BURHAN

Structures algébriques : groupes, anneaux, corps (résumé)

2ème Année Baccalauréat · Sciences Mathématiques · Mathématiques

Version en ligne : burhan.ma/2bac/sciences-mathematiques/mathematiques/structures-algebriques/resume

Chapitre	Semestre
Structures algébriques : groupes, anneaux, corps	Semestre 2

L'essentiel en une page

Ce chapitre manipule des ensembles munis d'une ou de deux lois. Chaque structure se reconnaît à une liste d'axiomes. À l'examen, tu nommes l'ensemble, la loi, puis chaque axiome vérifié.

Partie H stable pour la loi

$$\forall x \in H,\ \forall y \in H,\ x * y \in H$$

Neutre e

$$x * e = e * x = x$$

Symétrique x′ de x

$$x * x' = x' * x = e$$

Symétrique d'un composé (loi associative, x et y symétrisables)

$$(x * y)' = y' * x'$$

Sous-groupe H de (G, ∗)

$$H \neq \emptyset \text{ et } \forall x, y \in H,\ x * y' \in H$$

Homomorphisme f

$$f(x * y) = f(x) \top f(y)$$

Produit de deux matrices

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Anneau $\mathbb{Z}/n\mathbb{Z}$, n ≥ 2

$$\mathbb{Z}/n\mathbb{Z} \text{ est un corps} \Leftrightarrow n \text{ est premier}$$

> **À retenir : La chaîne à reconnaître**
>
> 1. Une partie stable : la loi devient interne.
> 2. Un homomorphisme surjectif issu d'un groupe connu : un groupe, par transfert.
> 3. Un sous-groupe additif stable pour le produit : un anneau.
> 4. Une unité $1 \neq 0$ et un inverse pour chaque élément non nul : un corps.
>
> Chaque maillon finit par une phrase qui nomme la structure obtenue.

Lois, parties stables, propriétés

En clair : une loi sur E fabrique, à partir de deux éléments de E, un élément de E. Sur $\mathbb{R}$, $x * y = x + y + 2xy$ est une loi, par exemple $3 * 1 = 10$. Elle servira de fil rouge.

En revanche, la division n'est pas une loi sur $\mathbb{Z}^*$: $\frac{2}{3} \notin \mathbb{Z}^*$.

> **Définition : Partie stable et loi induite**

Soient $(E, *)$ un ensemble muni d'une loi de composition interne et A une partie non vide de E. On dit que A est **stable** pour $*$ si :

$$\forall x \in A,\ \forall y \in A, \quad x * y \in A.$$

La restriction de $*$ à $A \times A$ est alors une loi de composition interne sur A, appelée **loi induite** par $*$ sur A ; on la note encore $*$.

Exemple : Une partie stable, une partie qui ne l'est pas

Dans $(\mathbb{R}, \times)$, l'intervalle $]0, 1]$ est stable : soient x et y dans $]0, 1]$; de $0 < x \leq 1$ et $0 < y \leq 1$, on tire $0 < xy \leq 1$.

En revanche, la partie $\{1, 3\}$ n'est pas stable : $3 \times 3 = 9$ en sort.

Méthode : Montrer qu'une partie est stable

1. Prends x et y quelconques dans H et traduis leur appartenance.
2. Transforme $x * y$ jusqu'à retrouver la condition qui définit H.
3. Conclus en nommant la partie et la loi.

Rédaction attendue, avec $H = \left]-\frac{1}{2}, +\infty\right[$: « Soient x et y dans H. On a

$$1 + 2(x * y) = (1 + 2x)(1 + 2y),$$

produit de deux réels strictement positifs. Donc $x * y > -\frac{1}{2}$: H est stable pour $*$. »

Définition : Associativité et commutativité

Soit $(E, *)$ un ensemble muni d'une loi de composition interne.

1. La loi $*$ est **associative** si : $\forall x, y, z \in E,\ (x * y) * z = x * (y * z)$. On écrit alors $x * y * z$ sans parenthèses.
2. La loi $*$ est **commutative** si : $\forall x, y \in E,\ x * y = y * x$.

Définition : Distributivité

Soit E un ensemble muni de deux lois de composition interne $*$ et $\top$. La loi $\top$ est **distributive par rapport à** $*$ si, pour tous x, y, z de E :

$$x \top (y * z) = (x \top y) * (x \top z)$$

et

$$(y * z) \top x = (y \top x) * (z \top x).$$

Si $\top$ est commutative, l'une des deux égalités suffit.

