Structures algébriques usuelles

Binyze Mohamed

MP 2025-2026

Sommaire

Dans ce chapitre est sauf indication contraire, la notation $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Groupes

G désigne un groupe multiplicatif de neutre e.

Compléments sur les groupes

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 : $\boxed{\forall \overline{a},\overline{b} \in \mathbb{Z}/n\mathbb{Z},\ \ \overline{a}+\overline{b}=\overline{a+b}}$ est un groupe abélien de neutre $n\mathbb{Z}$. De plus :

1. $\forall\, \overline{a} \in \mathbb{Z}/n\mathbb{Z},\ \ -\overline{a}=\overline{-a}$.

2. $\mathbb{Z}/n\mathbb{Z}=\left\{\overline{0},\ldots,\overline{n-1}\right\}$.

Proposition 1.1. **intersection de sous-groupes**

Soit $\left(H_i\right)_{i\in I}$ 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 $< A >$, défini par

$$< A > \overset{\text{déf}}{=} \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H}} H.$$

Lorsque $G =< A >$, 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. $< A >$ est le plus petit sous-groupe (au sens de l'inclusion) de G contenant A.
2. Si $A = \varnothing$, alors $< A >= \{e\}$. Si $A \neq \varnothing$, alors $< A >= \left\{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n},\ \ n \in \mathbb{N}^*,\ \forall i \in [\![1, n]\!],\ \ \varepsilon_i \in \{-1, 1\},\ a_i \in A\right\}$.

Exemple 1.1. ■ $n\mathbb{Z} =< n >$.

■ $\mathbb{Z}/n\mathbb{Z} =< \overline{1} >$ où $\overline{1}$ la classe de 1 modulo n.

■ 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 que [1] $\boxed{G =< a >= \left\{a^k,\ \ k \in \mathbb{Z}\right\}}$. L'élément a est appelé un ***générateur*** du groupe G.
2. On dit que G est ***cyclique*** lorsqu'il est monogène et fini.

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

Exemple 1.2. ■ $n\mathbb{Z} =< n >$, donc $(n\mathbb{Z}, +)$ est monogène.

■ $\mathbb{Z}/n\mathbb{Z} =< \overline{1} >$, donc $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.

■ $\mathbb{U}_n =< \omega_1 >$ 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 $\overline{k},\ \ k \in [\![1, n-1]\!]$ 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 : $\boxed{\text{l'ordre de } a = \min\left\{k \in \mathbb{N}^*,\ \ a^k = e\right\}}$.

Remarque 1.1. ■ Le neutre e est l'unique élément d'ordre fini égal à 1.

- Soit $a \in G \setminus \{e\}$. On a $\boxed{a \text{ est d'ordre } n \iff \left(a^n = e \text{ et } \forall k \in [\![1, n-1]\!],\ a^k \neq e\right)}$.

Exemple 1.3. - Dans $(\mathbb{Z}/6\mathbb{Z}, +)$, l'élément $\overline{4}$ est d'ordre 3.

- Dans $(\mathcal{GL}_2(\mathbb{K}), \times)$, l'élément $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.
- Dans $(\mathbb{C}^*, \times)$, l'élément $\omega_1 = e^{2i\pi/n}$ est d'ordre n.
- Dans $(\mathcal{S}_n, \circ)$, toute transposition $\tau \in \mathcal{S}_n \setminus \{\mathrm{Id}\}$ 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 d si, et seulement si, $< a >$ est d'ordre fini. Dans ce cas, $\boxed{< a >= \{e, a, \ldots, a^{d-1}\}}$.
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. $G = \{e, a, a^2, \ldots, a^{n-1}\}$.
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 a est d'ordre fini : $a^n = e$. De plus, l'ordre de a divise n.

