

Chapitre 2

Structures algébriques

1. Groupes

Introduction : utilité de la notion de structures algébriques, de morphismes

1.1. Définition et premières propriétés

Définition 1 : **groupe**

Soit G un ensemble. On dit que $(G, *)$ est un groupe si

- $*$ est une loi de composition interne sur G .
- $*$ est associative.
- G possède un élément neutre pour $*$.
- Tout élément de G admet pour $*$ un symétrique appartenant à G .

Si de plus $*$ est commutative, le groupe est dit **abélien** ou **commutatif**.

Propriétés : dans un groupe $(G, *)$

- Le neutre est unique
- Le symétrique d'un élément est unique : on le note a^{-1} .
- $(a^{-1})^{-1} = a$
- Tout élément est **régulier** pour la loi $*$.

- **Démonstration** 1.

1.2. Exemples de groupes « connus »

- Groupes de nombres : $(\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}_+^*, \times), (\mathbb{C}^*, \times)$
- Groupe $GL_n(K)$ des matrices inversibles (loi \times)
- Groupe orthogonal $O(E)$ (loi \circ)
- Groupe symétrique d'ordre n , noté \mathfrak{S}_n (loi \circ)

2.3.4.

1.3. Sous-groupes

Définition 2 : **sous-groupe**

Soit $(G, *)$ un groupe. On dit que H est un sous-groupe de G (pour la loi $*$) si $H \subset G$ et si $(H, *)$ est lui-même un groupe.

Propriétés : si H est un sous-groupe de G

- Le neutre de H est nécessairement le neutre de G .
- Le symétrique d'un élément dans H est aussi son symétrique dans G .

- **Démonstration** 5.

Proposition : caractérisations d'un sous-groupe

Soit $(G, *)$ un groupe dont l'élément neutre est noté e .

Les trois affirmations suivantes sont équivalentes :

- 1) H est un sous-groupe de G .
- 2) $H \subset G$, $e \in H$ et $\forall (a, b) \in H^2, a * b \in H$ et $a^{-1} \in H$
- 3) $H \subset G$, $e \in H$ et $\forall (a, b) \in H^2, a * b^{-1} \in H$

- **Démonstration** 6.
- Intérêt de cette notion : elle permet de justifier simplement qu'un ensemble H est un groupe, comme sous-groupe d'un groupe connu □.
- Exemples :
 - Chaîne de groupes pour l'addition : $\mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
 - Chaîne de groupes pour la multiplication : $\{1\} \subset \{-1, 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$.
 - Autre chaîne de groupes pour la multiplication : $\mathbb{Q}_+^* \subset \mathbb{R}_+^* \subset \mathbb{R}^*$.

Propriété : intersection de deux sous-groupes

L'intersection de deux sous-groupes de $(G, *)$ est aussi un sous-groupe de G .

- **Démonstration** 7.

1.4. Sous-groupes de \mathbb{Z}

Proposition : sous-groupes de $(\mathbb{Z}, +)$

Les seuls sous-groupes $(\mathbb{Z}, +)$ sont du type $n\mathbb{Z}$ où $n \in \mathbb{N}$.

- **Démonstration** 8.

1.5. Sous-groupes de \mathbb{R} (complément hors-programme)

- On rappelle (MPSI) que tout intervalle de \mathbb{R} rencontre \mathbb{Q} et $\mathbb{R} \setminus \mathbb{Q}$: on dit que \mathbb{Q} et $\mathbb{R} \setminus \mathbb{Q}$ sont **denses** dans \mathbb{R} (notion reprise au chapitre 5).
- Il est bon de connaître le résultat suivant ([hors-programme](#)) :

Proposition : sous-groupes de $(\mathbb{R}, +)$

Les seuls sous-groupes $(\mathbb{R}, +)$ sont :

- ou bien du type $\alpha\mathbb{Z}$ où $\alpha \in \mathbb{R}_+$
- ou bien denses dans \mathbb{R} .

