algébrique car $P_2 \coloneqq X^3 - 1 \in \mathbb{Q}[X]$ est un polynôme annulateur de j. Lorsqu'on effectue des calculs avec un nombre algébrique z, il est souvent plus économe en calculs d'exploiter le fait que $P(z) = 0$ plutôt que de remplacer z par une expression parfois complexe. Par exemple, si $x \coloneqq \left(1+\sqrt{5}\right)/2$, en exploitant le fait que $x^2 = x + 1$, on a

$$\left(\frac{1+\sqrt{5}}{2}\right)^3 = x^3 = x \cdot x^2 = x(x+1) = x^2 + x = 2x + 1 = 2 + \sqrt{5}$$

Si on souhaite calculer $1/x$, on exploite le fait que $x^2 - x - 1 = 0$, ce qui donne $x(x-1) = 1$, puis $1/x = x - 1$. Donc

$$\frac{1}{\left(\frac{1+\sqrt{5}}{2}\right)} = \frac{-1+\sqrt{5}}{2}.$$

⇨ On dit qu'un élément de $\mathbb{C}$ est *transcendant* lorsqu'il n'est pas algébrique. On peut montrer, mais c'est difficile, que e et π sont transcendants.

Exercice 7

⇨ Montrer que $1 + \sqrt{7}$ et $\sqrt{2} + \sqrt{5}$ sont algébriques.

⇨ Soit $D \coloneqq \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) \in \mathcal{M}_n(\mathbb{K})$ et $P \in \mathbb{K}[X]$. Montrer que $P(D) = \mathrm{Diag}(P(\lambda_1), \ldots, P(\lambda_n))$.

Définition 3.4

Soit $P, Q \in \mathbb{K}[X]$. On définit le polynôme $P \circ Q$ par

$$P \circ Q \coloneqq P(Q).$$

Remarque

⇨ Si $P \in \mathbb{K}[X]$, $P(X) = P$. Un polynôme peut donc indifféremment être noté P ou $P(X)$.

Définition 3.5

Soit $P \in \mathbb{K}[X]$. On dit que
- P est *pair* lorsque $P(-X) = P(X)$.
- P est *impair* lorsque $P(-X) = -P(X)$.

Proposition 3.6

Soit $\mathbb{K}$ un corps qui n'est pas de caractéristique 2 et $P \in \mathbb{K}[X]$. Alors
- P est pair si et seulement si ses coefficients d'indices impairs sont nuls.
- P est impair si et seulement si ses coefficients d'indices pairs sont nuls.

3.3 Degré d'un polynôme

Définition 3.7

Soit $P \in \mathbb{K}[X]$. On définit le *degré* de P que l'on note $\deg P$ par
- Si $P = 0$, on pose $\deg P := -\infty$.
- Sinon, il existe $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$ tels que

$$P = a_0 + a_1 X + \cdots + a_n X^n \quad \text{et} \quad a_n \neq 0.$$

De plus n et les $a_0, \dots, a_n$ sont uniques ; on pose alors $\deg P := n$. Le coefficient a_n est appelé *coefficient dominant* de P.

Remarques

⇨ Si $P \in \mathbb{K}[X]$ est non nul, son coefficient dominant est parfois noté $\mathrm{cd}(P)$.

⇨ Un polynôme $P \in \mathbb{K}[X]$ est de degré inférieur ou égal à $n \in \mathbb{N}$ si et seulement si il existe $a_0, \dots, a_n \in \mathbb{K}$ tels que

$$P = \sum_{k=0}^{n} a_k X^k.$$

⇨ On dit qu'un polynôme P est constant lorsqu'il existe $\lambda \in \mathbb{K}$ tel que $P = \lambda$, c'est-à-dire lorsque son degré est inférieur ou égal à 0.

Proposition 3.8

Soit $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.
- Soit $\lambda, \mu \in \mathbb{K}$. Si $\deg P \leqslant n$ et $\deg Q \leqslant n$, alors

$$\deg(\lambda P + \mu Q) \leqslant n.$$

- Soit $\lambda \in \mathbb{K}^*$ et $\mu \in \mathbb{K}$. Si $\deg P = n$ et $\deg Q < n$, alors

$$\deg(\lambda P + \mu Q) = n \qquad \text{et} \qquad \mathrm{cd}(\lambda P + \mu Q) = \lambda \mathrm{cd}(P).$$

Remarque

⇨ Lorsque P et Q sont des polynômes de degré n, il est possible que $P + Q$ soit de degré strictement inférieur à n. Par exemple $P := X + 1$ et $Q := -X$ sont de degré 1 mais $P + Q = 1$ est de degré 0.