Méthode : Étudier les propriétés d'une loi

1. **Commutativité** : compare $x * y$ et $y * x$ pour x et y quelconques.
2. **Associativité** : développe $(x * y) * z$, puis $x * (y * z)$, chacun de son côté.
3. **Réfutation** : un seul choix de valeurs chiffrées suffit.
4. **Conclusion** : « la loi $*$ est associative sur E », avec la loi et l'ensemble.

Exemple : Le fil rouge est commutatif et associatif

Soient x, y et z trois réels. On a $x + y + 2xy = y + x + 2yx$: la loi $*$ est commutative.

Les deux développements donnent la même expression :

$$\begin{aligned}(x * y) * z = x * (y * z) \\ &= x + y + z + 2xy \\ &\quad + 2xz + 2yz + 4xyz.\end{aligned}$$

La loi $*$ est donc associative sur $\mathbb{R}$.

Exemple : Ni commutative ni associative

Sur $\mathbb{R}$, soit $x \top y = x^2 + y$. On a $1 \top 2 = 3$ et $2 \top 1 = 5$: la loi n'est pas commutative.

De plus, $(1 \top 1) \top 0 = 4$ alors que $1 \top (1 \top 0) = 2$: elle n'est pas associative.

Neutre, symétriques, itérés

Définition : Élément neutre

Soit $(E, *)$ un ensemble muni d'une loi de composition interne. Un élément e de E est un **élément neutre** pour $*$ si :

$$\forall x \in E, \quad x * e = e * x = x.$$

Exemple : Neutre et symétriques du fil rouge

Pour tout réel x, $x * 0 = x$, et $0 * x = x$ par commutativité : 0 est le neutre.

Soit x un réel. On résout $x + x' + 2xx' = 0$, d'inconnue x'. Pour $x \neq -\dfrac{1}{2}$, on trouve :

$$x' = -\frac{x}{1 + 2x}.$$

Ainsi le symétrique de 1 est $-\frac{1}{3}$. Le réel $-\frac{1}{2}$ n'en a aucun : $\left(-\frac{1}{2}\right) * y = -\frac{1}{2}$ pour tout réel y.

Définition : Élément symétrique

Soient $(E, *)$ un ensemble muni d'une loi de composition interne admettant un élément neutre e, et $x \in E$. Un élément x' de E est un **symétrique** de x pour $*$ si :

$$x * x' = x' * x = e.$$

On dit alors que x est **symétrisable**. En notation additive, le symétrique s'appelle l'**opposé** et se note $-x$; en notation multiplicative, il s'appelle l'**inverse** et se note x^{-1}.

Méthode : Chercher le neutre et les symétriques

1. Résous $x * e = x$ pour **tout** x de E, puis vérifie $e \in E$.
2. Si la loi n'est pas commutative, vérifie aussi $e * x = x$.
3. Résous $x * x' = e$ d'inconnue x' ; vérifie $x' \in E$ et $x' * x = e$.
4. Nomme les éléments qui n'ont pas de symétrique.

Propriété : Symétrique pour une loi associative

Soit $(E, *)$ un ensemble muni d'une loi de composition interne **associative**, admettant un élément neutre e.

1. Un élément symétrisable x a un seul symétrique x', et x' est symétrisable de symétrique x : $(x')' = x$.
2. Si x et y sont symétrisables, alors $x * y$ est symétrisable et $(x * y)' = y' * x'$.

Exemple : Le symétrique d'un composé

Pour la loi $*$, le symétrique de 1 est $-\frac{1}{3}$ et celui de 2 est $-\frac{2}{5}$. Or $1 * 2 = 7$. Son symétrique est donc :

$$\left(-\frac{2}{5}\right) * \left(-\frac{1}{3}\right) = -\frac{7}{15}.$$

Contrôle : $7 * \left(-\frac{7}{15}\right) = 0$.

Exemple : Des itérés qui ne sont pas des puissances usuelles

Pour la loi $*$, $1^0 = 0$, le neutre. Puis $1^2 = 1 * 1 = 4$ et $1^3 = 4 * 1 = 13$. Ici 1^2 se calcule avec $*$, pas avec le produit usuel.

En notation additive, on écrit nx : dans $(\mathbb{Z}/9\mathbb{Z}, +)$, $4\overline{5} = \overline{20} = \overline{2}$.