- **Idée de la démonstration** (plan) 9.
- Les deux prototypes de sous-groupes de \mathbb{R} sont ainsi \mathbb{Z} et \mathbb{Q} .

1.6. Groupe-produit

Proposition - Définition 4 : **groupe-produit**

Soient $(G_1, *)$ et (G_2, \circ) deux groupes.

On définit sur $G_1 \times G_2$ une loi notée \otimes définie par :

$$\forall (a, b) \in G_1 \times G_2, \forall (c, d) \in G_1 \times G_2 : (a, b) \otimes (c, d) = (a * c, b \circ d)$$

Alors $(G_1 \times G_2, \otimes)$ est un groupe.

Ce groupe est appelé le groupe-produit des groupes $(G_1, *)$ et (G_2, \circ) .

- **Démonstration** à faire en exercice (**aucune difficulté majeure**).
- Exemple : en définissant $(a, b) + (c, d) = (a + c, b + d)$, on démontre que $(\mathbb{R}^2, +)$ est naturellement muni de cette structure de groupe-produit.
- De la même manière, on obtient des structures naturelles de groupes pour $(\mathbb{R}^n, +), (\mathbb{C}^n, +)$.

1.7. Morphismes de groupes

a) Définition

Définition 6 : **morphisme de groupes**

On appelle morphisme du groupe $(G_1, *)$ vers le groupe (G_2, \circ) toute application $\Phi : G_1 \rightarrow G_2$ telle que $\forall (x, y) \in G_1 : \Phi(x * y) = \Phi(x) \circ \Phi(y)$.

Si Φ est de plus bijective, on parle d'isomorphisme de groupes

b) Exemples

- $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$ et $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ sont des isomorphismes.
- La signature $\varepsilon : (\mathfrak{S}_n, \circ) \rightarrow (\{-1, 1\}, \times)$ est un morphisme de groupes
- Le déterminant $\det : (GL_n(\mathbb{K}), \times) \rightarrow (\mathbb{K}^*, \times)$ est un morphisme de groupes

c) Propriétés

Propriété 1 : **image du neutre, du symétrique**

Soit Φ un morphisme du groupe $(G_1, *)$ vers le groupe (G_2, \circ) .

Soit e_1 (resp. e_2) le neutre de G_1 (resp. G_2).

1. $\Phi(e_1) = e_2$
2. $\forall x \in G : \Phi(x^{-1}) = [\Phi(x)]^{-1}$

- Noter pour 1. la situation identique à celle de l'algèbre linéaire
- **Démonstration** 10.

Propriété 2 : image directe et image réciproque de sous-groupes

Soit Φ un morphisme du groupe $(G_1, *)$ vers le groupe (G_2, \circ) .

Soit H_1 (resp. H_2) un sous-groupe de G_1 (resp. G_2).

1. $\Phi(H_1)$ est un sous-groupe de G_2 .
2. $\Phi^{-1}(H_2)$ est un sous-groupe de G_1 .

- **Démonstration** 11. En particulier :

Propriété 3 : image et noyau d'un morphisme

Soit Φ un morphisme du groupe $(G_1, *)$ vers le groupe (G_2, \circ) de neutre e_2 .

1. $\text{Im}(\Phi) = \Phi(G_1)$ est un sous-groupe de G_2 appelé image de Φ .
2. $\text{Ker}(\Phi) = \Phi^{-1}(\{e_2\}) = \{x \in G_1 / \Phi(x) = e_2\}$ est un sous-groupe de G_1 appelé noyau de Φ .

