

Chapitre 1

Structures algébriques usuelles

M. BINYZE

<https://supspé.com>

CPGE Laâyoune

Filière MP

2025-2026

Plan

- 1 Groupes
- 2 Anneaux
- 3 Idéal d'un anneau commutatif
- 4 Anneau des polynômes à une indéterminée
- 5 Algèbres

Plan

- 1 Groupes
- 2 Anneaux
- 3 Idéal d'un anneau commutatif
- 4 Anneau des polynômes à une indéterminée
- 5 Algèbres

Compléments sur les groupes

G désigne un groupe multiplicatif de neutre e .

Théorème 1.1 (sous-groupes de $(\mathbb{Z}, +)$).

Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Théorème 1.2 (groupe $(\mathbb{Z}/n\mathbb{Z}, +)$).

Soit $n \in \mathbb{N}^$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruences modulo n muni de la l.c.i. notée $+$ définie par :*

$$\forall \bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}, \quad \bar{a} + \bar{b} = \overline{a + b}$$

est un groupe abélien de neutre $n\mathbb{Z}$. De plus :

- 1** $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}, \quad -\bar{a} = \overline{-a}.$
- 2** $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}.$

Proposition 1.1 (intersection de sous-groupes).

Soit $(H_i)_{i \in I}$ une famille de sous-groupes de G . L'ensemble $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition 1.1 (groupe engendré par une partie).

Soit A une partie de G . On appelle **groupe engendré** par A l'ensemble, noté $\langle A \rangle$, défini par

$$\langle A \rangle \stackrel{\text{déf}}{=} \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H}} H.$$

Lorsque $G = \langle A \rangle$, on dit que G est **engendré** par A ou que A est une **partie génératrice** de G .

Théorème 1.3 (caractérisation du sous-groupe engendré par une partie).

Soit A une partie de G .

- 1 $\langle A \rangle$ est le plus petit sous-groupe (au sens de l'inclusion) de G contenant A .
- 2 Si $A = \emptyset$, alors $\langle A \rangle = \{e\}$.
- 3 Si $A \neq \emptyset$, alors

$$\langle A \rangle = \left\{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}, \quad n \in \mathbb{N}^*, \quad \forall i \in \llbracket 1, n \rrbracket, \quad \varepsilon_i \in \{-1, 1\}, \quad a_i \in A \right\}.$$



- 1 $n\mathbb{Z} = \langle n \rangle$.
- 2 $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ où $\bar{1}$ la classe de 1 modulo n .
- 3 Le groupe symétrique $(\mathcal{S}_n, \circ)$ est engendré par les transpositions.

Groupe monogène, groupe cyclique

Définition 1.2 (groupe monogène, groupe cyclique).

- 1 On dit que G est **monogène** lorsqu'il existe $a \in G$ tel que¹

$$G = \langle a \rangle = \{a^k, k \in \mathbb{Z}\}.$$

L'élément a est appelé un **générateur** du groupe G .

- 2 On dit que G est **cyclique** lorsqu'il est monogène et fini.

¹En notation additive, $\langle a \rangle = \{ka, k \in \mathbb{Z}\}$.



- 1 $n\mathbb{Z} = \langle n \rangle$, donc $(n\mathbb{Z}, +)$ est monogène.
- 2 $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$, donc $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.
- 3 $\mathbb{U}_n = \langle \omega_1 \rangle$ où $\omega_1 = e^{2i\pi/n}$, donc $(\mathbb{U}_n, \times)$ est cyclique.

Proposition 1.2 (générateurs de $\mathbb{Z}/n\mathbb{Z}$).

Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$, $k \in \llbracket 1, n \rrbracket$ avec $k \wedge n = 1$.

Théorème 1.4 (classification des groupes monogènes).

- 1 *Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.*
- 2 *Tout groupe monogène fini (cyclique) de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Ordre d'un élément dans un groupe

Soit G un groupe de neutre e .

Définition 1.3 (ordre d'un groupe, ordre d'un élément).