Matrices carrées d'ordre 2 et 3

En clair : deux matrices de même ordre s'additionnent place par place, et un réel multiplie chaque coefficient. Avec $A = \begin{pmatrix} 1 & -3 \\ 2 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 4 & 1 \\ -1 & 2 \end{pmatrix}$, on obtient :

$$A + B = \begin{pmatrix} 5 & -2 \\ 1 & 2 \end{pmatrix},$$

$$2A = \begin{pmatrix} 2 & -6 \\ 4 & 0 \end{pmatrix}.$$

Définition : Produit de deux matrices carrées

Soient $n \in \{2, 3\}$, $A = (a_{ij})$ et $B = (b_{ij})$ dans $\mathcal{M}_n(\mathbb{R})$. Le **produit** $A \times B$, noté aussi AB, est la matrice $C = (c_{ij})$ de $\mathcal{M}_n(\mathbb{R})$ définie par

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} :$$

le coefficient de la ligne i et de la colonne j se calcule avec la ligne i de A et la colonne j de B. Pour $n = 2$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} aa_1 + bc_1 & ab_1 + bd_1 \\ ca_1 + dc_1 & cb_1 + dd_1 \end{pmatrix}.$$

La **matrice unité** I d'ordre n a des 1 sur la diagonale ($i = j$) et des 0 ailleurs.

Méthode : Calculer un produit de matrices

1. Contrôle que les deux matrices ont le même ordre.
2. Pour la place (i, j), associe la ligne i du premier facteur et la colonne j du second : produits terme à terme, puis somme.
3. Écris chaque somme avant de la réduire.
4. Pour l'autre ordre, refais un calcul complet.

$$\begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} 2+0 & 8+2 \\ 3+0 & 12-2 \end{pmatrix} = \begin{pmatrix} 2 & 10 \\ 3 & 10 \end{pmatrix}.$$

Exemple : Un produit d'ordre 3

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 3 & 1 & 4 \\ -1 & 0 & 0 \end{pmatrix}.$$

Par exemple, la place $(2,3)$ vaut $0 \times 0 + 2 \times 2 + 1 \times 0 = 4$.

Propriété : Propriétés du produit des matrices

Soit $n \in \{2, 3\}$.

1. Le produit est une loi de composition interne **associative** sur $\mathcal{M}_n(\mathbb{R})$, d'élément neutre I : $AI = IA = A$.
2. Le produit est distributif par rapport à l'addition : $A(B + C) = AB + AC$ et $(B + C)A = BA + CA$.
3. Pour tout réel α : $(\alpha A)B = A(\alpha B) = \alpha(AB)$.
4. Le produit n'est **pas commutatif** : il existe A et B dans $\mathcal{M}_n(\mathbb{R})$ telles que $AB \neq BA$.

Exemple : Vérifier un inverse par deux produits

Avec $P = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$, on calcule $PQ = I$ et $QP = I$. Donc P est inversible, d'inverse Q.

On écrit les deux produits, car le produit n'est pas commutatif.

Groupes

Définition : Groupe

Soit G un ensemble non vide muni d'une loi de composition interne $*$. On dit que $(G, *)$ est un **groupe** si :

1. la loi $*$ est associative ;
2. la loi $*$ admet un élément neutre e ;
3. tout élément de G admet un symétrique pour $*$.

Si de plus la loi $*$ est commutative, le groupe $(G, *)$ est dit **commutatif** (ou abélien).

Exemple : Exemple et contre-exemple

Exemple. $(\mathbb{Q}^*, \times)$ est un groupe commutatif. Le produit de deux rationnels non nuls est un rationnel non nul, et 1 est neutre. Pour p et q entiers non nuls, l'inverse de $\frac{p}{q}$ est $\frac{q}{p}$.

Contre-exemple. $(\mathbb{Q}, \times)$ n'est pas un groupe : 0 n'a pas d'inverse.

Propriété : Règles de calcul dans un groupe

Soient $(G, *)$ un groupe de neutre e et a, b, x, y des éléments de G.

1. **Simplification** : si $a * x = a * y$, alors $x = y$; si $x * a = y * a$, alors $x = y$.
2. **Équations** : l'équation $a * x = b$, d'inconnue $x \in G$, a une seule solution, $x = a' * b$; l'équation $x * a = b$ a une seule solution, $x = b * a'$.