- **Démonstration** 12.
- Exemple d'utilisation du noyau :

Groupe	Morphisme utilisé	Sous-groupe
(\mathfrak{S}_n, \circ)	$\varepsilon : (\mathfrak{S}_n, \circ) \rightarrow (\{-1, 1\}, \times)$	Groupe alterné \mathfrak{A}_n
$(O(E), \circ)$	$dét : (O(E), \circ) \rightarrow (\{-1, 1\}, \times)$	Groupe spécial orthogonal $SO(E)$
(\mathbb{C}^*, \times)	$Module : (\mathbb{C}^*, \times) \rightarrow (\mathbb{R}_+^*, \times)$	$U = \{z \in \mathbb{C} / z = 1\}$

Propriété 4 : condition d'injectivité d'un morphisme de groupe

Soit Φ un morphisme du groupe $(G_1, *)$ de neutre e_1 vers le groupe (G_2, \circ) .

Φ est injectif si et seulement si $\text{Ker}(\Phi) = \{e_1\}$

- **Démonstration** 13.
- Noter que la situation est identique à celle de l'algèbre linéaire.

Propriété 5 : isomorphisme réciproque

Soit Φ un isomorphisme du groupe $(G_1, *)$ sur le groupe (G_2, \circ) .

Alors Φ^{-1} est un isomorphisme du groupe (G_2, \circ) sur le groupe $(G_1, *)$.

- **Démonstration** 14.

2. Anneaux

2.1. Définition

Définition 1 : anneau, anneau commutatif

On dit que $(A, +, \times)$ est un anneau si

- $(A, +)$ est un groupe commutatif (neutre noté 0_A).
- \times est une loi de composition interne, associative et A possède un neutre distinct de 0_A , noté 1_A (souvent appelé l'élément **unité** de l'anneau).
- \times est distributive par rapport à la loi $+$

Si de plus \times est commutative, l'anneau est dit commutatif.

2.2. Exemples

- $(\mathbb{Z}, +, \times)$, $(\mathbb{R}[X], +, \times)$, $(\mathcal{L}(E), +, \circ)$, $(\mathcal{M}_n(K), +, \times)$ sont des anneaux
seuls les deux premiers sont commutatifs et intègres (cf. plus loin)

2.3. Groupe des inversibles d'un anneau

- On note que pour la loi \times , les éléments d'un anneau A ne sont pas nécessairement inversibles. On rappelle à ce sujet la propriété :

Proposition : groupe des inversibles d'un anneau

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

Soit A^* l'ensemble de ses éléments inversibles (pour la loi \times).

Alors (A^*, \times) est un groupe.

- Exemples : $(GL(E), \circ)$, $(GL_n(K), \times)$, $(\{-1, 1\}, \times)$, (\mathbb{R}^*, \times) **15**.

2.4. Autre exemple d'anneau : produit d'anneaux

Définition 2 : anneau produit

Si $(A_1, +, \times)$ et $(A_2, +, \times)$ sont des anneaux, $(A_2 \times A_2, \oplus, \otimes)$ est un anneau appelé anneau-produit des anneaux A_1 et A_2 si on a posé :

$$\forall (a, b) \in A_2 \times A_2, \forall (c, d) \in A_2 \times A_2 :$$

$$(a, b) \oplus (c, d) = (a + c, b + d) \quad \text{et} \quad (a, b) \otimes (c, d) = (a \times c, b \times d)$$

- Justification : $(A_1 \times A_2, \oplus, \otimes)$ est bien un anneau **16**.
- On généralise sans difficulté cette définition à un produit de n anneaux

2.5. Sous-anneau

Définition 2 : **sous-anneau**

On dit que $(A', +, \times)$ est un sous-anneau d'un anneau $(A, +, \times)$ si $A' \subset A$ et si $(A', +, \times)$ est lui-même un anneau de même unité 1_A .

Proposition : **caractérisation d'un sous-anneau**

$(A', +, \times)$ est un sous-anneau de l'anneau A si :

- $A' \subset A$
- $1_A \in A'$
- $\forall a, b \in A'^2 : a + b \in A', (-a) \in A' \text{ et } a \times b \in A'$

• Démonstration 17.

• Exemple : le plus petit sous-anneau de \mathbb{R} est \mathbb{Z} 18.