- 1 On dit que G est **d'ordre fini** si G est fini. On appelle alors **ordre** de G le cardinal de G .
- 2 On dit qu'un élément a de G est **d'ordre fini** s'il existe $n \in \mathbb{N}^*$ vérifiant $a^n = e$. le plus petit entier $n \in \mathbb{N}^*$ vérifiant $a^n = e$ est appelé **l'ordre** de a :

$$\text{l'ordre de } a = \min \left\{ k \in \mathbb{N}^*, a^k = e \right\}.$$



- 1 Le neutre e est l'unique élément d'ordre fini égal à 1.
- 2 Soit $a \in G \setminus \{e\}$. On a

$$a \text{ est d'ordre } n \iff \begin{cases} a^n = e \\ \forall k \in \llbracket 1, n-1 \rrbracket, a^k \neq e \end{cases}.$$



- 1 Dans $(\mathbb{Z}/6\mathbb{Z}, +)$, l'élément $\overline{4}$ est d'ordre 3.
- 2 Dans $(\mathcal{GL}_2(\mathbb{K}), \times)$, l'élément $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.
- 3 Dans $(\mathbb{C}^*, \times)$, l'élément $\omega_1 = e^{2i\pi/n}$ est d'ordre n .
- 4 Dans $(\mathcal{S}_n, \circ)$, toute transposition $\tau \in \mathcal{S}_n \setminus \{\text{Id}\}$ est d'ordre 2.

Proposition 1.3 (ordre d'un élément et ordre du sous-groupe engendré cet élément).

Soit $a \in G$.

- 1 a est d'ordre fini si, et seulement si, $\langle a \rangle$ est d'ordre fini.

Dans ce cas,

$$\langle a \rangle = \{e, a, \dots, a^{d-1}\}.$$

- 2 En particulier, l'ordre de a est l'ordre du sous-groupe engendré par a .

Corollaire 1.1 (éléments et générateurs d'un groupe cyclique).

Soit G un groupe cyclique d'ordre n de générateur a .

- 1 $G = \{e, a, a^2, \dots, a^{n-1}\}.$

- 2 Les générateurs de G sont les a^k , où $k \wedge n = 1$.

Proposition 1.4 (caractérisation de l'ordre d'un élément).

Soit $a \in G$. Alors

a est d'ordre n si, et seulement si, $\forall k \in \mathbb{Z}, a^k = e \iff n \mid k$.

Théorème 1.5 (ordre d'un élément divise l'ordre du groupe).

Soit G un groupe d'ordre fini $n \in \mathbb{N}^*$ et $a \in G$. Alors

- 1 a est d'ordre fini : $a^n = e$.
- 2 L'ordre de a divise n .

Plan

- 1 Groupes
- 2 Anneaux**
- 3 Idéal d'un anneau commutatif
- 4 Anneau des polynômes à une indéterminée
- 5 Algèbres

Théorème 2.1 (produit d'anneaux).

Soit $(A_i)_{1 \leq i \leq k}$ une famille d'anneaux. On définit les lois $+$ et $\times$ sur $A_1 \times \dots \times A_k$ en posant, pour tout $(a_1, \dots, a_k) \in A_1 \times \dots \times A_k$ et $(b_1, \dots, b_k) \in A_1 \times \dots \times A_k$:

$$\begin{cases} (a_1, \dots, a_k) + (b_1, \dots, b_k) &= (a_1 + b_1, \dots, a_k + b_k) \\ (a_1, \dots, a_k) \times (b_1, \dots, b_k) &= (a_1 \times b_1, \dots, a_k \times b_k) \end{cases}$$

Alors $(A_1 \times \dots \times A_k, +, \times)$ est un anneau, appelé **anneau produit**, d'élément neutre $(0_{A_1}, \dots, 0_{A_k})$ et d'élément unité $(1_{A_1}, \dots, 1_{A_k})$.

On note $\mathbb{U}(A)$ le groupe des éléments inversibles de l'anneau A .

Proposition 2.1 (les inversibles de l'anneau produit).

Si $A_1, \dots, A_k$ sont des anneaux, alors

$$\mathbb{U}(A_1 \times \dots \times A_k) = \mathbb{U}(A_1) \times \dots \times \mathbb{U}(A_k).$$

Définition 2.1 (éléments associés).

Soit x et y dans A . On dit que x et y sont **associés** si

$$\exists a \in \mathbb{U}(A), \quad x = ay.$$

Anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Théorème 2.2 (anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$).

