BURHAN

Structures algébriques : groupes, anneaux, corps

2ème Année Baccalauréat · Sciences Mathématiques · Mathématiques

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

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

Ce que cache une opération

Sur $\mathbb{R}$, invente une opération. À deux réels x et y, elle associe :

$$x * y = xy - 2x - 2y + 6.$$

Quelques essais : $4 * 5 = 8$, $1 * 7 = -3$ et $3 * 7 = 7$.

Le nombre 3 semble ne rien changer : $3 * 7 = 7$, et aussi $3 * (-1) = -1$. Et le nombre 2 ? Avant de calculer, fais un pari.

Devine : Un nombre têtu

Avec la même opération, existe-t-il un réel y tel que $2 * y = 3$?

A. Oui, un seul : $y = 3$.

Faux.

Calcule : $2 * 3 = 6 - 4 - 6 + 6 = 2$, et non 3.

B. Non, aucun réel ne convient.

Juste.

Pour tout réel y, $2 * y = 2y - 4 - 2y + 6 = 2$. Le résultat ne vaut jamais 3.

C. Oui, et même deux : $y = 0$ et $y = 1$.

Faux.

$2 * 0 = 0 - 4 - 0 + 6 = 2$ et $2 * 1 = 2 - 4 - 2 + 6 = 2$. Aucun des deux ne donne 3.

Indice 1

Développe $2 * y$ avec la définition, sans choisir de valeur pour y.

Indice 2

Les termes en y se simplifient : que reste-t-il ?

Correction

Soit y un réel. On développe avec la définition :

$$\begin{aligned} 2 * y &= 2y - 4 - 2y + 6 \\ &= 2. \end{aligned}$$

Le résultat vaut toujours 2, jamais 3.

Conclusion. Aucun réel y ne vérifie $2 * y = 3$. Le nombre 2 « absorbe » tout ce qu'on lui associe.

Le secret de cette opération tient en une égalité, vraie pour tous réels x et y :

$$(x * y) - 2 = (x - 2)(y - 2).$$

C'est un produit déguisé, décalé de 2. Le nombre 3 y joue le rôle de 1, et 2 celui de 0.

Dans ce chapitre, tu vas apprendre à lire une opération comme celle-ci : élément neutre, symétriques, groupes, anneaux, corps. Tu sauras surtout **rédiger** chaque vérification, comme on l'attend à l'examen.

Lois de composition interne et parties stables

Une opération qui reste dans l'ensemble

Devine : Rester dans l'ensemble

Une opération mérite le nom de loi sur un ensemble si son résultat reste dans cet ensemble. Laquelle de ces opérations donne **toujours** un résultat dans l'ensemble indiqué ?

A. La soustraction $x - y$ sur $\mathbb{N}$.

Faux.
$3 - 7 = -4$, qui n'est pas un entier naturel.

B. La moyenne $\dfrac{x + y}{2}$ sur $\mathbb{Z}$.

Faux.
$\dfrac{1 + 4}{2} = \dfrac{5}{2}$, qui n'est pas un entier.

C. L'écart $|x - y|$ sur $\mathbb{N}$.

Juste.
Pour deux entiers naturels, $x - y$ est un entier, et sa valeur absolue est un entier naturel.

Indice 1
Pour écarter une opération, un seul couple suffit : cherche un couple qui fait sortir de l'ensemble.

Correction
Seul l'écart convient : pour x et y dans $\mathbb{N}$, $x - y$ est un entier, donc $|x - y| \in \mathbb{N}$.

Les deux autres sortent de l'ensemble dès un couple : la soustraction sort de $\mathbb{N}$ avec $3 - 7 = -4$, la moyenne sort de $\mathbb{Z}$ avec $\dfrac{1 + 4}{2} = \dfrac{5}{2}$.

Conclusion. Seul l'écart donne toujours un résultat dans l'ensemble indiqué.

Petit rappel de 1BAC. Une **application** f d'un ensemble A dans un ensemble B associe à **chaque** élément x de A un **unique** élément $f(x)$ de B.

L'ensemble $E \times E$ est formé des couples (x, y) d'éléments de E. L'ordre compte : $(2, 5)$ et $(5, 2)$ sont deux couples différents de $\mathbb{N} \times \mathbb{N}$.

Définition : Loi de composition interne

Soit E un ensemble non vide. Une **loi de composition interne** sur E est une application de $E \times E$ dans E : elle associe à tout couple (x, y) d'éléments de E un élément de E, noté par exemple $x * y$. On dit que $(E, *)$ est un ensemble muni d'une loi de composition interne.

Exemple : Trois lois de composition interne

- Sur $\mathbb{R}$, $x * y = x + y - 5$ définit une loi : le résultat est un réel. Par exemple, $2 * 9 = 6$.
- Sur $\mathbb{Z}/6\mathbb{Z}$ (chapitre d'arithmétique), l'addition est une loi : $\overline{4} + \overline{5} = \overline{3}$, car $9 \equiv 3\ [6]$.
- Sur l'ensemble des fonctions polynômes de degré au plus 2, la somme est une loi. Avec $P(t) = 1 + 2t - t^2$ et $Q(t) = 3 - 2t + t^2$, on obtient $(P + Q)(t) = 4$, de degré 0.

Exemple : Deux opérations qui ne sont pas des lois

- La division n'est pas une loi sur $\mathbb{R}$: le couple $(1, 0)$ n'a pas d'image, car $\dfrac{1}{0}$ n'existe pas.
- Le produit n'est pas une loi sur les fonctions polynômes de degré au plus 2 : $t^2 \times t^2 = t^4$, de degré 4.

Une seule image manquante, ou une seule image hors de l'ensemble, suffit à écarter une opération.

Parties stables

Dans $(\mathbb{R}, \times)$, prends la partie $H = \{-1, 1\}$. Les quatre produits $(-1) \times (-1)$, $(-1) \times 1$, $1 \times (-1)$ et 1×1 valent 1 ou -1 : on ne sort pas de H.

Avec la partie $\{1, 2\}$, en revanche, $2 \times 2 = 4$ fait sortir de la partie. Une partie dont la loi ne fait jamais sortir s'appelle une partie **stable**.

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 $*$.

Vérifie : Laquelle est stable ?

Parmi ces parties de $\mathbb{R}$, laquelle est stable pour la multiplication ?

A. L'intervalle $]1, 2]$.

Faux.

$2 \times 2 = 4$, et 4 n'appartient pas à $]1, 2]$.

B. L'ensemble des réels strictement négatifs.

Faux.

$(-1) \times (-3) = 3$ est positif : le produit sort de la partie.

C. La partie $\{0, 2\}$.

Faux.

$2 \times 2 = 4$ n'appartient pas à $\{0, 2\}$.

D. L'intervalle $[-1, 1]$.

Juste.

Si $|x| \leq 1$ et $|y| \leq 1$, alors $|xy| = |x| \times |y| \leq 1$.

Indice 1

Pour chaque partie, cherche d'abord un couple qui fait sortir. Si tu n'en trouves pas, cherche une preuve.

Correction

Seul $[-1, 1]$ est stable. Soient x et y dans $[-1, 1]$. Alors :

$$\begin{aligned} |xy| &= |x| \times |y| \\ &\leq 1 \times 1 = 1, \end{aligned}$$

donc $xy \in [-1, 1]$.

Pour les trois autres, un seul couple suffit à sortir : $2 \times 2 = 4$, ou $(-1) \times (-3) = 3$.

Conclusion. Parmi ces parties, seule $[-1, 1]$ est stable pour la multiplication.

Montrer qu'une partie est stable

Méthode : montrer qu'une partie est stable

1. **Prendre** deux éléments quelconques x et y de H, et traduire leur appartenance à H.
2. **Transformer** $x * y$ pour faire apparaître la condition qui définit H.
3. **Conclure** en nommant la partie et la loi.

Rédaction attendue. Sur $\mathbb{R}$, soit $x * y = xy - x - y + 2$, et $H =]1, +\infty[$.

« Soient x et y dans H. On a :

$$(x * y) - 1 = (x - 1)(y - 1).$$

Or $x - 1 > 0$ et $y - 1 > 0$, donc $(x * y) - 1 > 0$, soit $x * y \in H$. Ainsi H est stable pour $*$. »

À toi : Un intervalle stable

Sur $\mathbb{R}$, on pose $x \top y = x + y - xy$. Montre que l'intervalle $H =]0, 1[$ est stable pour $\top$.

Indice 1
Calcule $1 - (x \top y)$, puis factorise.
Indice 2
Pour x et y dans $]0, 1[$, où se trouvent $1 - x$ et $1 - y$?
Indice 3
Un produit de deux réels de $]0, 1[$ est encore dans $]0, 1[$.

Réponse
Soient x et y dans H. On factorise :

$$\begin{aligned} & 1 - (x \top y) \\ & = 1 - x - y + xy \\ & = (1 - x)(1 - y). \end{aligned}$$

Or $1 - x$ et $1 - y$ appartiennent à $]0, 1[$. Leur produit est strictement positif et strictement inférieur à $1 \times 1 = 1$.

Donc $0 < 1 - (x \top y) < 1$, soit $0 < x \top y < 1$.

Conclusion. Pour tous x et y de H, $x \top y \in H$: l'intervalle H est stable pour $\top$.

Attention : Des essais ne prouvent rien

Dans $\mathbb{Z}$, soit H l'ensemble des entiers multiples de 2 ou de 3. Les essais $2 + 4 = 6$, $3 + 9 = 12$ et $4 + 6 = 10$ restent dans H.

Pourtant H n'est pas stable pour $+$: $2 + 3 = 5$, qui n'est multiple ni de 2 ni de 3. Des essais réussis ne prouvent rien. Pour prouver, on prend deux éléments **quelconques** ; pour réfuter, un seul couple suffit.