Exercice 8

⇨ Soit $P \in \mathbb{C}[X]$. Calculer le degré de $P(X + 1) - P(X)$ en fonction de celui de P.

Définition 3.9

Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X]$ l'espace vectoriel des polynômes de degré inférieur ou égal à n.

Remarque

⇨ Si $n \geqslant 1$, $\mathbb{K}_n[X]$ n'est pas stable par produit. En effet, $X^n \in \mathbb{K}_n[X]$ mais $X^{2n} = X^n \cdot X^n \notin \mathbb{K}_n[X]$.

Proposition 3.10

Soit $P, Q \in \mathbb{K}[X]$. Alors

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

De plus, si P et Q sont non nuls, alors $\mathrm{cd}(PQ) = \mathrm{cd}(P)\mathrm{cd}(Q)$.

Remarques

⇨ Si $P \in \mathbb{K}[X]$ est non nul et si $n \in \mathbb{N}$, alors $\deg(P^n) = n \deg P$.

⇨ Si $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ n'est pas constant, alors $\deg(P \circ Q) = \deg(P)\deg(Q)$.

Proposition 3.11

$\mathbb{K}[X]$ est une algèbre intègre

$$\forall P, Q \in \mathbb{K}[X], \quad PQ = 0 \quad \Longrightarrow \quad [P = 0 \quad \text{ou} \quad Q = 0].$$

Proposition 3.12

Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0, c'est-à-dire les polynômes constants non nuls.

Définition 3.13

On dit qu'un polynôme non nul U est unitaire lorsque son coefficient dominant est égal à 1. Tout polynôme P non nul s'écrit de manière unique sous la forme $P = \lambda P_u$ où $\lambda \in \mathbb{K}^*$ et P_u est unitaire. Lorsque $P = 0$, on pose par convention $P_u := 0$.

Définition 3.14: Division euclidienne

Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

$$A = QB + R \quad \text{et} \quad \deg R < \deg B.$$

Q est appelé *quotient* de la division euclidienne de A par B, R son *reste*.

Remarques

⇨ Si B est un polynôme annulateur non nul de x et $A \in \mathbb{K}[X]$. Alors $A(x) = R(x)$ où R est le reste de la division euclidienne de A par B. En effet

$$A(x) = Q(x)\underbrace{B(x)}_{=0} + R(x)$$

⇨ Il est parfois utile de calculer le reste de la division euclidienne de A par B sans calculer son quotient. Par exemple, si $A := X^n$ et $B := (X-1)(X-2)$, le reste R de la division euclidienne de A par B est de degré inférieur ou égal à 1 donc il existe $a, b \in \mathbb{R}$ tels que $R = aX + b$. Comme $A = QB + R$, on en déduit que $A(1) = Q(1)B(1) + R(1)$. Comme $B(1) = 0$, on a $A(1) = R(1)$. De même $A(2) = R(2)$. Donc

$$\begin{cases} a + b = 1 \\ 2a + b = 2^n. \end{cases}$$

On en déduit que $a = 2^n - 1$ et $b = 2 - 2^n$. Donc $R = (2^n - 1)X + (2 - 2^n)$. Cette méthode fonctionne dès que le polynôme B, de degré n, admet n racines deux à deux distinctes.

Exercices 9

⇨ Calculer $x^5 + x^4 - 1$ où $x := (1 + \sqrt{5})/2$.

⇨ On pose

$$A := \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix}$$

Vérifier que $A^2 - 5A + 6I_2 = 0$ puis calculer A^n pour tout $n \in \mathbb{N}$.

Proposition 3.15

Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$. Alors, il existe un unique polynôme unitaire ou nul P tel que $\mathcal{I} = P\mathbb{K}[X]$.

Remarque

⇨ En particulier, dans $\mathbb{K}[X]$, tout idéal est principal.