Soit $n \in \mathbb{N}^*$. On muni $\mathbb{Z}/n\mathbb{Z}$ de deux l.c.i. notées $+$ et $\times$ définies par :

$$\forall \bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}, \quad \bar{a} + \bar{b} = \overline{a + b} \quad \text{et} \quad \bar{a} \times \bar{b} = \overline{a \times b}.$$

Alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif d'élément neutre $\bar{0}$ et d'élément unité $\bar{1}$.

Théorème 2.3 (les inversibles de $\mathbb{Z}/n\mathbb{Z}$).

Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ avec $k \wedge n = 1$.



Les inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont exactement les générateurs du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.

Théorème 2.4 (restes chinois).

Soient $n_1, \dots, n_r$ des entiers deux à deux premiers entre eux et n leur produit. L'application¹ :

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z} \\ \overline{x}^n &\longmapsto (\overline{x}^1, \dots, \overline{x}^r) \end{aligned}$$

est un isomorphisme d'anneaux.

¹où $\overline{x}^i$ est la classe de x modulo n_i

Corollaire 2.1 (système de congruences d'entiers).

Soient $n_1, \dots, n_r$ des entiers strictement positifs premiers entre eux deux à deux, et $a_1, \dots, a_r$ des entiers quelconques. Le système

$$(S) : \begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

admet une **unique solution modulo** $\prod_{i=1}^r n_i$.

Définition 2.2 (indicatrice d'Euler).

On appelle **fonction indicatrice d'Euler** l'application $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ définie par :

$$\varphi(n) = \text{Card} \left\{ k \in \llbracket 0, n-1 \rrbracket, k \wedge n = 1 \right\}.$$



Le nombre des inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est $\varphi(n)$.

Proposition 2.2 (multiplicativité de l'indicatrice d'Euler).

L'indicatrice d'Euler φ est multiplicative :

$$\forall p, q \in \mathbb{N}^*, \quad p \wedge q = 1 \implies \varphi(pq) = \varphi(p)\varphi(q).$$

Proposition 2.3 (calcul de $\varphi(n)$).

- 1 Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
- 2 Soit $n \geq 2$ et $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers.

$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Théorème 2.5 (théorème d'Euler et le petit théorème de Fermat).

- 1 Soit n un entier supérieur à 2 et k un entier premier avec n .

$$k^{\varphi(n)} \equiv 1 [n]. \quad (\text{théorème d'Euler})$$

- 2 Soit k un entier et p un nombre premier non diviseur de k .

$$k^{p-1} \equiv 1 [p]. \quad (\text{petit théorème de Fermat})$$

Proposition 2.4 (corps $(\mathbb{Z}/p\mathbb{Z}, +, \times)$).

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps si, et seulement si, p est un nombre premier.

Plan

- 1 Groupes
- 2 Anneaux
- 3 Idéal d'un anneau commutatif**
- 4 Anneau des polynômes à une indéterminée
- 5 Algèbres

Dans ce paragraphe, $(A, +, \times)$ désigne un anneau commutatif d'élément neutre 0_A et d'élément unité 1_A .

Définition 3.1 (idéal).

On appelle **idéal** de A toute partie I de A non vide vérifie :

$$\left\{ \begin{array}{l} \forall (x, y) \in I^2, \quad x + y \in I \\ \forall x \in I, \forall a \in A, \quad ax \in I \end{array} \right.$$



- 1 $\{0_A\}$ et A sont des idéaux de A .
- 2 L'ensemble $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Proposition 3.1 (caractérisation d'un idéal).

$$I \text{ est un idéal de } A \iff \begin{cases} (I, +) \text{ sous-groupe de } (A, +) \\ \forall x \in I, \forall a \in A, \quad ax \in I \end{cases}$$

Théorème 3.1 (idéaux de $(\mathbb{Z}, +, \times)$).

Les idéaux de $(\mathbb{Z}, +, \times)$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Proposition 3.2.

Soit $f : A \longrightarrow B$ un morphisme d'anneaux commutatifs et I un idéal de B . Alors $f^{-1}(I)$ est un idéal de A .

En particulier, $\ker(f)$ est un idéal de A .

Définition 3.2 (idéal engendré par un élément).

Soit $x \in A$. On appelle **idéal engendré par x** l'ensemble

$$xA \stackrel{\text{déf}}{=} \{xa, a \in A\}$$

des multiples de x .