Exemple : Résoudre une équation dans un groupe

On note $G = \mathbb{R} \setminus \left\{-\frac{1}{2}\right\}$. La section du transfert établit que $(G, *)$ est un groupe. L'équation $1 * x = 7$ y a une seule solution :

$$\begin{aligned} x &= 1' * 7 \\ &= \left(-\frac{1}{3}\right) * 7 = 2. \end{aligned}$$

Contrôle : $1 * 2 = 1 + 2 + 4 = 7$.

Propriété : Groupes de référence

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs, de neutre 0.
2. $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs, de neutre 1.
3. Pour tout entier naturel $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif, de neutre $\overline{0}$.
4. Pour $n \in \{2, 3\}$, $(\mathcal{M}_n(\mathbb{R}), +)$ est un groupe commutatif, de neutre O.

Théorème : Groupe des bijections d'un ensemble

Soient E un ensemble non vide et $\mathcal{S}(E)$ l'ensemble des bijections de E sur E. Alors $(\mathcal{S}(E), \circ)$ est un groupe, de neutre l'application identité id_E ; le symétrique d'une bijection f est sa bijection réciproque f^{-1}.

Exemple : Un groupe non commutatif

Dans $(\mathcal{S}(\mathbb{R}), \circ)$, prends $u : x \mapsto -x$ et $v : x \mapsto x + 1$. Alors $(u \circ v)(0) = -1$, mais $(v \circ u)(0) = 1$. Ce groupe n'est donc pas commutatif.

Méthode : Montrer qu'un ensemble est un groupe

1. **Sous-groupe** : si l'ensemble vit dans un groupe de référence muni de la même loi, utilise la caractérisation.
2. **Transfert** : sinon, cherche un homomorphisme surjectif issu d'un groupe connu.
3. **Axiomes** : en dernier recours, loi interne, associativité, neutre, symétriques.
4. **Conclusion** : « $(H, *)$ est un groupe commutatif », avec l'ensemble, la loi et la structure.

Sous-groupes

Théorème : Caractérisation d'un sous-groupe

Soient $(G, *)$ un groupe de neutre e et H une partie de G. H est un sous-groupe de $(G, *)$ si et seulement si :

1. $H \neq \emptyset$;
2. $\forall x \in H,\ \forall y \in H, \quad x * y' \in H$, où y' est le symétrique de y dans G.

Méthode : Montrer qu'une partie est un sous-groupe

Montrer que $H = \{2^a 3^b \ / \ (a, b) \in \mathbb{Z}^2\}$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

1. Chaque $2^a 3^b$ est un réel strictement positif : $H \subset \mathbb{R}_+^*$.
2. $1 = 2^0 3^0$, donc $1 \in H$ et $H \neq \emptyset$.
3. Soient $x = 2^a 3^b$ et $y = 2^c 3^d$ dans H. Le symétrique de y est $y^{-1} = 2^{-c} 3^{-d}$, et $x \times y^{-1} = 2^{a-c} 3^{b-d} \in H$.
4. « D'après la caractérisation, H est un sous-groupe de $(\mathbb{R}_+^*, \times)$, donc $(H, \times)$ est un groupe commutatif. »

Propriété : Sous-groupes de référence

1. Pour tout entier naturel n, l'ensemble $n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$.
2. L'ensemble $\mathbb{U} = \{z \in \mathbb{C} \ / \ |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
3. L'ensemble $\mathbb{R}_+^*$ des réels strictement positifs est un sous-groupe de $(\mathbb{R}^*, \times)$.

Exemple : Exemple et contre-exemple dans $(\mathbb{Z}, +)$

$5\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$: il contient 0 et, pour tous entiers k et m, $5k - 5m = 5(k - m)$.

En revanche, l'ensemble des entiers impairs n'en est pas un : il ne contient pas le neutre 0.

Homomorphismes et transfert

Définition : Homomorphisme et isomorphisme

Soient $(E, *)$ et $(F, \top)$ deux ensembles munis chacun d'une loi de composition interne, et f une application de E dans F.

1. f est un **homomorphisme** (ou morphisme) de $(E, *)$ dans $(F, \top)$ si, pour tous x, y de E :
$$f(x * y) = f(x) \top f(y).$$
2. f est un **isomorphisme** de $(E, *)$ sur $(F, \top)$ si f est un homomorphisme bijectif. On dit alors que $(E, *)$ et $(F, \top)$ sont **isomorphes**.