3.4 Racines, fonctions polynôme

Définition 3.16

Soit $P \in \mathbb{K}[X]$. On appelle racine de P tout élément $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.

Remarques

- Les polynômes de degré 1 admettent une unique racine.
- D'après le théorème des valeurs intermédiaires, tout polynôme réel de degré impair admet (au moins) une racine réelle.
- La notion de racine dépend du corps considéré. En effet, si on le considère comme élément de $\mathbb{C}[X]$, les racines de $(X^2-2)(X^2+1)$ sont $\sqrt{2}, -\sqrt{2}, \mathrm{i}, -\mathrm{i}$. Considéré comme élément de $\mathbb{R}[X]$, ses racines sont $\sqrt{2}, -\sqrt{2}$. Enfin il n'a aucune racine si on le considère comme un élément de $\mathbb{Q}[X]$.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{L}$, on dit que α est une racine de P sur $\mathbb{L}$ lorsque $P(\alpha) = 0$.
- Si $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$ est une racine de P, alors $\overline{\alpha}$ est une racine de P. Les racines de P sont donc soit réelles, soit conjuguées deux à deux.

Proposition 3.17

Soit $P \in \mathbb{K}[X]$. Si $\alpha \in \mathbb{K}$ est une racine de P, alors il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha)Q.$$

Remarque

- Cette factorisation se calcule en pratique en effectuant la division euclidienne de P par $X - \alpha$.

Proposition 3.18

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

Remarques

- On en déduit qu'un polynôme de degré inférieur ou égal à n admettant $n+1$ racines deux à deux distinctes est nul. De même, si deux polynômes de degrés inférieurs ou égaux à n prennent la même valeur en $n+1$ points deux à deux distincts, alors ils sont égaux.
- Un polynôme admettant une infinité de racines est donc nul. De même, deux polynômes prenant la même valeur sur un ensemble infini sont égaux.

Exercices 10

- Montrer que les polynômes de $\mathbb{C}[X]$ tels que $P(X) = P(X+1)$ sont les polynômes constants.
- Montrer qu'il n'existe pas de polynôme $P \in \mathbb{C}[X]$ tel que, pour tout $z \in \mathbb{C}$, $P(z) = \overline{z}$.

Proposition 3.19: Polynôme interpolateur de Lagrange

Soit $x_0, \dots, x_n \in \mathbb{K}$, $n+1$ éléments deux à deux distincts et $y_0, \dots, y_n \in \mathbb{K}$. Alors, il existe un unique polynôme P de degré inférieur ou égal à n tel que

$$\forall i \in [\![0, n]\!], \quad P(x_i) = y_i.$$

On l'appelle *polynôme interpolateur de Lagrange* associé aux familles $(x_0, \dots, x_n)$ et $(y_0, \dots, y_n)$.

Remarque

- Pour tout $i \in [\![0, n]\!]$, on note L_i le polynôme défini par

$$L_i := \prod_{\substack{k=0 \\ k \neq i}}^{n} \frac{X - x_k}{x_i - x_k}.$$

Les polynômes L_i sont appelés *polynômes de Lagrange* et vérifient : $\forall i, j \in [\![0, n]\!], \quad L_i(x_j) = \delta_{i,j}$. Le polynôme interpolateur de Lagrange associé aux familles $(x_0, \dots, x_n)$ et $(y_0, \dots, y_n)$ est donné par

$$P = \sum_{i=0}^{n} y_i L_i.$$

Définition 3.20

On dit qu'une application $f : \mathbb{K} \to \mathbb{K}$ est une fonction polynôme lorsqu'il existe $P \in \mathbb{K}[X]$ tel que

$$\forall x \in \mathbb{K}, \quad f(x) = P(x).$$

Proposition 3.21

Si $\mathbb{K}$ est infini, l'application de l'algèbre $\mathbb{K}[X]$ dans l'algèbre $\mathcal{F}(\mathbb{K}, \mathbb{K})$, qui au polynôme P associe la fonction polynôme $\tilde{P}$, est injective.

Remarques

➪ Cette proposition permet, lorsque $\mathbb{K}$ est infini, d'identifier polynômes et fonctions polynôme. C'est pourquoi de rares énoncés se permettent de les confondre, identification que nous ne ferons que lorsque l'énoncé le demande explicitement.