Théorème 3.2 (caractérisation de xA).

Pour tout $x \in A$, on a :

$$xA = \bigcap_{\substack{J \text{ idéal de } A \\ x \in J}} J.$$

Ainsi xA est le plus petit idéal de A contenant x .

Définition 3.3 (divisibilité dans un anneau intègre).

Supposons A intègre¹ et soit $(a, b) \in A^2$.

On dit que a **divise** b , et on écrit $a \mid b$ si $\exists u \in A, b = au$.

¹L'intégrité de A assure que le u ci-dessus est unique si $a \neq 0$.

Proposition 3.3 (association et divisibilité en termes d'idéaux).

Supposons A intègre et soit $(a, b) \in A^2$.

$$1 \quad a \text{ divise } b \iff bA \subset aA.$$

$$2 \quad a \text{ et } b \text{ sont associés} \iff aA = bA.$$

Théorème 3.3 (somme d'idéaux).

Soient $I_1, \dots, I_k$ des idéaux de A . L'ensemble

$$I_1 + \dots + I_k \stackrel{\text{déf}}{=} \left\{ \sum_{i=1}^k x_i, x_i \in I_i, 1 \leq i \leq k \right\}$$

est un idéal de A qui contient chaque I_i et est inclus dans tout idéal contenant $I_1, \dots, I_k$.



Plus grand commun diviseur

Soit $(a_1, \dots, a_k) \in \mathbb{Z}^k$ non nuls.

- 1 Il existe $d \in \mathbb{N}^*$ **unique** tel que : $a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = d\mathbb{Z}$.
L'entier d est appelé le plus grand commun diviseur des a_i , $1 \leq i \leq k$. On note $d = \text{pgcd}(a_1, \dots, a_k)$.
- 2 d est caractérisé par :

$$\left\{ \begin{array}{l} \forall i \in \llbracket 1, k \rrbracket, \quad d \mid a_i \\ \text{et} \\ \forall c \in \mathbb{Z}, \quad (\forall i \in \llbracket 1, k \rrbracket, \quad c \mid a_i \implies c \mid d) \end{array} \right\}.$$



- 1 En effet : $a_1\mathbb{Z} + \dots + a_k\mathbb{Z}$ est un idéal de $\mathbb{Z}$ donc il existe $d \in \mathbb{N}^*$ tel que $a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = d\mathbb{Z}$. S'il existe $\delta \in \mathbb{N}^*$ tel que $a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = \delta\mathbb{Z}$ alors d et δ sont associés, par suite $d = \delta$ car $(d, \delta) \in (\mathbb{N}^*)^2$.
- 2 On a $\forall i \in \llbracket 1, k \rrbracket, a_i\mathbb{Z} \subset a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = d\mathbb{Z}$ donc $d \mid a_i$ pour tout $i \in \llbracket 1, k \rrbracket$. Soit $c \in \mathbb{Z}$ tel que $c \mid a_i$ pour tout $i \in \llbracket 1, k \rrbracket$. On a $\forall i \in \llbracket 1, k \rrbracket, a_i\mathbb{Z} \subset c\mathbb{Z}$ donc $d\mathbb{Z} = a_1\mathbb{Z} + \dots + a_k\mathbb{Z} \subset c\mathbb{Z}$ et $c \mid d$.
Réciproquement soit $\delta \in \mathbb{N}^*$ tel que $a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = \delta\mathbb{Z}$. On a d divise chaque a_i donc $\delta\mathbb{Z} = a_1\mathbb{Z} + \dots + a_k\mathbb{Z} \subset d\mathbb{Z}$ et par suite $\delta\mathbb{Z} \subset d\mathbb{Z}$. Or $\forall i \in \llbracket 1, k \rrbracket, \delta \mid a_i$ donc $\delta \mid d$ et par suite $d\mathbb{Z} \subset \delta\mathbb{Z}$. D'où $\delta = d$.

Plan

- 1 Groupes
- 2 Anneaux
- 3 Idéal d'un anneau commutatif
- 4 Anneau des polynômes à une indéterminée
- 5 Algèbres

Arithmétique dans $\mathbb{K}[X]$

Dans ce paragraphe, la notation $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ et le triplet $(\mathbb{K}[X], +, \times)$ désigne l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$.