Exemple : Exemple et contre-exemple

Exemple. $f : x \mapsto 2^x$ va de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$, et, pour tous réels x et y, $2^{x+y} = 2^x \times 2^y$: c'est un homomorphisme.

Pour tout $u > 0$, l'équation $2^x = u$ a une seule solution, $x = \dfrac{\ln u}{\ln 2}$. Donc f est un isomorphisme.

Contre-exemple. $g : x \mapsto x^2$, de $(\mathbb{R}, +)$ dans $(\mathbb{R}, +)$, n'est pas un homomorphisme : $g(1+1) = 4$, alors que $g(1) + g(1) = 2$.

Méthode : Montrer qu'une application est un isomorphisme

1. Nomme les structures : $f : (E, *) \to (F, \top)$.
2. Calcule $f(x * y)$, puis $f(x) \top f(y)$, séparément, et constate l'égalité.
3. Pour un isomorphisme, prouve en plus que f est bijective : pour tout $u \in F$, l'équation $f(x) = u$ admet une solution unique dans E.
4. Conclus : « f est un isomorphisme de $(E, *)$ sur $(F, \top)$ ».

Théorème : Transfert de structure de groupe

Soient $(G, *)$ un groupe de neutre e, $(F, \top)$ un ensemble muni d'une loi de composition interne, et f un homomorphisme de $(G, *)$ dans $(F, \top)$.

1. L'image $f(G)$ est stable pour $\top$, et $(f(G), \top)$ est un groupe de neutre $f(e)$; pour tout $x \in G$, le symétrique de $f(x)$ dans $f(G)$ est $f(x')$.
2. Si $(G, *)$ est commutatif, $(f(G), \top)$ l'est aussi.
3. En particulier, si f est surjective (par exemple si f est un isomorphisme), alors $(F, \top)$ est un groupe, commutatif si $(G, *)$ l'est.

Un homomorphisme, un isomorphisme ou un transport de structure apparaît dans 13 des 14 exercices de structures consultés.

Méthode : Transférer une structure de groupe

Montrer que $(G, *)$ est un groupe commutatif, avec $G = \mathbb{R} \setminus \left\{-\frac{1}{2}\right\}$.

1. **Départ** : $(\mathbb{R}^*, \times)$ est un groupe commutatif.
2. **Homomorphisme** : pour $f : t \mapsto \frac{t-1}{2}$, de $\mathbb{R}^*$ dans G, on a $f(t) \neq -\frac{1}{2}$, car $t \neq 0$: f prend ses valeurs dans G. Pour tous t et s de $\mathbb{R}^*$, $f(t) * f(s) = \frac{ts-1}{2} = f(ts)$.
3. **Surjectivité** : tout $x \in G$ s'écrit $f(1+2x)$, avec $1+2x \neq 0$.
4. **Conclusion** : « par transfert de structure, $(G, *)$ est un groupe commutatif, de neutre $f(1) = 0$. »

À retenir : Des symétriques sans équation

Le transfert donne aussi les symétriques : celui de $f(t)$ est $f\left(\frac{1}{t}\right)$. Pour $x = 3 = f(7)$, le symétrique est $f\left(\frac{1}{7}\right) = -\frac{3}{7}$.

Propriété : Homomorphisme entre deux groupes

Soient $(G, *)$ et $(G_1, \top)$ deux groupes de neutres respectifs e et e_1, et f un homomorphisme de $(G, *)$ dans $(G_1, \top)$.

1. $f(e) = e_1$ et, pour tout $x \in G$, $f(x')$ est le symétrique de $f(x)$ dans G_1.
2. $f(G)$ est un sous-groupe de $(G_1, \top)$.

Anneaux

Définition : Anneau

Soit A un ensemble muni de deux lois de composition interne, notées $+$ et $\times$. On dit que $(A, +, \times)$ est un **anneau** si :

1. $(A, +)$ est un groupe commutatif ; son neutre est noté 0 et le symétrique de x, son opposé, est noté $-x$;
2. la loi $\times$ est associative ;
3. la loi $\times$ est distributive par rapport à la loi $+$.

L'anneau est **commutatif** si la loi $\times$ est commutative, et **unitaire** si la loi $\times$ admet un élément neutre, noté 1.

Exemple : Exemple et contre-exemple

Exemple. L'ensemble $B = \{a + ib \ / \ (a, b) \in \mathbb{Z}^2\}$, muni de $+$ et $\times$, est un anneau commutatif unitaire : la méthode ci-dessous le rédige.

