Structures algébriques

البنيات الجبرية

📚 Résumé du cours

⚠️ **Hors programme officiel — Enrichissement** : Ce chapitre n'est pas exigible au baccalauréat marocain standard. Il est proposé comme approfondissement pour les élèves souhaitant aller plus loin.

I. Loi de composition interne

Définition

Une **loi de composition interne** (LCI) sur un ensemble E non vide est une application :

$$* : E \times E \to E, (x, y) \mapsto x * y$$

On dit aussi que E est **stable** pour la loi $*$.

Exemples

- $+$, $-$ et $\times$ sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$.
- $\div$ n'est PAS une LCI sur $\mathbb{Z}$ (résultat hors de $\mathbb{Z}$), mais l'est sur $\mathbb{R}^*$.
- $\cap$, $\cup$ sur $\mathcal{P}(E)$ (parties d'un ensemble E).
- Composition $\circ$ sur l'ensemble des applications $f : E \to E$.

II. Propriétés d'une LCI

Associativité

$*$ est **associative** sur E si : $\forall x, y, z \in E, (x * y) * z = x * (y * z)$.

Commutativité

$*$ est **commutative** sur E si : $\forall x, y \in E, x * y = y * x$.

Élément neutre

$e \in E$ est **neutre** pour $*$ si : $\forall x \in E, x * e = e * x = x$.

Si un neutre existe, il est **unique**.

Symétrique (inverse)

Soit e le neutre. $x \in E$ est **symétrisable** s'il existe $x' \in E$ tel que $x * x' = x' * x = e$.

Si $*$ est associative et admet un neutre, et si x est symétrisable, son symétrique est **unique**, noté x^{-1} (ou $-x$ en notation additive).

III. Groupes

Définition

Un ensemble G muni d'une loi $*$ est un **groupe** $(G, *)$ si :

1. $*$ est associative sur G.
2. $*$ admet un élément neutre $e \in G$.
3. Tout élément $x \in G$ est symétrisable.

Si de plus $*$ est commutative, $(G, *)$ est un **groupe commutatif** (ou **abélien**).

Exemples fondamentaux

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$: groupes abéliens.
- $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$: groupes abéliens.
- $(\mathbb{Z}/n\mathbb{Z}, +)$: groupe abélien.
- $(\mathbb{N}, +)$: **N'EST PAS** un groupe (pas de symétrique).
- Le groupe des rotations du plan de centre O : groupe abélien.

IV. Sous-groupes

Définition

Soit $(G, *)$ un groupe et $H \subseteq G$ non vide. H est un **sous-groupe** de G si :

1. $e \in H$ (le neutre est dans H)
2. $\forall x, y \in H : x * y \in H$ (stabilité)
3. $\forall x \in H : x^{-1} \in H$ (stabilité par symétrique)

On note $H \leq G$ (ou $H \subset G$ comme sous-groupe).

Caractérisation (un seul test)

$H \subseteq G$ non vide est un sous-groupe de $(G, *)$ ssi :

$$\forall x, y \in H : x * y^{-1} \in H$$

Exemples

- $(\mathbb{Z}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.
- Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ ($n \in \mathbb{N}$).
- $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
- $\mathbb{U}_n = \{z : z^n = 1\}$ est un sous-groupe fini de $\mathbb{U}$.

V. Morphismes de groupes

Définition

Soient $(G, *)$ et $(G', \top)$ deux groupes. Une application $f : G \to G'$ est un **morphisme de groupes** si :

$$\forall x, y \in G : f(x * y) = f(x) \top f(y)$$

- **Isomorphisme :** morphisme bijectif.
- **Endomorphisme :** morphisme de G dans lui-même.
- **Automorphisme :** endomorphisme bijectif.

Propriétés d'un morphisme $f : G \to G'$

- $f(e_G) = e_{G'}$
- $f(x^{-1}) = f(x)^{-1}$
- **Noyau :** $\mathrm{Ker}(f) = \{x \in G : f(x) = e_{G'}\}$ est un sous-groupe de G.
- **Image :** $\mathrm{Im}(f) = f(G)$ est un sous-groupe de G'.
- f est injective $\Leftrightarrow \mathrm{Ker}(f) = \{e_G\}$.

VI. Anneaux

Définition

Un ensemble A muni de deux lois $+$ et $\times$ est un **anneau** $(A, +, \times)$ si :

1. $(A, +)$ est un groupe abélien (neutre : 0_A).
2. $\times$ est associative.
3. $\times$ est **distributive** par rapport à $+$:
   $\forall a, b, c \in A : a(b + c) = ab + ac$ et $(b + c)a = ba + ca$.

Si $\times$ admet un neutre 1_A, l'anneau est **unitaire**. Si $\times$ est commutative, l'anneau est **commutatif**.