2 Anneaux

Compléments sur les anneaux

Théorème 2.1. — produit d'anneaux

Soit $(A_i)_{1 \leq i \leq k}$ une famille d'anneaux. On définit les lois + et × sur $A_1 \times \ldots \times A_k$ en posant :

$$\forall \big((a_1, \ldots, a_k), (b_1, \ldots, b_k)\big) \in (A_1 \times \ldots \times A_k)^2,\ \begin{cases} (a_1, \ldots, a_k) + (b_1, \ldots, b_k) &= (a_1 + b_1, \ldots, a_k + b_k) \\ (a_1, \ldots, a_k) \times (b_1, \ldots, b_k) &= (a_1 \times b_1, \ldots, a_k \times b_k) \end{cases}$$

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

Proposition 2.1. — les inversibles de l'anneau produit

Si $A_1, \ldots, A_k$ sont des anneaux, alors [1] $\boxed{\mathbb{U}(A_1 \times \ldots \times A_k) = \mathbb{U}(A_1) \times \ldots \times \mathbb{U}(A_k)}$.

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

Définition 2.1. — éléments associés

On dit que deux éléments x et y de A sont ***associés*** si $\boxed{\exists a \in \mathbb{U}(A),\ x = ay}$.

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 :

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

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

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

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

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. **théorème des restes chinois**

Soient $n_1, \ldots, n_r$ des entiers deux à deux premiers entre eux et n leur produit. L'application [1] :

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

est un isomorphisme d'anneaux.

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

Corollaire 2.1. **système de congruences d'entiers**

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

$$(\mathrm{S}) : \begin{cases} x & \equiv & a_1 & [n_1] \\ \vdots & & \vdots & \\ x & \equiv & a_r & [n_r] \end{cases}$$

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 [1] :

$$\boxed{\varphi(n) = \mathrm{card}\Big\{k \in [\![0, n-1]\!],\ \ k \wedge n = 1\Big\}}.$$

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

Proposition 2.2. **multiplicativité de l'indicatrice d'Euler**

L'indicatrice d'Euler φ est multiplicative : $\boxed{\forall p, q \in \mathbb{N}^*,\ \ p \wedge q = 1 \implies \varphi(pq) = \varphi(p)\varphi(q)}$.

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

1. Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. $\boxed{\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}}$.

2. Soit $n \geq 2$ et $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. $\boxed{\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)}$.

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. $\boxed{k^{\varphi(n)} \equiv 1\,[n]}$. (théorème d'Euler)
2. Soit k un entier et p un nombre premier non diviseur de k. $\boxed{k^{p-1} \equiv 1\,[p]}$. (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.

3 Idéal d'un anneau commutatif

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

Idéaux

Définition 3.1. — idéal

On appelle ***idéal*** de A toute partie I de A non vide vérifie : $\boxed{\forall (x,y) \in I^2,\ x+y \in I \ \text{ et } \ \forall x \in I,\ \forall a \in A,\ ax \in I}$.

Proposition 3.1. — caractérisation d'un idéal

I est un idéal de A si, et seulement si, $(I, +)$ est un sous-groupe de $(A, +)$ et $\forall x \in I,\ \forall a \in A,\ ax \in I$.

Exemple 3.1. ■ $\{0_A\}$ et A sont des idéaux de A. ■ L'ensemble $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

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 $\boxed{xA \overset{\text{déf}}{=} \{xa,\ a \in A\}}$ des multiples de x.

Théorème 3.2. — caractérisation de xA

Soit $x \in A$. $\boxed{xA = \bigcap_{\substack{J \text{ idéal de } A \\ x \in J}} J}$. Ainsi xA est le plus petit idéal de A contenant x.

Arithmétique et idéaux

Définition 3.3. — divisibilité dans un anneau intègre

Supposons A intègre [1] et soit $(a,b) \in A^2$. On dit que a ***divise*** b, et on écrit $a \mid b$ si $\boxed{\exists u \in A,\ \ b = au}$.

1. L'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. $\boxed{a \text{ divise } b \iff bA \subset aA}$.
2. $\boxed{a \text{ et } b \text{ sont associés} \iff aA = bA}$.

Théorème 3.3. **somme d'idéaux**

Soient $I_1, \dots, I_k$ des idéaux de A. L'ensemble $\boxed{I_1 + \dots + I_k \overset{\text{déf}}{=} \left\{ \sum_{i=1}^{k} x_i,\ x_i \in I_i,\ 1 \leq i \leq k \right\}}$ est un idéal de A qui contient chaque I_i et est inclus dans tout idéal contenant $I_1, \dots, I_k$.