Associativité, commutativité, distributivité

L'ordre des calculs

Devine : Où placer les parenthèses ?

Sur $\mathbb{R}$, on pose $x \top y = x - y$. Compare $(9 \top 4) \top 2$ et $9 \top (4 \top 2)$.

A. Ils sont égaux, comme pour l'addition.
Faux.
$(9 - 4) - 2 = 3$, alors que $9 - (4 - 2) = 7$.

B. Ils sont différents : 3 et 7.

Juste.
$(9-4)-2=3$ et $9-(4-2)=9-2=7$.

C. On ne peut pas calculer $(9\top 4)\top 2$.

Faux.
Le résultat $9\top 4=5$ est un réel : on peut le composer avec 2, et on trouve 3.

Correction
On trouve $(9\top 4)\top 2=5-2=3$ et $9\top(4\top 2)=9-2=7$.

Les parenthèses changent le résultat : la soustraction n'est pas associative. On ne peut donc pas écrire $9\top 4\top 2$ sans parenthèses.

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 : $\forall x,y\in E,\ x*y=y*x$.

Exemple : Trois lois, trois comportements

- Sur $\mathbb{R}$, $x*y=x+y+4$ est associative : $(x*y)*z$ et $x*(y*z)$ valent tous deux $x+y+z+8$. Elle est aussi commutative.
- Sur $\mathbb{R}$, $x\top y=2x+y$ n'est pas commutative : $1\top 0=2$ et $0\top 1=1$. Elle n'est pas associative : $(1\top 0)\top 0=4$, mais $1\top(0\top 0)=2$.
- La composition $\circ$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ est associative, mais pas commutative. Avec $f(x)=x+1$ et $g(x)=x^2$: $(f\circ g)(1)=2$ et $(g\circ f)(1)=4$.

Vérifie : Une loi à étudier

Sur $\mathbb{R}$, on pose $x*y=x+y-3xy$. Que peut-on dire de cette loi ?

A. Elle est associative, mais pas commutative.

Faux.
$x+y-3xy$ et $y+x-3yx$ sont égaux : la loi est commutative.

B. Elle est commutative, mais pas associative.

Faux.
Développe les deux membres : tu trouves la même expression, symétrique en x, y et z.

C. Elle est commutative et associative.

Juste.
Les deux membres valent $x+y+z-3xy-3xz-3yz+9xyz$.

Indice 1
Commence par $(x*y)*z=(x*y)+z-3(x*y)z$.
Indice 2
Remplace $x*y$ par son expression, puis développe.

Correction
Commutativité. Soient x et y deux réels. Comme $xy=yx$, on a $x*y=y*x$.

Associativité. Soit aussi z un réel. On remplace $x*y$ par son expression, puis on développe :

$$\begin{aligned}(x*y)*z&=x+y-3xy+z\\&\quad-3(x+y-3xy)z\\&=x+y+z-3xy\\&\quad-3xz-3yz+9xyz.\end{aligned}$$

Le même calcul donne $x*(y*z)=x+y+z-3xy-3xz-3yz+9xyz$. Les deux membres sont égaux.

Conclusion. La loi $*$ est commutative et associative sur $\mathbb{R}$.

Deux lois sur un même ensemble

Dans $\mathbb{R}$, $3\times(4+5)=3\times4+3\times5=27$: la multiplication se **distribue** sur l'addition.

L'inverse est faux : $3+(4\times5)=23$, alors que $(3+4)\times(3+5)=56$. Quand un ensemble porte deux lois, on se demande donc laquelle se distribue sur l'autre.

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 :

$$x\top(y*z)=(x\top y)*(x\top z)\quad\text{et}\quad(y*z)\top x=(y\top x)*(z\top x).$$

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

Exemple : Exemple guidé : une distributivité à vérifier

Sur $\mathbb{R}$, on pose $x*y=x+y-1$ et $x\top y=xy-x-y+2$. La loi $\top$ est commutative : une seule égalité suffit. Soient x, y et z trois réels.

Premier membre.

$$\begin{aligned} & x\top(y*z) \\ &= x(y+z-1)-x \\ &\quad -(y+z-1)+2 \\ &= xy+xz-2x-y-z+3. \end{aligned}$$

Second membre.

$$\begin{aligned} & (x\top y)*(x\top z) \\ &= (xy-x-y+2) \\ &\quad +(xz-x-z+2)-1 \\ &= xy+xz-2x-y-z+3. \end{aligned}$$

Conclusion. Les deux membres sont égaux pour tous réels x, y et z : la loi $\top$ est distributive par rapport à $*$.

Ce qui passe à une partie stable

L'addition est associative sur $\mathbb{R}$, et la partie $\mathbb{Z}$ est stable pour $+$. Faut-il revérifier l'associativité sur $\mathbb{Z}$? Non.

Pourquoi est-ce vrai ? L'égalité $(x+y)+z=x+(y+z)$ est vraie pour **tous** les réels. Elle l'est donc en particulier pour les entiers.

Propriété : Propriétés héritées par une loi induite

Soient E un ensemble muni d'une loi de composition interne $*$ et A une partie de E stable pour $*$.

1. Si $*$ est associative (respectivement commutative) sur E, la loi induite l'est sur A.
2. Si E est muni d'une seconde loi $\top$, si A est aussi stable pour $\top$ et si $\top$ est distributive par rapport à $*$ sur E, alors elle l'est sur A.

Démonstration

Étape 1. Les égalités qui définissent l'associativité, la commutativité et la distributivité sont vraies **pour tous** les éléments de E.

Étape 2. Les éléments de A sont des éléments de E. Donc ces égalités sont vraies en particulier pour tous les éléments de A.

Étape 3. Comme A est stable, chaque membre de ces égalités est calculé par la loi induite, dans A. Les propriétés sont donc vraies pour la loi induite.

Méthode : étudier l'associativité et la commutativité

1. **Commutativité** : calculer $x*y$ et $y*x$ pour x et y quelconques, puis comparer.
2. **Associativité** : développer $(x*y)*z$, puis $x*(y*z)$, **séparément**, et comparer.

3. **Réfuter** : si les expressions diffèrent, donner des valeurs chiffrées qui donnent deux résultats différents.
4. **Hériter** : sur une partie stable, citer les propriétés héritées par la loi induite, sans tout recalculer.

Rédaction attendue. « Pour tous x, y, z de E, $(x * y) * z = \dots$ et $x * (y * z) = \dots$. Ces deux expressions sont égales, donc la loi $*$ est associative sur E. »

À toi : Une loi avec une racine

Sur $[0, +\infty[$, on pose $x * y = \sqrt{x^2 + y^2}$. Par exemple, $3 * 4 = 5$. Montre que $*$ est une loi de composition interne, commutative et associative.

Indice 1
Pour la loi interne : une racine carrée est un réel positif ou nul.
Indice 2
Calcule $(x * y)^2$: il vaut $x^2 + y^2$.
Indice 3
Développe $(x * y) * z$ en utilisant $(x * y)^2 = x^2 + y^2$.

Réponse
Loi interne. Soient x et y dans $[0, +\infty[$. Alors $x^2 + y^2 \geq 0$, donc $\sqrt{x^2 + y^2}$ existe et appartient à $[0, +\infty[$.

Commutativité. Comme $x^2 + y^2 = y^2 + x^2$, on a $x * y = y * x$.

Associativité. Soit aussi $z \in [0, +\infty[$. Comme $(x * y)^2 = x^2 + y^2$:

$$\begin{aligned}(x * y) * z &= \sqrt{(x * y)^2 + z^2} \\ &= \sqrt{x^2 + y^2 + z^2}.\end{aligned}$$

De même, $x * (y * z) = \sqrt{x^2 + y^2 + z^2}$.

Conclusion. $*$ est une loi de composition interne sur $[0, +\infty[$, commutative et associative.

Élément neutre, éléments symétriques, itérés

Un élément qui ne change rien

Devine : L'élément discret

Sur $\mathbb{R}$, on pose $x * y = x + y - 4$. Quel réel e vérifie $x * e = x$ pour **tout** réel x ?

A. $e = 4$
Juste.

$x * 4 = x + 4 - 4 = x$, pour tout réel x.

B. $e = 0$

Faux.

$x * 0 = x - 4$, qui n'est pas égal à x.

C. $e = -4$

Faux.

$x * (-4) = x - 8$: on s'éloigne encore de x.

Correction

L'équation $x + e - 4 = x$ donne $e = 4$. Réciproquement, pour tout réel x, $x * 4 = x$; comme la loi est commutative, on a aussi $4 * x = x$.

Conclusion. Le réel 4 ne change rien : c'est l'élément neutre de $*$.

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 :

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

Attention : Un neutre se vérifie des deux côtés

Sur $\mathbb{R}$, on pose $x * y = x + y^2$. Le réel 0 vérifie $x * 0 = x$ pour tout x. Pourtant 0 n'est pas neutre : $0 * 3 = 9$, et non 3.

Aucun autre réel ne convient, car $x * e = x$ impose $e = 0$. Cette loi n'a donc pas d'élément neutre. Une loi non commutative se vérifie **des deux côtés** : $x * e = x$ **et** $e * x = x$.

Exemple : Avec ou sans neutre

- Dans $(\mathbb{R}, \times)$, le neutre est 1. Pour la composition des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, c'est l'identité $x \mapsto x$.
- Pour la loi de la découverte, $x * y = xy - 2x - 2y + 6$, le neutre est 3 : $x * 3 = 3x - 2x - 6 + 6 = x$, et la loi est commutative.
- Dans $\mathbb{N}^*$, l'addition n'a pas de neutre : $n + e = n$ impose $e = 0$, qui n'appartient pas à $\mathbb{N}^*$.