Proposition 4.1 (intégrité de $\mathbb{K}[X]$).

L'anneau $\mathbb{K}[X]$ est intègre.

Théorème 4.1 (idéaux de $\mathbb{K}[X]$).

Les idéaux de $\mathbb{K}[X]$ sont de la forme

$$P.\mathbb{K}[X] \stackrel{\text{déf}}{=} \{PQ, Q \in \mathbb{K}[X]\}$$

où $P \in \mathbb{K}[X]$ unique à un coefficient multiplicatif non nul près.



Tout idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$ est engendré par un polynôme ***unitaire unique***.



L'idéal $I = \{P \in \mathbb{K}[X], P(0) = P(1) = 0\}$ est engendré par le polynôme $X(X - 1)$.



Plus grand commun diviseur

Soit $(P_1, \dots, P_k) \in \mathbb{K}[X]^k$.

1 Il existe $D \in \mathbb{K}[X]$ **unitaire unique** tel que :

$$P_1.\mathbb{K}[X] + \dots + P_k.\mathbb{K}[X] = D.\mathbb{K}[X].$$

Le polynôme D est appelé le plus grand commun diviseur des P_i , $1 \leq i \leq k$. On note $D = \text{pgcd}(P_1, \dots, P_k)$.

2 D est caractérisé par :

$$\left\{ \begin{array}{l} \forall i \in \llbracket 1, k \rrbracket, \quad D \mid P_i \\ \text{et} \\ \forall Q \in \mathbb{K}[X], \quad (\forall i \in \llbracket 1, k \rrbracket, \quad Q \mid P_i \implies Q \mid D) \end{array} \right\}.$$

Théorème 4.2 (être premiers entre eux versus avoir des racines dans $\mathbb{K}$).

Soit $(A, B) \in \mathbb{K}[X]^2$.

$A \wedge B = 1 \iff A \text{ et } B \text{ n'ont aucunes racines complexes en commun}.$

Polynôme irréductible sur un corps

Définition 4.1 (polynôme irréductible sur un corps).

On dit qu'un polynôme $P \in \mathbb{K}[X]$ est **irréductible**¹ sur $\mathbb{K}$ lorsque

- 1 P est non constant : $\deg P \geq 1$.
- 2 Les seuls diviseurs dans $\mathbb{K}[X]$ de P sont les polynômes constants non nuls et les polynômes associés à P .

¹Le polynôme P est dit réductible sur $\mathbb{K}$, s'il n'est pas irréductible sur $\mathbb{K}$.



$P \in \mathbb{K}[X]$ est irréductible si, et seulement si, P est non constant et si $A = BC$, alors B ou C est constant.



Attention, cette notion dépend du corps considéré. Ainsi $X^2 + 1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$.

Théorème 4.3 (décomposition en produit d'irréductibles).

Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) \geq 1$. Il existe $r \in \mathbb{N}^$, des polynômes $P_1, \dots, P_r \in \mathbb{K}[X]$ irréductibles sur $\mathbb{K}$, unitaires et deux à deux distincts, des entiers naturels non nuls $n_1, \dots, n_r$ tels que :*

$$P = \lambda P_1^{n_1} \dots P_r^{n_r}$$

où λ est le coefficient dominant de P . De plus cette décomposition est unique à l'ordre près des facteurs.

Théorème 4.4 (irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$).

- 1 P est irréductible sur $\mathbb{C}$ si, et seulement si, $\deg(P) = 1$.
- 2 P est irréductible sur $\mathbb{R}$ si, et seulement si, $\deg(P) = 1$ ou $\deg(P) = 2$ et de discriminant strictement négatif.

Théorème 4.5 (décomposition en produit d'irréductibles dans $\mathbb{C}[X]$).

Soit $P \in \mathbb{C}[X]$ tel que $\deg(P) \geq 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbb{C}[X]$ est de la forme :

$$P = \lambda \prod_{i=1}^r (X - \alpha_i)^{n_i}$$

où λ le coefficient dominant de P et $\alpha_1, \dots, \alpha_r$ sont les racines complexes deux à deux distincts de P .

Théorème 4.6 (décomposition en produit d'irréductibles dans $\mathbb{R}[X]$).