➪ Cette proposition est fausse lorsque le corps $\mathbb{K}$ est fini. En effet, si $\mathbb{K} = \{a_1, \dots, a_n\}$, le polynôme

$$P \coloneqq \prod_{k=1}^{n} (X - a_k)$$

est non nul car $\deg P = n$, mais la fonction polynôme associée est nulle.

3.5 Polynôme dérivé

Définition 3.22

Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$. On définit le polynôme dérivé de P par

$$\begin{aligned} P' &\coloneqq a_1 + 2a_2 X + \cdots + n a_n X^{n-1} \\ &= \sum_{k=1}^{n} k a_k X^{k-1}. \end{aligned}$$

Remarque

➪ Dans le cas où $\mathbb{K} = \mathbb{R}$, la fonction polynôme associée à P' est la dérivée (comme définie dans le cours d'analyse) de la fonction polynôme associée à P.

Proposition 3.23

Soit $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$. Alors

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q' \qquad (PQ)' = P'Q + PQ' \quad \text{et} \quad (P \circ Q)' = Q' \left(P' \circ Q\right).$$

Remarque

➪ On peut utiliser le polynôme dérivé pour calculer la reste de la division euclidienne de A par B lorsque B possède des racines multiples. Par exemple, si $A \coloneqq X^n$ et $B \coloneqq (X-1)^2$, le reste R de la division euclidienne de A par B est de degré inférieur ou égal à 1 donc il existe $a, b \in \mathbb{R}$ tels que $R = aX + b$. Comme plus haut, $A(1) = R(1)$. En dérivant la relation $A = QB + R$, on obtient $A' = B'Q + BQ' + R'$. Puisque 1 est racine de B et de B', on en déduit que $A'(1) = R'(1)$. Donc

$$\begin{cases} a + b = 1 \\ a \quad\;\; = n. \end{cases}$$

On en déduit que $a = n$ et $b = 1 - n$, donc $R = nX + (1 - n)$.

Définition 3.24

Soit $P \in \mathbb{K}[X]$. On définit par récurrence la dérivée n-ième de P par
- $P^{(0)} \coloneqq P$
- $\forall n \in \mathbb{N}, \quad P^{(n+1)} \coloneqq \left[P^{(n)}\right]'$.

Remarque

➪ Soit $n \in \mathbb{N}$. Alors

$$\forall k \in \mathbb{N}, \quad \left(X^n\right)^{(k)} = \begin{cases} \frac{n!}{(n-k)!} X^{n-k} & \text{si } k \leqslant n \\ 0 & \text{sinon.} \end{cases}$$

En particulier, si $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$, alors

$$\forall k \in \mathbb{N}, \quad P^{(k)}(0) = k! a_k.$$

Proposition 3.25

Soit $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$

— Soit $\lambda, \mu \in \mathbb{K}$. Alors

$$(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}.$$

— On a

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(n-k)} Q^{(k)}.$$

Cette formule est appelée formule de Leibniz.

Exercice 11

⇨ Calculer $(X^2 P)^{(n)}$ en fonction des dérivées successives de P.

Dans la suite du cours, on suppose que $\mathbb{K}$ est un corps de caractéristique nulle.

Proposition 3.26

Soit $P \in \mathbb{K}[X]$. Alors

$$\deg P' = \begin{cases} \deg(P) - 1 & \text{si } \deg P \geqslant 1, \\ -\infty & \text{sinon.} \end{cases}$$

Remarques

⇨ $P' = 0$ si et seulement si P est constant.

⇨ Pour tout $P \in \mathbb{K}[X]$, $\deg P' \leqslant \deg(P) - 1$.

⇨ Soit $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. Alors

$$\deg P^{(n)} = \begin{cases} \deg(P) - n & \text{si } \deg P \geqslant n, \\ -\infty & \text{sinon.} \end{cases}$$

En particulier, $\deg P^{(n)} \leqslant \deg(P) - n$.

Proposition 3.27: Formule de Taylor

Soit $P \in \mathbb{K}[X]$ un polynôme de degré inférieur ou égal à n et $\alpha \in \mathbb{K}$. Alors

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