Dans chaque cas, on trouve au plus un neutre. Pourquoi jamais deux ?

Propriété : Unicité de l'élément neutre

Soit $(E, *)$ un ensemble muni d'une loi de composition interne. Si $*$ admet un élément neutre, celui-ci est unique.

Démonstration

Étape 1. Soient e et e_1 deux éléments neutres pour $*$.

Étape 2. Comme e est neutre, $e * e_1 = e_1$. Comme e_1 est neutre, $e * e_1 = e$.

Conclusion. $e_1 = e * e_1 = e$: les deux neutres sont égaux.

Revenir au neutre

Devine : Le chemin du retour

Avec $x * y = x + y - 4$, de neutre 4, quel réel x' vérifie $10 * x' = 4$?

A. $x' = -2$

Juste.
$10 + (-2) - 4 = 4$: on revient bien au neutre.

B. $x' = -10$

Faux.
$10 * (-10) = -4$. L'opposé ramène à 0, mais le neutre de cette loi est 4.

C. $x' = \dfrac{1}{10}$

Faux.
L'inverse sert pour la multiplication. Ici, $10 * \dfrac{1}{10} = \dfrac{61}{10}$, et non 4.

Correction

On résout $10 + x' - 4 = 4$, d'inconnue réelle x' : $x' = -2$. La loi est commutative, donc $(-2) * 10 = 4$ aussi.

Conclusion. Le réel -2 est le symétrique de 10 pour $*$.

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. **Neutre** : résoudre $x * e = x$ pour **tout** x ; vérifier $e \in E$, puis $e * x = x$ si la loi n'est pas commutative.
2. **Symétrique** : résoudre $x * x' = e$ d'inconnue x' ; vérifier $x' \in E$, puis $x' * x = e$.
3. **Exclure** : nommer les éléments pour lesquels cette équation n'a pas de solution dans E.

Rédaction attendue. Avec $x * y = x + y - 4$ sur $\mathbb{R}$:

« Pour tout réel x, $x * 4 = 4 * x = x$, donc 4 est le neutre.

Soit x un réel. Alors $8 - x \in \mathbb{R}$ et

$$x * (8 - x) = (8 - x) * x = 4,$$

donc x a pour symétrique $x' = 8 - x$. »

Exemple : Symétriques dans deux cadres

- Dans $\mathbb{Z}/10\mathbb{Z}$ muni de la multiplication, de neutre $\overline{1}$: $\overline{3} \times \overline{7} = \overline{21} = \overline{1}$, donc $\overline{3}$ a pour inverse $\overline{7}$. En revanche, $\overline{2}$ n'a pas d'inverse : pour tout entier k, $2k - 1$ est impair, donc jamais multiple de 10.
- Pour la loi de la découverte, de neutre 3 : $x * x' = 3$ équivaut à $(x - 2)(x' - 2) = 1$. Pour $x \neq 2$, on trouve $x' = 2 + \dfrac{1}{x - 2}$. Le symétrique de 5 est $\dfrac{7}{3}$, et 2 n'en a pas.

Dernière observation : $\overline{3} \times \overline{9} = \overline{7}$, dont l'inverse est $\overline{3}$. On obtient aussi cet inverse par $\overline{9}^{-1} \times \overline{3}^{-1} = \overline{9} \times \overline{7}$.

Pourquoi est-ce vrai ? Ici, la loi est commutative et l'ordre ne compte pas. L'énoncé suivant traite le cas général, où l'ordre compte.

Le symétrique d'un composé

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

Démonstration

Étape 1 (unicité). Soient x' et x'' deux symétriques de x. Par associativité,

$$x'' = x'' * e = x'' * (x * x') = (x'' * x) * x' = e * x' = x'.$$

Étape 2. L'égalité $x * x' = x' * x = e$ dit aussi que x est un symétrique de x'. Par l'étape 1, $(x')' = x$.

Étape 3 (point 2). Par associativité, $(x * y) * (y' * x') = \big(x * (y * y')\big) * x' = (x * e) * x' = x * x' = e$. De même, $(y' * x') * (x * y) = \big(y' * (x' * x)\big) * y = (y' * e) * y = y' * y = e$. Donc $y' * x'$ est le symétrique de $x * y$.

À retenir : Ce qu'il faut retenir de la preuve

Unicité : on insère le neutre sous la forme $e = x * x'$, puis on regroupe autrement grâce à l'associativité.

Symétrique d'un composé : on propose un candidat, $y' * x'$, et on vérifie qu'il ramène au neutre **des deux côtés**. On défait dans l'ordre inverse, comme on retire ses chaussures avant ses chaussettes.

Vérifie : Le pivot de l'étape 1

À l'étape 1 de la démonstration, on passe de $x'' * (x * x')$ à $(x'' * x) * x'$. Quelle hypothèse le permet ?

A. La commutativité de $*$.

Faux.
La loi n'est pas supposée commutative. Et l'égalité ne permute aucun facteur : elle déplace seulement les parenthèses.

B. L'existence du neutre e.

Faux.
Le neutre sert juste avant et juste après, pour écrire $x'' = x'' * e$ et $e * x' = x'$. Il ne déplace pas les parenthèses.

C. L'associativité de $*$.

Juste.
Déplacer les parenthèses sans changer l'ordre des facteurs, c'est exactement l'associativité.

Correction
C'est l'associativité :

$$x'' * (x * x') = (x'' * x) * x'.$$

Les trois facteurs restent dans le même ordre ; seules les parenthèses bougent. Sans associativité, la preuve s'arrête là.

Exemple : Sans associativité, deux symétriques

Sur $E = \{e, a, b\}$, on définit une loi $*$ par sa table : à la ligne x et à la colonne y, on lit $x * y$.

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	a

Le neutre est e. Or $a * a = e$ et $a * b = b * a = e$: a a deux symétriques, a et b. Ce n'est pas une contradiction, car la loi n'est pas associative : $(a * a) * b = b$, mais $a * (a * b) = a$.

Composer un élément avec lui-même

Définition : Itérés d'un élément

Soient $(E, *)$ un ensemble muni d'une loi de composition interne associative, de neutre e, et $x \in E$. On pose $x^0 = e$ et, pour tout entier naturel n, $x^{n+1} = x^n * x$. Ainsi $x^n = x * x * \cdots * x$ (n facteurs, $n \geq 1$). Si x est symétrisable, on pose $x^{-n} = (x')^n$ pour tout entier naturel n.

En notation additive, on écrit nx au lieu de x^n : $0x = 0$, $(n+1)x = nx + x$ et $(-n)x = n(-x)$.

Exemple : Itérés pour deux lois

- Avec $x * y = x + y - 4$, de neutre 4 : $7^2 = 7 * 7 = 10$, puis $7^3 = 10 * 7 = 13$, et $7^0 = 4$. Le symétrique de 7 est 1, donc $7^{-2} = 1 * 1 = -2$.
- Ici, 7^2 n'est pas le carré usuel 49 : c'est un itéré pour la loi $*$.
- Dans $(\mathbb{Z}/10\mathbb{Z}, +)$, on écrit $n\overline{a}$: $3\overline{4} = \overline{4} + \overline{4} + \overline{4} = \overline{2}$.

Les matrices carrées d'ordre 2 et 3

Des tableaux de nombres

Devine : Case par case

On additionne deux tableaux de même taille case par case. Que vaut $\begin{pmatrix} 3 & -1 \\ 2 & 0 \end{pmatrix} + \begin{pmatrix} -3 & 4 \\ 1 & 5 \end{pmatrix}$?

A. $\begin{pmatrix} 0 & 3 \\ 3 & 5 \end{pmatrix}$
Juste.
Chaque case est la somme des cases de même place : $3 + (-3) = 0$, $-1 + 4 = 3$, $2 + 1 = 3$ et $0 + 5 = 5$.

B. $\begin{pmatrix} 0 & 0 \\ 6 & 5 \end{pmatrix}$
Faux.

Tu as lu le second tableau colonne par colonne. La case de la ligne 1 et de la colonne 2 vaut $-1+4=3$.

C. Le nombre 11.

Faux.
11 est la somme de toutes les cases. Une somme de tableaux est encore un tableau de même taille.

Correction
On additionne les coefficients de même place :

$$\begin{pmatrix} 3+(-3) & -1+4 \\ 2+1 & 0+5 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 3 & 5 \end{pmatrix}.$$

Définition : Matrices carrées d'ordre 2 et 3 ; somme et produit par un réel

Soit $n \in \{2, 3\}$. Une **matrice carrée d'ordre** n à coefficients réels est un tableau $A = (a_{ij})$ de n^2 réels, où a_{ij} est placé à la ligne i et à la colonne j ($1 \leq i \leq n$, $1 \leq j \leq n$). Par exemple, pour $n = 2$: $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. On note $\mathcal{M}_2(\mathbb{R})$ et $\mathcal{M}_3(\mathbb{R})$ ces ensembles. Deux matrices de même ordre sont **égales** si elles ont les mêmes coefficients aux mêmes places.

Pour $A = (a_{ij})$ et $B = (b_{ij})$ dans $\mathcal{M}_n(\mathbb{R})$ et $\alpha \in \mathbb{R}$:

$$A + B = (a_{ij} + b_{ij}) \quad \text{et} \quad \alpha A = (\alpha a_{ij}).$$

La **matrice nulle** O a tous ses coefficients nuls ; on note $-A = (-a_{ij})$.