Soit $P \in \mathbb{R}[X]$ tel que $\deg(P) \geq 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbb{R}[X]$ est de la forme :

$$P = \lambda \prod_{i=1}^r (X - \alpha_i)^{n_i} \prod_{j=1}^s (X^2 + a_j X + b_j)^{m_j}$$

où λ est le coefficient dominant de P , $\alpha_1, \dots, \alpha_r$ sont des réels deux à deux distincts et $(a_1, b_1), \dots, (a_s, b_s)$ sont des couples deux à deux distincts de réels tels que pour tout $j \in \llbracket 1, s \rrbracket$, $a_j^2 - 4b_j < 0$.



- 1 Tout polynôme de $\mathbb{R}[X]$ de degré impair admet au moins une racine réelle.
- 2 Si $z \in \mathbb{C}$ est une racine d'un polynôme réel P , alors $\bar{z}$ est aussi une racine de P .

Plan

- 1 Groupes
- 2 Anneaux
- 3 Idéal d'un anneau commutatif
- 4 Anneau des polynômes à une indéterminée
- 5 Algèbres

Dans ce paragraphe, la notation $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

Définition 5.1 (algèbre).

On appelle $\mathbb{K}$ -**algèbre** un ensemble $\mathcal{A}$ muni de deux lois internes, notées $+$ et $\times$ et une loi externe sur le corps $\mathbb{K}$, notée $.$, telle que :

- 1 $(\mathcal{A}, +, .)$ est un espace vectoriel sur $\mathbb{K}$.
- 2 $(\mathcal{A}, +, \times)$ est un anneau.
- 3 $\forall \alpha \in \mathbb{K}, \forall (x, y) \in \mathcal{A}^2 \quad (\alpha.x) \times y = x \times (\alpha.y) = \alpha.(x \times y).$

L'algèbre¹ est dite **commutative** si $\times$ est commutative. On note usuellement $(\mathcal{A}, +, \times, .)$.

¹Les algèbres sont unitaires.



Les exemples suivants sont des $\mathbb{K}$ -algèbres usuelles :

- 1 $(\mathbb{K}[X], +, \times, .)$ est une algèbre commutative.
- 2 Si E est un $\mathbb{K}$ -espace vectoriel, $(\mathcal{L}(E), +, \circ, .)$ est une algèbre non commutative.
- 3 Pour $n \geq 2$, $(\mathcal{M}_n(\mathbb{K}), +, \times, .)$ est une algèbre non commutative.
- 4 Soit X un ensemble non vide. $(\mathcal{F}(X, \mathbb{K}), +, \times, .)$ est une algèbre commutative.

Définition 5.2 (sous-algèbre).

On dit que $\mathcal{B}$ est une **sous-algèbre** de l'algèbre $\mathcal{A}$ si $\mathcal{B}$ est un sous-anneau et un sous-espace vectoriel de $\mathcal{A}$.

Proposition 5.1 (caractérisation d'une sous-algèbre).

$$\mathcal{B} \text{ est une sous-algèbre de } \mathcal{A} \iff \begin{cases} 1_{\mathcal{A}} \in \mathcal{B} \\ \forall \lambda \in \mathbb{K}, \forall (x, y) \in \mathcal{B}^2, \quad x + \lambda.y \in \mathcal{B} \\ \forall (x, y) \in \mathcal{B}^2, \quad x \times y \in \mathcal{B} \end{cases}$$

Définition 5.3 (morphisme d'algèbres).

Soit $\mathcal{A}$ et $\mathcal{B}$ deux $\mathbb{K}$ -algèbres. On dit que $f : \mathcal{A} \longrightarrow \mathcal{B}$ est un **morphisme d'algèbres** si f est un morphisme d'anneaux et un morphisme d'espaces vectoriels¹.

$$^1 \forall (x, y) \in \mathcal{A}^2, \forall \lambda \in \mathbb{K}, \quad f(x + \lambda.y) = f(x) + \lambda.f(y).$$



Soit E un espace vectoriel sur $\mathbb{K}$ de dimension n et $\mathcal{B}$ une base de E . L'application qui, à $u \longmapsto \text{Mat}_{\mathcal{B}}(u)$ est un morphisme d'algèbres de $(\mathcal{L}(E), +, \circ, .)$ dans $(\mathcal{M}_n(\mathbb{K}), +, \times, .)$.

*Merci
pour votre
attention!*