Exemples

- $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$: anneaux commutatifs unitaires.
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$: anneau commutatif unitaire.
- Anneau des polynômes $(\mathbb{R}[X], +, \times)$: commutatif unitaire.
- Anneau des matrices $(M_n(\mathbb{R}), +, \times)$: unitaire, **non commutatif** pour $n \geq 2$.

Anneau intègre

Un anneau commutatif unitaire non nul est **intègre** si :

$$\forall a, b \in A : ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Autrement dit : **pas de diviseurs de zéro**.

Exemples : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ intègres ; $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car $2 \cdot 3 = 6 \equiv 0 \pmod 6$.

VII. Corps

Définition

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

$$\forall x \in K \setminus \{0\} : \exists x^{-1} \in K, x \cdot x^{-1} = 1$$

Exemples

- $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$: corps.
- $(\mathbb{Z}, +, \times)$ n'est **pas** un corps (2 n'est pas inversible).

- $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps $\Leftrightarrow$ p **est premier**.

VIII. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Structure

Pour $n \geq 2$:

- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini de cardinal n.
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire.
- $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est **inversible** pour $\times \Leftrightarrow \gcd(x, n) = 1$.
- $(\mathbb{Z}/n\mathbb{Z})^*$ (éléments inversibles) a pour cardinal $\varphi(n)$ (indicatrice d'Euler).

Corps $\mathbb{Z}/p\mathbb{Z}$

Pour p premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps fini à p éléments. Tout élément non nul est inversible.

IX. Méthodologie

Pour montrer que $(G, *)$ est un groupe

1. Vérifier que $*$ est bien une LCI sur G (résultat dans G).
2. Vérifier l'associativité.
3. Trouver l'élément neutre e.
4. Montrer que tout x admet un symétrique $x^{-1} \in G$.

Pour montrer que H est un sous-groupe de G

1. $H \subseteq G$ et $H \neq \emptyset$ (généralement : $e \in H$).
2. Montrer : $\forall x, y \in H, x * y^{-1} \in H$.

🎯 Formules clés

- **Groupe** $(G, *)$ **:** associativité + neutre + inverse
- **Groupe abélien :** groupe + commutativité
- **Sous-groupe :** $H \neq \emptyset$ et $\forall x, y \in H, x * y^{-1} \in H$
- **Morphisme :** $f(x * y) = f(x) \top f(y)$
- **Noyau :** $\mathrm{Ker}(f) = f^{-1}(\{e'\})$ sous-groupe de G
- f **injective** $\Leftrightarrow \mathrm{Ker}(f) = \{e\}$
- **Anneau :** $(A, +)$ groupe abélien + $(\times)$ associative et distributive sur $+$
- **Anneau intègre :** $ab = 0 \Rightarrow a = 0$ ou $b = 0$
- **Corps :** anneau commutatif unitaire où tout $x \neq 0$ est inversible
- $\mathbb{Z}/p\mathbb{Z}$ **corps** $\Leftrightarrow p$ **premier**
- $\overline{x}$ **inversible dans** $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \gcd(x, n) = 1$

💡 Astuces & méthodes

🔴 Pièges classiques

❌

Prouver qu'une loi est associative : l'associativité doit être vérifiée pour TOUS triplets (x, y, z). Tester sur un exemple ne prouve rien — il faut une preuve algébrique générale.

❌

Élément neutre vs élément absorbant : l'élément neutre e vérifie $e * x = x * e = x$ pour tout x. L'élément absorbant a vérifie $a * x = x * a = a$ (ex : 0 pour la multiplication). Ce sont des rôles différents !

❌

Morphisme : vérifier TOUTES les opérations : pour un morphisme d'anneaux, vérifier $f(x + y) = f(x) + f(y)$ ET $f(x \cdot y) = f(x) \cdot f(y)$ et $f(1) = 1$. Oublier une condition = erreur !

🟢 Astuces de pros

✅

Critère de sous-groupe (méthode rapide) : $H \neq \emptyset$ et $\forall x, y \in H, x * y^{-1} \in H$. Une seule condition à vérifier (pas trois séparément). C'est la méthode la plus efficace pour les démonstrations.

✅

$\mathbb{Z}/n\mathbb{Z}$ **est un corps** $\Leftrightarrow n$ **est premier :** si n est composé ($n = ab$ avec $1 < a, b < n$), alors a et b sont des diviseurs de zéro dans $\mathbb{Z}/n\mathbb{Z}$ (car $\overline{a} \cdot \overline{b} = \overline{0}$), donc $\overline{a}$ n'est pas inversible.

💡

Ordre d'un élément : l'ordre de g dans un groupe fini G divise $|G|$ (théorème de Lagrange). Utile pour prouver que $g^{|G|} = e$ et réduire des puissances dans les groupes finis.