Contre-exemple. $([0, +\infty[\,, +, \times)$ n'est pas un anneau : $([0, +\infty[\,, +)$ n'est pas un groupe, car 2 n'a pas d'opposé dans $[0, +\infty[$.

Propriété : Anneau induit sur une partie

Soient $(A, +, \times)$ un anneau et B une partie de A. Si B est un sous-groupe de $(A, +)$ et si B est stable pour $\times$, alors $(B, +, \times)$ est un anneau. Il est commutatif si $(A, +, \times)$ l'est, et unitaire, de même unité 1, si $(A, +, \times)$ est unitaire et si $1 \in B$.

Méthode : Montrer qu'un ensemble est un anneau

Montrer que $(B, +, \times)$ est un anneau commutatif unitaire.

1. **Référence** : $B \subset \mathbb{C}$, et $(\mathbb{C}, +, \times)$ est un anneau commutatif unitaire.
2. **Sous-groupe** : $0 \in B$. Soient $a + ib$ et $c + id$ dans B : $(a + ib) - (c + id) = (a - c) + i(b - d) \in B$.
3. **Stabilité** : $(a + ib)(c + id) = (ac - bd) + i(ad + bc) \in B$.
4. **Unité** : $1 = 1 + 0i \in B$.
5. « D'après l'anneau induit sur une partie, $(B, +, \times)$ est un anneau commutatif unitaire. »

Définition : Élément inversible, diviseur de zéro, anneau intègre

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

1. Si l'anneau est unitaire, un élément x de A est **inversible** s'il admet un symétrique pour $\times$, c'est-à-dire s'il existe $y \in A$ tel que $x \times y = y \times x = 1$. Ce symétrique est unique (« Symétrique pour une loi associative ») ; on le note x^{-1}. On note $A^\times$ l'ensemble des éléments inversibles de A.
2. Un élément $a \neq 0$ de A est un **diviseur de zéro** s'il existe $b \neq 0$ dans A tel que $a \times b = 0$ ou $b \times a = 0$.
3. Un anneau commutatif unitaire, avec $1 \neq 0$, est **intègre** s'il n'a aucun diviseur de zéro : pour tous a, b de A, si $a \times b = 0$, alors $a = 0$ ou $b = 0$.

Exemple : Inversibles et diviseurs de zéro

Dans $\mathbb{Z}/15\mathbb{Z}$, $\overline{2} \times \overline{8} = \overline{16} = \overline{1}$: $\overline{2}$ est inversible. Mais $\overline{3} \times \overline{5} = \overline{0}$: $\overline{3}$ est un diviseur de zéro.

Dans $\mathcal{M}_2(\mathbb{R})$, $N = \begin{pmatrix} 3 & -9 \\ 1 & -3 \end{pmatrix}$ n'est pas nulle, et pourtant $N \times N = O$.

Dans B, $i \times (-i) = 1$: i est inversible.

Propriété : Anneaux de référence

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs unitaires intègres.
2. Pour tout entier naturel $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire, d'unité $\overline{1}$.
3. Pour $n \in \{2, 3\}$, $(\mathcal{M}_n(\mathbb{R}), +, \times)$ est un anneau unitaire, d'unité I, **non commutatif**, et il a des diviseurs de zéro.

Propriété : Groupe des éléments inversibles

Soit $(A, +, \times)$ un anneau unitaire. L'ensemble $A^\times$ de ses éléments inversibles est stable pour $\times$, et $(A^\times, \times)$ est un groupe, de neutre 1.

Exemple : Le groupe des inversibles de $\mathbb{Z}/15\mathbb{Z}$

Les inversibles de $\mathbb{Z}/15\mathbb{Z}$ sont les classes $\overline{a}$ où a est premier avec 15 : $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{7}$, $\overline{8}$, $\overline{11}$, $\overline{13}$ et $\overline{14}$.

Ils forment un groupe pour $\times$. Par exemple, $\overline{7} \times \overline{8} = \overline{56} = \overline{11}$ reste inversible.

Corps

Définition : Corps

Un **corps** est un anneau unitaire $(K, +, \times)$ tel que $1 \neq 0$ et dont tout élément non nul est inversible. Le corps est **commutatif** si la loi $\times$ est commutative. On note $K^* = K \setminus \{0\}$.

Exemple : Exemple et contre-exemple

Exemple. Dans le corps $(\mathbb{C}, +, \times)$, l'inverse de $3 - 4i$ est $\dfrac{3 + 4i}{25}$, car $(3 - 4i)(3 + 4i) = 25$.