Exemple : Additionner et multiplier par un réel

Avec $A = \begin{pmatrix} 2 & -1 \\ 0 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 3 \\ -2 & 5 \end{pmatrix}$:

$$A + B = \begin{pmatrix} 3 & 2 \\ -2 & 9 \end{pmatrix},$$

$$3A = \begin{pmatrix} 6 & -3 \\ 0 & 12 \end{pmatrix},$$

$$-B = \begin{pmatrix} -1 & -3 \\ 2 & -5 \end{pmatrix}.$$

En ordre 3, c'est le même geste :

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

Multiplier ligne par colonne

Le produit des matrices ne se fait pas case par case. Son geste de base associe une ligne et une colonne : on multiplie terme à terme, puis on additionne.

La ligne $\begin{pmatrix} 2 & 3 \end{pmatrix}$ et la colonne $\begin{pmatrix} 4 \\ -1 \end{pmatrix}$ donnent $2 \times 4 + 3 \times (-1) = 5$.

Les matrices servent de support dans 11 des 14 exercices de structures consultés. Ce geste doit donc devenir sûr.

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. **Contrôler** l'ordre : les deux matrices sont toutes deux d'ordre 2, ou toutes deux d'ordre 3.
2. **Pour la case** (i, j) de AB, prendre la ligne i de A et la colonne j de B ; multiplier terme à terme, puis additionner.
3. **Écrire** chaque somme avant de l'effectuer.
4. **Garder l'ordre** : BA est un autre calcul, avec les lignes de B et les colonnes de A.

Rédaction attendue. On calcule le produit $\begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & -4 \end{pmatrix}$ case par case, en notant c_{ij} la case (i, j) du produit :

$$
\begin{aligned}
c_{11} &= 1 \times 2 + 2 \times 1 = 4,\\
c_{12} &= 1 \times 0 + 2 \times (-4) = -8,\\
c_{21} &= (-1) \times 2 + 3 \times 1 = 1,\\
c_{22} &= (-1) \times 0 + 3 \times (-4) = -12.
\end{aligned}
$$

Donc

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

À toi : Un produit d'ordre 3

Calcule AB, avec $A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 3 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}$.

Indice 1

La case $(1, 1)$ utilise la ligne 1 de A et la colonne 1 de B : $1 \times 2 + 0 \times 0 + 2 \times 1$.

Indice 2

Avance ligne par ligne : trois cases pour la ligne 1 de A, puis la ligne 2, puis la ligne 3.

Indice 3

Attention aux signes dans la ligne 2 de A.

Réponse

On calcule ligne par ligne, chaque case avec une ligne de A et une colonne de B.

Ligne 1 de A : $2 + 0 + 2 = 4$, $1 + 0 + 0 = 1$ et $0 + 0 + 2 = 2$.

Ligne 2 de A : $0 + 0 + 1 = 1$, $0 - 1 + 0 = -1$ et $0 + 1 + 1 = 2$.

Ligne 3 de A : $6 + 0 + 0 = 6$, $3 + 1 + 0 = 4$ et $0 - 1 + 0 = -1$.

Conclusion.

$$
AB = \begin{pmatrix} 4 & 1 & 2 \\ 1 & -1 & 2 \\ 6 & 4 & -1 \end{pmatrix}.
$$

Les règles du calcul matriciel

L'addition et le produit par un réel se font case par case. Chaque case obéit donc aux règles de calcul dans $\mathbb{R}$. Par exemple, $A + B = B + A$, car $a_{ij} + b_{ij} = b_{ij} + a_{ij}$ pour chaque place (i, j).

Pourquoi est-ce vrai pour toutes les règles ? La propriété suivante le démontre, case par case.

Propriété : Propriétés de l'addition des matrices et du produit par un réel

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

1. L'addition est une loi de composition interne sur $\mathcal{M}_n(\mathbb{R})$, associative et commutative ; O est son élément neutre, et toute matrice A a pour symétrique $-A$.
2. Pour tous réels α, β et toutes matrices A, B de $\mathcal{M}_n(\mathbb{R})$: $\alpha(A+B)=\alpha A+\alpha B$, $(\alpha+\beta)A=\alpha A+\beta A$, $\alpha(\beta A)=(\alpha\beta)A$ et $1A=A$.

Démonstration

Étape 1. Les deux opérations se font coefficient par coefficient : le coefficient de place (i,j) de $A+B$ est $a_{ij}+b_{ij}$, celui de αA est αa_{ij}. La somme de deux matrices d'ordre n est une matrice d'ordre n.

Étape 2 (point 1). Pour chaque place (i,j), les règles de calcul dans $\mathbb{R}$ donnent $(a_{ij}+b_{ij})+c_{ij}=a_{ij}+(b_{ij}+c_{ij})$, $a_{ij}+b_{ij}=b_{ij}+a_{ij}$, $a_{ij}+0=a_{ij}$ et $a_{ij}+(-a_{ij})=0$.

Étape 3 (point 2). De même, $\alpha(a_{ij}+b_{ij})=\alpha a_{ij}+\alpha b_{ij}$, $(\alpha+\beta)a_{ij}=\alpha a_{ij}+\beta a_{ij}$, $\alpha(\beta a_{ij})=(\alpha\beta)a_{ij}$ et $1\times a_{ij}=a_{ij}$.

Conclusion. Les deux membres de chaque égalité ont les mêmes coefficients aux mêmes places : ils sont égaux.

Devine : L'ordre compte-t-il ?

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

A. $AB=BA$, comme pour les réels.

Faux.
$AB=\begin{pmatrix}2&1\\1&0\end{pmatrix}$ et $BA=\begin{pmatrix}0&1\\1&2\end{pmatrix}$: ils diffèrent.

B. $AB\neq BA$.

Juste.
$AB=\begin{pmatrix}2&1\\1&0\end{pmatrix}$, alors que $BA=\begin{pmatrix}0&1\\1&2\end{pmatrix}$.

C. $AB=BA$ ici, car B ne contient que des 0 et des 1.

Faux.
Des coefficients simples n'y changent rien : la case $(1,1)$ vaut 2 dans AB et 0 dans BA.

Correction

On calcule ligne par colonne :

$$\begin{aligned}&AB\\&=\begin{pmatrix}1\times0+2\times1&1\times1+2\times0\\0\times0+1\times1&0\times1+1\times0\end{pmatrix}\\&=\begin{pmatrix}2&1\\1&0\end{pmatrix},\qquad BA=\begin{pmatrix}0&1\\1&2\end{pmatrix}.\end{aligned}$$

> **Conclusion.** $AB \neq BA$: le produit des matrices n'est pas commutatif.

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 $AB \neq BA$.

Démonstration

Idée de la preuve. On compare les coefficients de même place.

- **Neutre.** Le coefficient (i, j) de AI est $\sum_k a_{ik}\delta_{kj}$, où δ_{kj} vaut 1 si $k = j$ et 0 sinon : il vaut a_{ij}. De même pour IA.
- **Distributivité.** Le coefficient (i, j) de $A(B + C)$ est $\sum_k a_{ik}(b_{kj} + c_{kj}) = \sum_k a_{ik}b_{kj} + \sum_k a_{ik}c_{kj}$; de même à droite.
- **Produit par un réel.** Le coefficient (i, j) de $(\alpha A)B$ est $\sum_k (\alpha a_{ik})b_{kj} = \alpha \sum_k a_{ik}b_{kj}$; de même pour $A(\alpha B)$.
- **Associativité.** Le coefficient (i, j) de $(AB)C$ et celui de $A(BC)$ valent tous deux la somme des $a_{ik}b_{kl}c_{lj}$ sur tous les couples (k, l).
- **Non-commutativité.** Pour $n = 2$, $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ donnent $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $BA = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Pour $n = 3$, on complète ces matrices par des zéros.

Étapes omises : l'écriture détaillée des sommes doubles de l'associativité.

Attention : Ne pas permuter un produit

Avec $A = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix}$, on trouve $AB = \begin{pmatrix} 0 & 2 \\ 0 & 4 \end{pmatrix}$ et $BA = \begin{pmatrix} 1 & 1 \\ 3 & 3 \end{pmatrix}$.

Les identités remarquables changent donc : $(A + B)^2 = A^2 + AB + BA + B^2$, qui n'est pas égal à $A^2 + 2AB + B^2$ ici.

Un produit nul sans facteur nul

Devine : Un produit surprenant

Dans $\mathbb{R}$, $ab = 0$ impose $a = 0$ ou $b = 0$. Dans $\mathcal{M}_2(\mathbb{R})$, existe-t-il $A \neq O$ et $B \neq O$ telles que $AB = O$?

A. Non : la règle du produit nul reste vraie.

Faux.

Essaie $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$: $A \times A = O$, alors que $A \neq O$.

B. Seulement dans $\mathcal{M}_3(\mathbb{R})$.

Faux.

La matrice $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$, d'ordre 2, vérifie déjà $A \times A = O$.

C. Oui, cela arrive.

Juste.

Avec $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$, on a $A \neq O$ et pourtant $A \times A = O$.

Correction

Oui. Pour $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$, le calcul ligne par colonne donne

$$\begin{aligned} A \times A &= \begin{pmatrix} 1-1 & 1-1 \\ -1+1 & -1+1 \end{pmatrix} \\ &= O, \end{aligned}$$

alors que $A \neq O$.

Conclusion. La règle du produit nul de $\mathbb{R}$ ne passe pas aux matrices.

Attention : Ne pas simplifier par une matrice

Avec $A = \begin{pmatrix} 3 & 6 \\ 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} 4 & -6 \\ -2 & 3 \end{pmatrix}$, on calcule $AB = O$. Ainsi $AB = AO$, alors que $B \neq O$.

De $AB = AC$, on ne peut donc pas déduire $B = C$, même si $A \neq O$. On ne « divise » jamais par une matrice.

La section sur les anneaux dira quand une simplification est permise.

Groupes

Trois axiomes

Pour résoudre $x + 7 = 3$ dans $\mathbb{Z}$, tu ajoutes -7 des deux côtés, tu regroupes, puis 0 disparaît : $x = -4$.