2.6. Morphisme d'anneaux

Définition 2 : **morphisme d'anneau**

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux et une application $\Phi : A \rightarrow B$.

On dit que Φ est un morphisme d'anneaux si


- $\forall a, b \in A : \Phi(a + b) = \Phi(a) + \Phi(b)$
- $\forall a, b \in A : \Phi(a \times b) = \Phi(a) \times \Phi(b)$
- $\Phi(1_A) = 1_B$

- C'est en particulier un morphisme de groupes, et donc $\Phi(0_A) = 0_B$.
- **Exemple 1** : $z \mapsto \bar{z}$ est un automorphisme du corps $(\mathbb{C}, +, \times)$
- **Exemple 2** : $Id_{\mathbb{R}}$ est le seul automorphisme du corps $(\mathbb{R}, +, \times)$

Propriété : **image d'un anneau par un morphisme**

Si Φ est un morphisme d'anneaux de $(A, +, \times)$ vers $(B, +, \times)$, alors $\text{Im}(\Phi)$ est un sous anneau de B .

• Démonstration 19.

•  Attention : $\text{Ker}(\Phi)$ n'est pas un sous-anneau, mais un idéal de A .

2.7. Anneau intègre

Définitions 4 : **diviseurs de zéro, anneau intègre**

1. Soit $(A, +, \times)$ un anneau et a un élément de A . a est un **diviseur de zéro** si

$$a \neq 0_A \text{ et } \exists b \in A \setminus \{0_A\} / a \times b = 0_A$$

2. Un **anneau intègre** est un anneau commutatif sans diviseur de zéro.

• Autrement dit, si $(A, +, \times)$ est un anneau commutatif, il est intègre si :

$$\forall (a, b) \in A^2 : [a \times b = 0_A] \Rightarrow [a = 0_A \text{ ou } b = 0_A]$$

- Exemples : $(\mathbb{Z}, +, \times)$ et $(\mathbb{R}[X], +, \times)$ sont des anneaux intègres.
- Contre-exemples : $(\mathcal{L}(E), +, \circ)$ et $(\mathcal{M}_n(K), +, \times)$ ne sont pas intègres.

Exercice : le justifier par deux arguments très distincts 20.

3. Corps

3.1. Définition

- On note que dans un anneau A , 0_A n'est jamais inversible (exercice in TD).

Définition 1 : **corps**

Un corps $(K, +, \times)$ est un anneau commutatif dans lequel tout élément non nul est inversible.

- Exemples :
 - \mathbb{C} , \mathbb{R} sont des corps.
 - Le corps $\mathbb{R}(X)$ des fractions rationnelles sur \mathbb{R} (Idem pour \mathbb{C}).
- Propriété : tout corps est en particulier un anneau intègre

3.2. Sous-corps

Définition 2 : **sous-corps**

On dit que $(K', +, \times)$ est un sous-corps d'un corps $(K, +, \times)$ si $K' \subset K$ et si $(K', +, \times)$ est lui-même un corps de même unité 1_K .

Proposition : **caractérisation d'un sous-corps**

$(K', +, \times)$ est un sous-corps du corps K si :

- $K' \subset K$
- $1_K \in K'$
- $\forall (x, y) \in K'^2 : x + y \in K', (-x) \in K', x \times y \in K'$
- $\forall x \in K' \setminus \{0_K\} : x^{-1} \in K'$

- Justification **21**.
- Chaînes de corps : $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ et au-delà ? \Rightarrow \mathbb{H} quaternions **22**.

4. Algèbre

4.1. Définition

Définition 1 : **K-algèbre**

$(\mathcal{A}, +, \times, \cdot)$ est une K -algèbre si

- $(\mathcal{A}, +, \times)$ est un anneau
- $(\mathcal{A}, +, \cdot)$ est un K -espace vectoriel
- $\forall (x, y) \in \mathcal{A}, \forall \alpha \in K : \alpha \cdot (x \times y) = (\alpha \cdot x) \times y = x \times (\alpha \cdot y)$

L'algèbre est dite commutative (respectivement intègre) si l'anneau est commutatif (respectivement intègre).