Contre-exemple. $(\mathbb{Z}/15\mathbb{Z}, +, \times)$ n'est pas un corps : la classe $\overline{3}$ n'est pas nulle et n'a pas d'inverse.

Propriété : Un corps n'a pas de diviseur de zéro

Soit $(K, +, \times)$ un corps. Pour tous a et b de K : si $a \times b = 0$, alors $a = 0$ ou $b = 0$. En particulier, K^* est stable pour $\times$.

Théorème : Caractérisation d'un corps commutatif

Soit K un ensemble muni de deux lois de composition interne $+$ et $\times$, et 0 le neutre de $+$. On suppose :

1. $(K, +)$ est un groupe commutatif ;
2. $K^* = K \setminus \{0\}$ est stable pour $\times$, et $(K^*, \times)$ est un groupe commutatif ;
3. la loi $\times$ est distributive par rapport à la loi $+$ sur K.

Alors $(K, +, \times)$ est un corps commutatif.

Théorème : Corps $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel, $n \geq 2$. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps commutatif si et seulement si n est premier.

Exemple : Les inverses dans $\mathbb{Z}/13\mathbb{Z}$

Comme 13 est premier, $\mathbb{Z}/13\mathbb{Z}$ est un corps commutatif.

$\overline{a}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{12}$
inverse	$\overline{7}$	$\overline{9}$	$\overline{10}$	$\overline{8}$	$\overline{11}$	$\overline{12}$

En revanche, $\mathbb{Z}/9\mathbb{Z}$ n'est pas un corps : $\overline{3} \times \overline{3} = \overline{0}$, avec $\overline{3} \neq \overline{0}$.

Théorème : Transfert d'une structure d'anneau ou de corps

Soient $(A, +, \times)$ un anneau, E un ensemble muni de deux lois de composition interne $*$ et $\top$, et f une bijection de A sur E telle que, pour tous x, y de A :

$$f(x + y) = f(x) * f(y)$$

et

$$f(x \times y) = f(x) \top f(y).$$

Alors $(E, *, \top)$ est un anneau, de zéro $f(0)$. Il est commutatif (respectivement unitaire, d'unité $f(1)$) si $(A, +, \times)$ l'est, et c'est un corps si $(A, +, \times)$ est un corps ; dans ce cas, pour $x \neq 0$, l'inverse de $f(x)$ est $f(x^{-1})$.

Méthode : Montrer qu'un anneau est un corps, ou le réfuter

1. **Prouver** : utilise la caractérisation par les groupes $(K, +)$ et $(K^*, \times)$, un transfert depuis un corps connu, ou le calcul direct d'un inverse dans K pour chaque élément non nul.
2. **Réfuter** : montre un diviseur de zéro, ou un élément non nul qui n'a pas d'inverse dans l'ensemble.

3. **Conclure** : « $(K, +, \times)$ est un corps commutatif », ou « n'est pas un corps ».

Exemple : Transférer une structure de corps

À maîtriser : ce transfert, rédigé avec ses deux égalités. Sur $\mathbb{R}$, soient $x * y = x + y + 2$ et $x \top y = xy + 2x + 2y + 2$.

La bijection $f : t \mapsto t - 2$ de $\mathbb{R}$ sur $\mathbb{R}$ vérifie, pour tous réels t et s, $f(t) * f(s) = f(t + s)$ et $f(t) \top f(s) = f(ts)$.

Par transfert depuis le corps $(\mathbb{R}, +, \times)$, $(\mathbb{R}, *, \top)$ est un corps commutatif. Son zéro est $f(0) = -2$ et son unité $f(1) = -1$.

Méthodes d'examen

Tu dois montrer	Outil	À écrire d'abord
une partie stable	calcul sur deux éléments quelconques	la forme des éléments de la partie
un groupe	sous-groupe, transfert ou axiomes	le groupe de référence et sa loi
un sous-groupe	caractérisation	$H \neq \emptyset$, puis $x * y' \in H$
un isomorphisme	homomorphisme, puis bijection	les deux ensembles et leurs lois
un anneau	anneau induit sur une partie	le sous-groupe additif et la stabilité pour $\times$
un corps commutatif	caractérisation ou transfert	le groupe $(K^*, \times)$, ou la bijection
une propriété fausse	contre-exemple chiffré	la négation avec « il existe »

Une partie stable ou une propriété de loi est demandée dans chacun des 14 exercices de structures consultés.