Trois ingrédients ont servi : regrouper sans changer l'ordre, un élément qui ne change rien, un symétrique pour chaque élément. Ces trois ingrédients définissent un **groupe**.

Devine : Toujours une solution ?

Dans lequel de ces cadres l'équation $a * x = b$ a-t-elle une solution pour **tous** a et b de l'ensemble ?

A. $(\mathbb{Q}^*, \times)$

Juste.

Pour a et b rationnels non nuls, $x = \dfrac{b}{a}$ est un rationnel non nul, et $ax = b$.

B. $(\mathbb{N}, +)$

Faux.

$5 + x = 2$ donnerait $x = -3$, qui n'est pas un entier naturel.

C. $(\mathbb{Z}, \times)$

Faux.

$2x = 1$ donnerait $x = \dfrac{1}{2}$, qui n'est pas un entier.

Correction

Seul $(\mathbb{Q}^*, \times)$ convient : pour a et b rationnels non nuls, $x = \dfrac{b}{a}$ est rationnel et non nul.

Dans $(\mathbb{N}, +)$, $5 + x = 2$ n'a pas de solution ; dans $(\mathbb{Z}, \times)$, $2x = 1$ non plus. Il manque chaque fois des symétriques.

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 guidé : un groupe vérifié axiome par axiome

Soit $G = \mathbb{R} \setminus \{2\}$, muni de la loi de la découverte, $x * y = xy - 2x - 2y + 6$. On utilise

$$(x * y) - 2 = (x - 2)(y - 2),$$

vraie pour tous réels x et y, car $(x - 2)(y - 2) = xy - 2x - 2y + 4$.

Soient x, y et z dans G.

- **Loi interne.** Si $x \neq 2$ et $y \neq 2$, alors $(x - 2)(y - 2) \neq 0$, donc $x * y \in G$.

- **Associativité.** $(x * y) * z - 2 = (x-2)(y-2)(z-2) = x * (y * z) - 2$.
- **Neutre.** $3 \in G$ et $x * 3 = 3 * x = x$, car $(x * 3) - 2 = (x-2) \times 1$.
- **Symétrique.** $x' = 2 + \dfrac{1}{x-2}$ appartient à G, car $\dfrac{1}{x-2} \neq 0$; et $x * x' = x' * x = 3$.
- **Commutativité.** $x * y = y * x$.

Conclusion. $(G, *)$ est un groupe commutatif.

Calculer dans un groupe

Dans $(\mathbb{R}^*, \times)$, de $3x = 3y$ tu tires $x = y$: tu multiplies par l'inverse de 3. Dans $(\mathbb{R}, \times)$, qui n'est pas un groupe, c'est faux : $0 \times 1 = 0 \times 2$, et pourtant $1 \neq 2$.

Pourquoi est-ce vrai dans **tout** groupe ? Parce que chaque élément y a un symétrique.

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, $x = b * a'$.

Démonstration

Étape 1 (simplification à gauche). Si $a * x = a * y$, on compose à gauche par a' : $a' * (a * x) = a' * (a * y)$. Par associativité, $(a' * a) * x = (a' * a) * y$, soit $e * x = e * y$, donc $x = y$. À droite, on compose par a' à droite.

Étape 2 (existence). $a * (a' * b) = (a * a') * b = e * b = b$: $x = a' * b$ est solution.

Étape 3 (unicité). Si $a * x = b = a * (a' * b)$, l'étape 1 donne $x = a' * b$.

L'équation $x * a = b$ se traite de la même façon, à droite.

À retenir : Ce qu'il faut retenir de la preuve

On compose par le symétrique a', **du même côté** que a. Puis l'associativité regroupe $a' * a$, qui vaut e, et le neutre disparaît.

Pour l'unicité de la solution, on se ramène à la simplification déjà prouvée.

Vérifie : Le bon côté

Dans un groupe $(G, *)$ **non commutatif**, quelle est la solution de l'équation $a * x = b$?

A. $x = b * a'$

Faux.

Alors $a * x = a * b * a'$, qui n'a aucune raison de valoir b si la loi n'est pas commutative.

B. $x = a' * b$

Juste.

$a * (a' * b) = (a * a') * b = e * b = b$: on compose par a' à gauche, du côté de a.

C. $x = b * a$

Faux.

Le symétrique a' a disparu : $a * (b * a)$ ne se simplifie pas en b.

Correction

La solution est $x = a' * b$. On compose à gauche par a' : $a' * (a * x) = a' * b$. L'associativité donne alors $(a' * a) * x = e * x = x$.

Dans un groupe non commutatif, $b * a'$ est en général une autre valeur.

Exemple : Sans groupe, la simplification tombe

Dans $\mathbb{Z}/6\mathbb{Z}$ muni de la multiplication, qui n'est pas un groupe : $\overline{2} \times \overline{1} = \overline{2}$ et $\overline{2} \times \overline{4} = \overline{8} = \overline{2}$. Pourtant $\overline{1} \neq \overline{4}$: on ne simplifie pas par $\overline{2}$, qui n'a pas d'inverse.

De même, l'équation $\overline{2} \times x = \overline{1}$ n'a aucune solution : pour tout entier k, $2k - 1$ est impair, donc jamais multiple de 6.

Les ensembles de nombres usuels, eux, sont des groupes. **Pourquoi est-ce vrai ?** Leurs règles de calcul fournissent chaque axiome.

Les groupes de référence

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.

Démonstration

Étape 1 (point 1). Dans chacun de ces ensembles, la somme reste dans l'ensemble, l'addition est associative et commutative, 0 est neutre, et l'opposé $-x$ de x reste dans l'ensemble (règles de calcul dans $\mathbb{C}$).

Étape 2 (point 2). Un produit de deux nombres non nuls est non nul : le produit est une loi interne. Il est associatif et commutatif, 1 est neutre, et l'inverse $\dfrac{1}{x}$ d'un nombre non nul est non nul, rationnel si x l'est.

Étape 3 (point 3). C'est le contenu de la propriété « Opérations dans $\mathbb{Z}/n\mathbb{Z}$ » du chapitre d'arithmétique : addition associative et commutative, neutre $\overline{0}$, opposée $\overline{-a}$.

Étape 4 (point 4). C'est le point 1 de « Propriétés de l'addition des matrices et du produit par un réel ».

Exemple : Symétriques dans les groupes de référence

- Dans $(\mathbb{Z}/10\mathbb{Z}, +)$, l'opposé de $\overline{3}$ est $\overline{7}$, car $\overline{3} + \overline{7} = \overline{0}$.
- Dans $(\mathbb{C}^*, \times)$, l'inverse de $1+i$ est $\dfrac{1-i}{2}$, car $(1+i)(1-i) = 2$.
- Dans $(\mathcal{M}_2(\mathbb{R}), +)$, l'opposé de $\begin{pmatrix} 1 & -2 \\ 0 & 5 \end{pmatrix}$ est $\begin{pmatrix} -1 & 2 \\ 0 & -5 \end{pmatrix}$.

À l'examen, la structure de ces ensembles de référence est en général rappelée par l'énoncé. Ton travail : la **citer** au bon moment.

Le groupe des bijections

Petit rappel de 1BAC. Une application f de E dans E est **bijective** si tout y de E a exactement un antécédent x. Sa **réciproque** f^{-1} associe à y cet antécédent.

On a $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_E$, où l'identité id_E associe à chaque x lui-même. La composée de deux bijections est une bijection. Par exemple, sur $\mathbb{R}$, $f(x) = 2x - 1$ a pour réciproque $f^{-1}(y) = \dfrac{y+1}{2}$.

Les bijections de E forment-elles un groupe pour $\circ$? **Pourquoi est-ce vrai ?** Ces deux faits donnent la loi interne et les symétriques.

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}.

Démonstration

Étape 1 (loi interne). La composée de deux bijections de E sur E est une bijection de E sur E (rappel de 1BAC) : $\circ$ est une loi de composition interne sur $\mathcal{S}(E)$.

Étape 2 (associativité). Pour f, g, h dans $\mathcal{S}(E)$ et tout $x \in E$: $((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$.

Étape 3 (neutre). id_E est une bijection, et $f \circ \mathrm{id}_E = \mathrm{id}_E \circ f = f$.

Étape 4 (symétrique). La réciproque f^{-1} d'une bijection est une bijection de E sur E, et $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_E$ (rappel de 1BAC).

Vérifie : Composer dans les deux ordres

Sur $\mathbb{R}$, soient $f(x) = 2x$ et $g(x) = x + 3$, deux éléments de $\mathcal{S}(\mathbb{R})$. Que peut-on dire de $f \circ g$ et $g \circ f$?

A. Elles sont égales : $(\mathcal{S}(\mathbb{R}), \circ)$ est commutatif.

Faux.

$(f \circ g)(0) = f(3) = 6$, mais $(g \circ f)(0) = g(0) = 3$.

B. $f \circ g$ n'est pas une bijection.

Faux.

La composée de deux bijections est une bijection : $x \mapsto 2x + 6$ a pour réciproque $y \mapsto \dfrac{y - 6}{2}$.

C. Elles sont différentes : $(f \circ g)(x) = 2x + 6$ et $(g \circ f)(x) = 2x + 3$.

Juste.

$f(g(x)) = 2(x + 3)$ et $g(f(x)) = 2x + 3$: elles diffèrent en tout point.

Correction

$(f \circ g)(x) = 2x + 6$ et $(g \circ f)(x) = 2x + 3$. Ces deux bijections diffèrent.

$(\mathcal{S}(\mathbb{R}), \circ)$ est donc un groupe **non commutatif**.