Application 3.1 (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 [1] $d = \text{pgcd}(a_1, \dots, a_k)$.
   - 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. d est caractérisé par : $\boxed{\forall i \in [\![1,k]\!],\quad d \mid a_i \quad \text{et} \quad \forall\, c \in \mathbb{Z},\quad \big(\forall i \in [\![1,k]\!],\quad c \mid a_i \implies c \mid d\big)}$.
   - On a $\forall i \in [\![1,k]\!],\quad a_i\mathbb{Z} \subset a_1\mathbb{Z} + \dots + a_k\mathbb{Z} = d\mathbb{Z}$ donc $d \mid a_i$ pour tout $i \in [\![1,k]\!]$. Soit $c \in \mathbb{Z}$ tel que $c \mid a_i$ pour tout $i \in [\![1,k]\!]$. On a $\forall i \in [\![1,k]\!],\quad a_i\mathbb{Z} \subset c\mathbb{Z}$ 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 $\forall i \in [\![1,k]\!],\quad \delta \mid a_i$ donc $\delta \mid d$ et par suite $d\mathbb{Z} \subset \delta\mathbb{Z}$. D'où $\delta = d$.

4 Anneau des polynômes à une indéterminée

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 $\mathbb{K}$.

Arithmétique dans $\mathbb{K}[X]$

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 $P.\mathbb{K}[X] \overset{\text{déf}}{=} \left\{PQ,\ Q \in \mathbb{K}[X]\right\}$ où $P \in \mathbb{K}[X]$ unique à un coefficient multiplicatif non nul près [1].

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

Exemple 4.1. ■ L'idéal $I = \left\{P \in \mathbb{K}[X],\ P(0) = P(1) = 0\right\}$ est engendré par le polynôme $X(X-1)$.

Application 4.1 (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 : $\boxed{\forall i \in [\![1,k]\!],\quad D \mid P_i \quad \text{et} \quad \forall\, Q \in \mathbb{K}[X],\quad \big(\forall i \in [\![1,k]\!],\quad Q \mid P_i \implies Q \mid D\big)}$.

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

Soit $(A, B) \in \mathbb{K}[X]^2$. $A \wedge B = 1 \iff A$ et B n'ont aucunes racines complexes en commun.

1. $\text{pgcd}(a_1, \dots, a_k) = 0 \iff a_1 = \dots = a_k = 0$.

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.

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

Remarque 4.1. ■ Attention, cette notion dépend du corps considéré. Ainsi X^2+1 est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$.

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

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 :

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

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 $\mathbb{C}$ $\iff$ $\deg(P) = 1$.
2. P est irréductible sur $\mathbb{R}$ $\iff$ $\deg(P) = 1$ 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 :

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

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 :

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

où λ est le coefficient dominant de P, $\alpha_1, \dots, \alpha_r$ 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 $j \in [\![1, s]\!]$, $a_j^2 - 4b_j < 0$.

Remarque 4.2. ■ Tout polynôme de $\mathbb{R}[X]$ de degré impair admet au moins une racine réelle.

■ Si $z \in \mathbb{C}$ est une racine d'un polynôme ***réel*** P, alors $\overline{z}$ est aussi une racine de P.

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. $\forall \alpha \in \mathbb{K},\ \forall (x, y) \in \mathcal{A}^2\ \ (\alpha.x) \times y = x \times (\alpha.y) = \alpha.(x \times y)$.

L'algèbre [1] est dite ***commutative*** si $\times$ est commutative. On note usuellement $(\mathcal{A}, +, \times, .)$.

1. Les algèbres sont unitaires.

Exemple 5.1 (Exemples de références).

- Les exemples suivants sont des $\mathbb{K}$-algèbres usuelles :
  - $(\mathbb{K}[X], +, \times, .)$.
  - $(\mathcal{L}(E), +, \circ, .)$ où E un $\mathbb{K}$-ev.
  - $(\mathcal{M}_n(\mathbb{K}), +, \times, .)$ où $n \geq 2$.
  - $(\mathcal{F}(X, \mathbb{K}), +, \times, .)$ où X un ensemble non vide.

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 vectoriels [1].

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

Exemple 5.2. Soit E un $\mathbb{K}$-ev 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 $(\mathcal{M}_n(\mathbb{K}), +, \times, .)$.