Méthode : Réfuter une propriété par un contre-exemple

1. Écris la négation : « non associative » signifie qu'il **existe** x, y, z tels que $(x * y) * z \neq x * (y * z)$.
2. Choisis des valeurs simples : 0, 1, ou des matrices remplies de zéros.
3. Calcule entièrement les deux membres.
4. Conclus : « pour ces valeurs, les deux membres diffèrent, donc la loi n'est pas associative ».

À retenir : Six phrases de conclusion

- « H est stable pour $*$. »
- « f est un homomorphisme de $(E, *)$ dans $(F, \top)$. »
- « Par transfert de structure, $(F, \top)$ est un groupe commutatif. »

- « H est un sous-groupe de $(G, *)$. »
- « $(B, +, \times)$ est un anneau commutatif unitaire. »
- « $(K, +, \times)$ est un corps commutatif. »

Pièges classiques

Attention : Un neutre d'un seul côté

Sur $\mathbb{R}$, soit $x \star y = x + 3y$. On a $x \star 0 = x$ pour tout réel x. Pourtant $0 \star 2 = 6$, et non 2 : 0 n'est pas neutre.

Comme $x \star e = x$ impose $e = 0$, cette loi n'a aucun neutre. Pour une loi non commutative, vérifie les deux côtés.

Attention : Permuter un produit de matrices

Avec $A = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, on trouve $AB = \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}$ mais $BA = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix}$.

Donc $(A + B)^2 = A^2 + AB + BA + B^2$ diffère ici de $A^2 + 2AB + B^2$.

Attention : Simplifier par une matrice

Avec $C = \begin{pmatrix} 1 & -1 \\ -2 & 2 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 3 \\ 1 & 3 \end{pmatrix}$, on a $CD = O = CO$, alors que $D \neq O$.

On ne passe donc pas de $CD = CO$ à $D = O$. On ne simplifie que par une matrice inversible.

Attention : Stable et contenant le neutre ne suffit pas

Dans $(\mathbb{Q}^*, \times)$, la partie $\mathbb{N}^*$ contient le neutre 1 et elle est stable pour $\times$. Ce n'est pourtant pas un sous-groupe : l'inverse de 2 est $\frac{1}{2}$, qui n'est pas dans $\mathbb{N}^*$.

Le test porte sur $x \times y^{-1}$, et non sur $x \times y$.

Attention : Un homomorphisme qui n'est pas bijectif

$f : x \mapsto x^4$ est un homomorphisme de $(\mathbb{R}^*, \times)$ dans lui-même, car $(xy)^4 = x^4 y^4$ pour tous réels non nuls x et y.

Mais $f(-2) = f(2) = 16$, et -1 n'a pas d'antécédent : ce n'est pas un isomorphisme. Le transfert ne donne une structure que sur l'image, $\mathbb{R}_+^*$.

Attention : Un anneau commutatif unitaire qui n'est pas un corps

$(\mathbb{Z}/22\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire, mais pas un corps : $\overline{2} \times \overline{11} = \overline{0}$, avec $\overline{2} \neq \overline{0}$ et $\overline{11} \neq \overline{0}$.

Un seul diviseur de zéro suffit à écarter le corps.

Attention : L'ordre des symétriques

Sur $\mathbb{R}$, soient $u : x \mapsto x - 4$ et $v : x \mapsto 5x$. Alors $u \circ v : x \mapsto 5x - 4$ a pour réciproque $y \mapsto \dfrac{y+4}{5}$, c'est-à-dire $v^{-1} \circ u^{-1}$.

L'autre ordre, $u^{-1} \circ v^{-1}$, donne $y \mapsto \dfrac{y}{5} + 4$: c'est faux. Le symétrique de $x * y$ est $y' * x'$.

Checklist avant l'examen

- Chaque structure est nommée avec son ensemble et sa ou ses lois.
- La stabilité se prouve sur deux éléments quelconques, jamais sur quelques essais.
- Pour une loi non commutative, neutre et symétriques se vérifient des deux côtés.
- Chaque produit de matrices se calcule dans l'ordre écrit.
- Avant le mot « isomorphisme », la bijectivité est prouvée.
- Avant un transfert vers F tout entier, la surjectivité est écrite.
- Avant le mot « corps », chaque élément non nul a un inverse dans l'ensemble.