Attention : L'ordre des symétriques

Sur $\mathbb{R}$, soient $f : x \mapsto 3x$ et $g : x \mapsto x - 2$. Alors, pour tout réel x, $(f \circ g)(x) = 3x - 6$, de réciproque $y \mapsto \dfrac{y}{3} + 2$.

C'est bien $g^{-1} \circ f^{-1}$, car $g^{-1}\left(f^{-1}(y)\right) = \dfrac{y}{3} + 2$. En revanche, $f^{-1}\left(g^{-1}(y)\right) = \dfrac{y + 2}{3}$, qui est différent.

Dans un groupe, le symétrique de $x * y$ est $y' * x'$, dans cet ordre.

Sous-groupes

Un groupe à l'intérieur d'un groupe

Devine : Une partie qui reste un groupe

On reste dans le groupe $(\mathbb{Z}, +)$. Laquelle de ces parties, munie de l'addition, est encore un groupe ?

A. $\mathbb{N}$, les entiers naturels

Faux.

0 est bien neutre, mais $3 \in \mathbb{N}$ n'a pas d'opposé dans $\mathbb{N}$: $-3 \notin \mathbb{N}$.

B. Les entiers impairs

Faux.

L'addition n'y est même pas interne : $3 + 5 = 8$ est pair.

C. $4\mathbb{Z}$, les multiples de 4

Juste.

$4k + 4m = 4(k + m)$, $0 = 4 \times 0$, et l'opposé de $4k$ est $4(-k)$: tout reste dans $4\mathbb{Z}$.

D. $\{-1, 0, 1\}$

Faux.

$1 + 1 = 2$ sort de la partie : elle n'est pas stable.

Indice 1

Pour chaque partie, fais trois tests. La somme reste-t-elle dedans ? 0 y est-il ? L'opposé y est-il ?

Indice 2

Un seul exemple qui sort de la partie suffit à l'éliminer.

Correction

Seule $4\mathbb{Z}$ passe les trois tests. Pour tous entiers k et m :

- $4k + 4m = 4(k + m)$;
- $0 = 4 \times 0$;
- $-(4k) = 4(-k)$.

L'associativité et la commutativité viennent de $\mathbb{Z}$.

Une partie d'un groupe qui reste un groupe pour la même loi s'appelle un **sous-groupe**.

Définition : Sous-groupe

Soient $(G, *)$ un groupe et H une partie de G. On dit que H est un **sous-groupe** de $(G, *)$ si H est stable pour $*$ et si H, muni de la loi induite, est un groupe.

Exemple : Exemple et contre-exemple dans $\mathbb{C}^*$

Dans le groupe $(\mathbb{C}^*, \times)$, prends $H = \{1, i, -1, -i\}$. Sa table montre que H est stable :

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

1 est neutre, et chaque ligne contient 1 : $i \times (-i) = 1$ et $(-1) \times (-1) = 1$. Donc H est un sous-groupe de $(\mathbb{C}^*, \times)$.

Contre-exemple. $H_1 = \{1, i, -i\}$ n'est pas stable : $i \times i = -1$ et $-1 \notin H_1$. Ce n'est pas un sous-groupe.

Un critère en deux points

Vérifier la stabilité et les trois axiomes de groupe pour chaque partie serait long. Or l'associativité vient gratuitement de G. Restent la stabilité, le neutre et les symétriques.

Le théorème suivant les réunit en un seul test : $x * y' \in H$. **Pourquoi est-ce vrai ?** Avec $x = y$, ce test fournit le neutre. Avec $x = e$, il fournit les symétriques.

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.

Démonstration

Sens direct. H contient son neutre e_H, donc $H \neq \emptyset$. Dans G, $e_H * e_H = e_H = e_H * e$; par « Règles de calcul dans un groupe », $e_H = e$. Si $y \in H$ et y_1 est son symétrique dans H, alors $y * y_1 = y_1 * y = e$, donc $y_1 = y'$ (« Symétrique pour une loi associative »). Ainsi $y' \in H$ et, H étant stable, $x * y' \in H$.

Réciproque. Étape 1. Soit $a \in H$: $e = a * a' \in H$. **Étape 2.** Pour $y \in H$: $y' = e * y' \in H$. **Étape 3.** Pour $x, y \in H$: $x * y = x * (y')' \in H$, donc H est stable. **Étape 4.** La loi induite est associative (« Propriétés héritées par une loi induite »), $e \in H$ est neutre, et tout $y \in H$ a son symétrique y' dans H.

À retenir : Ce qu'il faut retenir de la preuve

Un seul test, appliqué trois fois avec des choix malins. D'abord $x = y$ donne $e \in H$. Puis $x = e$ donne $y' \in H$. Enfin, y' à la place de y donne la stabilité, car $(y')' = y$. Choisir les bons éléments dans une propriété générale : garde ce réflexe de preuve.

Vérifie : L'étape 2 de la réciproque

Dans la réciproque, on sait déjà que $e \in H$. Comment obtient-on $y' \in H$ pour tout $y \in H$?

A. On applique la condition 2 avec $x = e$, car $e * y' = y'$.

Juste.
e et y sont dans H : la condition 2 donne $e * y' \in H$, et $e * y' = y'$.

B. H est stable pour $*$, donc $y' \in H$.

Faux.
La stabilité n'est établie qu'à l'étape 3, et elle utilise justement $y' \in H$: le raisonnement tournerait en rond.

C. $(G, *)$ est un groupe, donc y' existe.

Faux.
y' existe bien dans G. Mais rien ne dit encore qu'il est dans H : c'est tout l'enjeu.

Indice 1
Relis l'étape 1 : on y obtient $e \in H$.
Indice 2
Dans la condition 2, tu choisis librement x dans H.

Correction
On applique la condition 2 au couple (e, y), formé de deux éléments de H : $e * y' \in H$. Comme e est neutre, $e * y' = y'$, donc $y' \in H$.

La stabilité vient ensuite, à l'étape 3.

Exemple : Contre-exemple : la partie vide

La condition 2 ne dit rien d'une partie vide : il n'y a aucun couple à tester. La partie $\emptyset$ la vérifie donc. Pourtant $\emptyset$ n'est pas un sous-groupe, car un groupe contient au moins son neutre.

La condition 1, $H \neq \emptyset$, est donc indispensable. En pratique, on la prouve en montrant que $e \in H$.

Ce critère suffit pour les sous-groupes à connaître. **Pourquoi est-ce vrai** pour $n\mathbb{Z}$, $\mathbb{U}$ et $\mathbb{R}_+^*$? Chaque fois, $x * y'$ se calcule en une ligne.

Les sous-groupes à connaître

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 $(\mathbb{R}^*, \times)$.

Démonstration

On applique « Caractérisation d'un sous-groupe » dans chaque groupe de « Groupes de référence ».

Étape 1 (point 1). $0 = n \times 0 \in n\mathbb{Z}$. Pour nk et nk_1 dans $n\mathbb{Z}$: $nk + (-nk_1) = n(k - k_1)$ et $k - k_1 \in \mathbb{Z}$.

Étape 2 (point 2). $1 \in \mathbb{U}$, et $\mathbb{U} \subset \mathbb{C}^*$ car $|0| = 0$. Pour $z, w \in \mathbb{U}$: $\left|z \times w^{-1}\right| = \dfrac{|z|}{|w|} = 1$.

Étape 3 (point 3). $1 > 0$. Pour $x > 0$ et $y > 0$: $x \times y^{-1} = \dfrac{x}{y} > 0$.

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

Cette rédaction sert dans 10 des 14 exercices de structures consultés. **Montrer que** $H = \{a + b\sqrt{3} \ / \ (a, b) \in \mathbb{Z}^2\}$ est un sous-groupe de $(\mathbb{R}, +)$.

1. **Placer H dans un groupe connu.** Tout $a + b\sqrt{3}$ est réel : $H \subset \mathbb{R}$, et $(\mathbb{R}, +)$ est un groupe.
2. **Le neutre.** $0 = 0 + 0\sqrt{3}$, donc $0 \in H$ et $H \neq \emptyset$.
3. **Le test.** Soient $x = a + b\sqrt{3}$ et $y = c + d\sqrt{3}$ dans H. Le symétrique de y est $-y$, et $x + (-y) = (a - c) + (b - d)\sqrt{3}$, avec $a - c$ et $b - d$ entiers. Donc $x - y \in H$.
4. **Conclure.** « D'après la caractérisation d'un sous-groupe, H est un sous-groupe de $(\mathbb{R}, +)$. L'addition étant commutative, $(H, +)$ est un groupe commutatif. »

À toi : les puissances de 2

Montre que $H_2 = \{2^k \ / \ k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{R}^*, \times)$. Rédige comme dans la méthode.

Indice 1
Le neutre de $(\mathbb{R}^*, \times)$ est 1 : écris-le sous la forme 2^k.
Indice 2
Ici, le symétrique de y est son inverse y^{-1}. Calcule $x \times y^{-1}$ pour $x = 2^k$ et $y = 2^m$.

Réponse
Groupe de référence. Tout 2^k est un réel non nul : $H_2 \subset \mathbb{R}^*$, et $(\mathbb{R}^*, \times)$ est un groupe.

Neutre. $1 = 2^0$, donc $1 \in H_2$ et $H_2 \neq \emptyset$.

Test. Soient $x = 2^k$ et $y = 2^m$, avec k et m entiers. Le symétrique de y dans $(\mathbb{R}^*, \times)$ est $y^{-1} = 2^{-m}$. Alors :

$$x \times y^{-1} = 2^{k-m},$$

avec $k - m \in \mathbb{Z}$: $x \times y^{-1} \in H_2$.

Conclusion. D'après la caractérisation d'un sous-groupe, H_2 est un sous-groupe de $(\mathbb{R}^*, \times)$: $(H_2, \times)$ est un groupe commutatif.