- Exemples :
 - Tout corps \mathbb{K} est une \mathbb{K} -algèbre ($\dim_{\mathbb{K}}(\mathbb{K}) = 1$)
 - \mathbb{C} est une \mathbb{R} -algèbre ($\dim_{\mathbb{R}} \mathbb{C} = 2$)
 - $(\mathbb{K}[X], +, \times, \cdot), (\mathcal{L}(E), +, \circ, \cdot), (\mathcal{M}_n(K), +, \times, \cdot), (\mathcal{F}(X, \mathbb{K}), +, \times, \cdot)$

4.2. Sous-algèbre

Définition 2 : On dit que \mathcal{A}' est une sous-algèbre d'une \mathbb{K} -algèbre $(\mathcal{A}, +, \times, .)$ si $\mathcal{A}' \subset \mathcal{A}$ et si \mathcal{A}' est elle-même une \mathbb{K} -algèbre de même unité $1_{\mathcal{A}}$.

Proposition : **caractérisation d'un sous-algèbre**

$(\mathcal{A}', +, \times, .)$ est une sous-algèbre de la \mathbb{K} -algèbre $(\mathcal{A}, +, \times, .)$ si :

- $\mathcal{A}' \subset \mathcal{A}$, $1_{\mathcal{A}} \in \mathcal{A}'$
- $\forall (x, y) \in \mathcal{A}'^2 : x + y \in \mathcal{A}'$, $x \times y \in \mathcal{A}'$, $\forall x \in \mathcal{A}'$, $\forall \alpha \in \mathbb{K} : \alpha.x \in \mathcal{A}'$

- Justification **23**.

5. Idéaux

5.1. Définition

Définition : On dit que \mathcal{I} est un idéal de l'anneau commutatif $(A, +, \times)$ si

- $(\mathcal{I}, +)$ est un sous-groupe du groupe $(A, +)$
- $\forall a \in A, \forall x \in \mathcal{I} : a \times x \in \mathcal{I}$ (surstabilité)

5.2. Exemples :

- **Exemple 1** : $\{0\}$ et A sont des idéaux de A . A ce sujet :

Si \mathcal{I} est un idéal de A : $[\mathcal{I} = A] \Leftrightarrow [1 \in \mathcal{I}]$ **24**.

- **Exemple 2** : Idéaux de \mathbb{Z} : les seuls idéaux de \mathbb{Z} sont du type $n\mathbb{Z}$ **25**.

- **Exemple 3** : le noyau d'un morphisme d'anneaux est un idéal **26**.



ce n'est jamais un sous-anneau de A : $1_A \notin \text{Ker}(\Phi)$!

5.3. Idéaux de $\mathbb{K}[X]$

Théorème : Les idéaux de $\mathbb{K}[X]$ sont tous du type $(P) = \{P \times Q, Q \in \mathbb{K}[X]\}$.

Si $P \neq 0$, P peut être choisi unitaire.

- **Démo.** **27**.

5.4. Applications

a) Exemple 1 : nombres algébriques

Définition : nombre **algébrique, transcendant**

Un nombre $\alpha \in \mathbb{K}$ (où. $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}) est dit algébrique s'il existe un polynôme non nul $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$.

Dans le cas contraire, il est dit transcendant.

- Endomorphisme (d'anneaux) d'évaluation : $Eval_{\alpha} : \begin{cases} \mathbb{K}[X] \rightarrow \mathbb{K} \\ P \rightarrow P(\alpha) \end{cases}$



Justification, nature du noyau **28**.

- Conséquence : polynôme minimal (irréductible) d'un nombre algébrique

b) Exemple 2 : polynôme minimal d'un endomorphisme, d'une matrice