Attention : Stable et contenant le neutre ne suffit pas

Dans $(\mathbb{R}^*, \times)$, prends $H_3 = [1, +\infty[$. Il contient le neutre 1. Il est stable : si $x \geq 1$ et $y \geq 1$, alors $xy \geq 1$.

Pourtant ce n'est pas un sous-groupe : $3 \in H_3$, mais son inverse $\dfrac{1}{3} \notin H_3$.

Le test porte sur $x * y'$, avec le **symétrique** de y, et non sur $x * y$.

Homomorphismes et isomorphismes

Une application qui respecte les lois

Devine : Changer une somme en produit

On cherche une application f de $\mathbb{R}$ dans $\mathbb{R}$ telle que $f(x+y) = f(x) \times f(y)$ pour tous réels x et y. Laquelle convient ? Ici, e^x désigne l'exponentielle de x : la lettre e n'y est pas un neutre.

A. $f(x) = 3x$

Faux.
$f(1+1) = 6$, alors que $f(1) \times f(1) = 9$.

B. $f(x) = x^3$

Faux.
$f(1+1) = 8$, alors que $f(1) \times f(1) = 1$.

C. $f(x) = 3 + x$

Faux.
$f(0+0) = 3$, alors que $f(0) \times f(0) = 9$.

D. $f(x) = e^{3x}$

Juste.
$e^{3(x+y)} = e^{3x+3y} = e^{3x} \times e^{3y}$: c'est la règle de l'exponentielle.

Indice 1

Teste chaque proposition avec des valeurs simples, comme $x = y = 1$ ou $x = y = 0$.

Indice 2

Quelle fonction de référence change une somme en produit ?

Correction

Pour tous réels x et y :

$$e^{3(x+y)} = e^{3x} \times e^{3y}.$$

Les trois autres échouent dès $x = y = 1$ ou $x = y = 0$.

Une telle application transporte l'addition sur la multiplication. On dit que c'est un **homomorphisme** de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.

En clair. Un homomorphisme f change un composé au départ en composé à l'arrivée : $f(x * y) = f(x) \top f(y)$. Les deux lois peuvent différer, comme $+$ et $\times$ pour l'exponentielle. Les sujets d'examen notent ces lois $*$ et $\top$, comme l'énoncé suivant.

Petit rappel de 1BAC. Une application f de E dans F est **injective** si deux éléments distincts ont des images distinctes : tout u de F a au plus un antécédent. Elle est **surjective** si tout u de F a au moins un antécédent. Elle est **bijective** si elle est les deux : l'équation $f(x) = u$ a alors une seule solution. La réciproque f^{-1} a été rappelée avec le groupe des bijections.

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 :
$$\forall x \in E,\ \forall y \in E, \quad f(x * y) = f(x) \top f(y).$$
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. L'application $f : \theta \mapsto e^{i\theta}$ va de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$. Pour tous réels θ et θ_1 :
$$e^{i(\theta+\theta_1)} = e^{i\theta} \times e^{i\theta_1},$$
donc f est un homomorphisme. Ce n'est pas un isomorphisme, car $f(0) = f(2\pi) = 1$: f n'est pas injective.

Contre-exemple. L'application $g : x \mapsto x + 1$, de $(\mathbb{R}, +)$ dans $(\mathbb{R}, +)$, n'est pas un homomorphisme : $g(0 + 0) = 1$, alors que $g(0) + g(0) = 2$.

Isomorphismes et réciproques

Vérifie : Un isomorphisme ?

L'application $f : x \mapsto e^{3x}$ est-elle un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$? Quel raisonnement est juste ?

A. Oui : f est un homomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$, et cela suffit.

Faux.
Un homomorphisme n'est pas forcément bijectif : $\theta \mapsto e^{i\theta}$ en est un exemple. Il manque la bijectivité.

B. Oui : f est un homomorphisme, et $e^{3x} = u$ a une seule solution pour tout $u > 0$.

Juste.
Les deux conditions de la définition sont vérifiées : homomorphisme et bijection, avec $x = \dfrac{\ln u}{3}$.

C. Non : un isomorphisme exige la même loi au départ et à l'arrivée.

Faux.
Rien n'oblige les deux lois à être les mêmes : la définition parle de $*$ au départ et de $\top$ à l'arrivée.

Indice 1
Un isomorphisme est un homomorphisme **bijectif** : il y a deux choses à vérifier.
Indice 2
Résous $e^{3x} = u$ pour $u > 0$.

Correction
Homomorphisme. Pour tous réels x et y, $e^{3(x+y)} = e^{3x} \times e^{3y}$: f est un homomorphisme.

Bijectivité. Soit $u > 0$. L'équation $e^{3x} = u$ équivaut à $3x = \ln u$, soit $x = \dfrac{\ln u}{3}$: une seule solution. Donc f est bijective.

Conclusion. f est un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$.

Sa réciproque respecte-t-elle encore les lois ? **Pourquoi est-ce vrai ?** On applique f, puis on lit l'égalité à l'envers.

Propriété : Composée et réciproque d'homomorphismes

Soient $(E, *)$, $(F, \top)$ et $(L, \star)$ trois ensembles munis chacun d'une loi de composition interne.

1. Si f est un homomorphisme de $(E, *)$ dans $(F, \top)$ et g un homomorphisme de $(F, \top)$ dans $(L, \star)$, alors $g \circ f$ est un homomorphisme de $(E, *)$ dans $(L, \star)$.
2. Si f est un isomorphisme de $(E, *)$ sur $(F, \top)$, alors sa réciproque f^{-1} est un isomorphisme de $(F, \top)$ sur $(E, *)$.

Démonstration
Étape 1 (point 1). Pour x, y dans E : $(g \circ f)(x * y) = g\big(f(x) \top f(y)\big) = g(f(x)) \star g(f(y))$, car f puis g sont des homomorphismes.

Étape 2 (point 2). La réciproque f^{-1} d'une bijection est une bijection de F sur E (rappel de 1BAC). Soient u, v dans F ; on pose $x = f^{-1}(u)$ et $y = f^{-1}(v)$. Comme f est un homomorphisme, $f(x * y) = f(x) \top f(y) = u \top v$.

Conclusion. En appliquant f^{-1} : $f^{-1}(u \top v) = x * y = f^{-1}(u) * f^{-1}(v)$.

Exemple : composer et inverser

La réciproque de $x \mapsto e^{3x}$ est $u \mapsto \dfrac{\ln u}{3}$. D'après l'énoncé sur la composée et la réciproque, c'est un isomorphisme de $(\mathbb{R}_+^*, \times)$ sur $(\mathbb{R}, +)$. On retrouve, pour tous $u > 0$ et $v > 0$:

$$\frac{\ln(uv)}{3} = \frac{\ln u}{3} + \frac{\ln v}{3}.$$

Compose aussi $x \mapsto e^x$, de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$, avec $u \mapsto u^2$, de $(\mathbb{R}_+^*, \times)$ dans lui-même. La composée $x \mapsto e^{2x}$ est un homomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.

Rédiger la preuve

Méthode : montrer qu'une application est un isomorphisme

Pour x réel, on pose $T(x) = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix}$, et on note ici $E = \{T(x) \ / \ x \in \mathbb{R}\}$. **Montrer que** $f : x \mapsto T(x)$ est un isomorphisme de $(\mathbb{R}, +)$ sur $(E, \times)$.

1. **Nommer** les structures : $f : (\mathbb{R}, +) \to (E, \times)$.
2. **Calculer les deux membres.** Soient x et y réels. $f(x) \times f(y) = \begin{pmatrix} 1 & 2y + 2x \\ 0 & 1 \end{pmatrix} = T(x + y) = f(x + y)$: f est un homomorphisme.
3. **Bijectivité.** Tout élément de E s'écrit $T(x)$: f est surjective. Si $T(x) = T(y)$, alors $2x = 2y$, donc $x = y$: f est injective.
4. **Conclure** : « f est un homomorphisme bijectif, donc un isomorphisme de $(\mathbb{R}, +)$ sur $(E, \times)$. »

À toi : un isomorphisme vers $(\mathbb{R}, +)$

Sur $\mathbb{R}$, on pose $x \top y = x + y + 5$. Montre que $g : x \mapsto x + 5$ est un isomorphisme de $(\mathbb{R}, \top)$ sur $(\mathbb{R}, +)$. Rédige comme dans la méthode.

Indice 1
Nomme les structures : $g : (\mathbb{R}, \top) \to (\mathbb{R}, +)$.
Indice 2
Calcule séparément $g(x \top y)$ et $g(x) + g(y)$.
Indice 3
Pour la bijectivité, résous $x + 5 = u$.

Réponse
Homomorphisme. Soient x et y deux réels quelconques. D'une part, $g(x \top y) = (x + y + 5) + 5 = x + y + 10$. D'autre part, $g(x) + g(y) = (x + 5) + (y + 5) = x + y + 10$.

Donc $g(x \top y) = g(x) + g(y)$: g est un homomorphisme de $(\mathbb{R}, \top)$ dans $(\mathbb{R}, +)$.

Bijectivité. Pour tout réel u, l'équation $x + 5 = u$ a une seule solution, $x = u - 5$: g est bijective.

Conclusion. g est un isomorphisme de $(\mathbb{R}, \top)$ sur $(\mathbb{R}, +)$.

Attention : Un homomorphisme qui n'est pas bijectif

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

Ce n'est pas un isomorphisme : $|-5| = |5| = 5$, et -2 n'a aucun antécédent. N'écris jamais « isomorphisme » sans avoir prouvé la bijectivité.

Ici, le transfert ne donne une structure que sur l'image, $\mathbb{R}_+^*$.

Transfert de structure

Une structure qui voyage

Devine : Un symétrique sans calcul

On reprend $E = \{T(x) \ / \ x \in \mathbb{R}\}$, avec $T(x) = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix}$, et l'isomorphisme $f : x \mapsto T(x)$ de $(\mathbb{R}, +)$ sur $(E, \times)$. Quel est le symétrique de $T(5)$ dans $(E, \times)$?

A. $T\left(\frac{1}{5}\right)$

Faux.
$T(5) \times T\left(\frac{1}{5}\right) = T\left(\frac{26}{5}\right) \neq I$: il faut l'opposé de 5, pas son inverse.

B. $T(-5)$

Juste.
$T(5) \times T(-5) = T(0) = I$, et de même dans l'autre ordre.

C. $-T(5)$

Faux.
$-T(5)$ a des coefficients diagonaux égaux à -1 : ce n'est même pas un élément de E.

D. $T(5)$

Faux.
$T(5) \times T(5) = T(10) \neq I$.

Indice 1
Le symétrique de 5 dans $(\mathbb{R}, +)$ est -5.
Indice 2
Utilise $T(x) \times T(y) = T(x + y)$ et $T(0) = I$.

Correction
Comme $T(x) \times T(y) = T(x + y)$ pour tous réels x et y :

$$\begin{aligned} & T(5) \times T(-5) \\ & = T(-5) \times T(5) \\ & = T(0) = I. \end{aligned}$$

Le symétrique de $T(5)$ est donc $T(-5)$, l'image du symétrique de 5. Le calcul dans E se ramène à un calcul dans $\mathbb{R}$.

L'activité montre l'idée : f transporte chaque calcul de $\mathbb{R}$ dans E. Un homomorphisme ou un transport de structure figure dans 13 des 14 exercices de structures consultés.

Pourquoi est-ce vrai ? Tout élément de l'image s'écrit $f(x)$. L'égalité $f(x) \top f(y) = f(x * y)$ ramène alors chaque axiome à un calcul dans G.

Le théorème de transfert

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.

Démonstration

Tout élément de $f(G)$ s'écrit $f(x)$ avec $x \in G$.

Étape 1 (stabilité). $f(x) \top f(y) = f(x * y)$ et $x * y \in G$: donc $f(x) \top f(y) \in f(G)$.

Étape 2 (associativité). $\big(f(x) \top f(y)\big) \top f(z) = f\big((x * y) * z\big) = f\big(x * (y * z)\big) = f(x) \top \big(f(y) \top f(z)\big)$.

Étape 3 (neutre). $f(e) \top f(x) = f(e * x) = f(x)$ et $f(x) \top f(e) = f(x * e) = f(x)$.

Étape 4 (symétrique). $f(x) \top f(x') = f(x * x') = f(e)$ et $f(x') \top f(x) = f(e)$; ce symétrique est unique (« Symétrique pour une loi associative », la loi étant associative sur $f(G)$ par l'étape 2).

Étape 5. Si $*$ est commutative : $f(x) \top f(y) = f(x * y) = f(y * x) = f(y) \top f(x)$. Si f est surjective, $f(G) = F$.

À retenir : Ce qu'il faut retenir de la preuve

On ne vérifie rien directement dans F. On écrit chaque élément de $f(G)$ sous la forme $f(x)$, on calcule dans G, puis on revient par f. La surjectivité ne sert qu'à la fin, pour dire que $f(G) = F$.

Vérifie : L'hypothèse du point 3

Le point 3 conclut que $(F, \top)$ tout entier est un groupe. Quelle hypothèse sur f permet de passer de $f(G)$ à F ?

A. f est injective.

Faux.
L'injectivité dit que deux éléments distincts ont des images distinctes. Elle ne dit pas que tout élément de F est atteint.

B. $(G, *)$ est commutatif.

Faux.
La commutativité sert au point 2, pour être transportée. Elle ne dit rien de $f(G)$.

C. f est surjective.

Juste.
Si f est surjective, $f(G) = F$: le groupe $f(G)$ du point 1 est F tout entier.

Indice 1
Le point 1 donne un groupe : lequel ?
Indice 2
Quelle propriété de f dit que $f(G) = F$?

Correction
Le point 1 prouve que $(f(G), \top)$ est un groupe. Pour conclure sur F, il faut $f(G) = F$, c'est-à-dire f surjective (étape 5).

L'injectivité n'est pas demandée : un homomorphisme surjectif suffit.

Exemple : Contre-exemple : l'image n'est pas tout

L'application $x \mapsto e^x$ est un homomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}, \times)$. Pourtant $(\mathbb{R}, \times)$ n'est pas un groupe : 0 n'a pas d'inverse.

Aucune contradiction : l'application n'est pas surjective. Le transfert donne seulement le groupe $(\mathbb{R}_+^*, \times)$, image de $\mathbb{R}$.

Remarque aussi : $e^0 = 1$ et, pour tout réel x, $e^{-x} = \dfrac{1}{e^x}$. Le neutre et les symétriques se correspondent. Est-ce toujours vrai entre deux groupes ? **Pourquoi est-ce vrai ?** Tout repose sur la simplification dans un groupe.

Entre deux groupes

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 $(G_1, \top)$.

Démonstration

Étape 1. $f(e) \top f(e) = f(e * e) = f(e) = f(e) \top e_1$. Par « Règles de calcul dans un groupe », appliquées dans G_1, on simplifie par $f(e)$: $f(e) = e_1$.

Étape 2. $f(x) \top f(x') = f(x * x') = f(e) = e_1$ et de même $f(x') \top f(x) = e_1$. Le symétrique de $f(x)$ dans G_1 est donc $f(x')$ (« Symétrique pour une loi associative »).

Étape 3 (point 2). $f(G)$ contient $e_1 = f(e)$. Pour $f(x)$ et $f(y)$ dans $f(G)$, le symétrique de $f(y)$ est $f(y')$, et $f(x) \top f(y') = f(x * y') \in f(G)$. On conclut par « Caractérisation d'un sous-groupe ».

À retenir : Ce qu'il faut retenir de la preuve

Pour prouver $f(e) = e_1$, on écrit le même élément de deux façons : $f(e) \top f(e)$ et $f(e) \top e_1$. On simplifie ensuite dans le groupe G_1. Retiens ce geste : deux écritures d'un même élément, puis une simplification.

Vérifie : Le droit de simplifier

À l'étape 1, on passe de $f(e) \top f(e) = f(e) \top e_1$ à $f(e) = e_1$. Qu'est-ce qui justifie cette simplification ?

A. $(G_1, \top)$ est un groupe : on compose à gauche par le symétrique de $f(e)$.
Juste.
C'est la règle de simplification dans un groupe, appliquée dans G_1.

B. f est injective.
Faux.
L'énoncé ne suppose pas f injective, et la simplification se fait dans G_1, pas par f.

C. La loi $\top$ est commutative.
Faux.
On simplifie du même côté, à gauche : la commutativité est inutile, et elle n'est pas supposée.

D. $f(e) \neq e_1$.
Faux.
C'est le contraire de ce qu'on veut prouver, et ce n'est pas une hypothèse.

Indice 1
La règle de simplification vaut dans un groupe.
Indice 2
Dans quel ensemble vit $f(e)$?

Correction
$f(e)$ est un élément du groupe $(G_1, \top)$: il a un symétrique dans G_1. En composant à gauche par ce symétrique, on obtient $f(e) = e_1$ (règles de calcul dans un groupe).

Aucune injectivité n'est utilisée.

Exemple : Contre-exemple : l'arrivée n'est pas un groupe

L'application nulle $g : n \mapsto 0$ va de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, \times)$. Pour tous entiers n et m, elle vérifie :

$$\begin{aligned} g(n+m) &= 0 = 0 \times 0 \\ &= g(n) \times g(m), \end{aligned}$$

donc c'est un homomorphisme. Pourtant $g(0) = 0$, alors que le neutre de $\times$ est 1.

L'énoncé ne s'applique pas : $(\mathbb{Z}, \times)$ n'est pas un groupe, car 2 n'a pas d'inverse dans $\mathbb{Z}$.

Rédiger un transfert

Méthode : transférer une structure de groupe

Montrer que $(E, \times)$ est un groupe commutatif, avec $E = \{T(x) \ / \ x \in \mathbb{R}\}$.

1. **Le groupe de départ.** $(\mathbb{R}, +)$ est un groupe commutatif, de neutre 0.
2. **L'homomorphisme.** $f : x \mapsto T(x)$ vérifie $f(x+y) = f(x) \times f(y)$ (méthode de la section précédente).
3. **La surjectivité.** Par définition de E, tout élément de E est un $T(x)$: $f(\mathbb{R}) = E$.
4. **Conclure.** « Par transfert de structure, $(E, \times)$ est un groupe commutatif. Son neutre est $f(0) = I$, et le symétrique de $T(x)$ est $T(-x)$. » La stabilité de E pour $\times$ est comprise dans le théorème.

À toi : Coin examen : une loi sur un intervalle

Sur $D =]1, +\infty[$, on pose $x * y = xy - x - y + 2$, une loi déjà rencontrée dans le chapitre. Rédige chaque réponse avant d'ouvrir la correction. Barème indicatif BURHAN.

- **Q1.** Montrer que $*$ est une loi de composition interne sur D.

- **Q2.** Pour $t > 0$, on pose $f(t) = t + 1$. Montrer que f est un homomorphisme de $(\mathbb{R}_+^*, \times)$ dans $(D, *)$.
- **Q3.** Montrer que f est une bijection de $\mathbb{R}_+^*$ sur D.
- **Q4.** En déduire que $(D, *)$ est un groupe commutatif, et préciser son neutre.
- **Q5.** Déterminer le symétrique d'un élément x de D.

Indice 1
Q1 : factorise $(x * y) - 1$.
Indice 2
Q2 : vérifie d'abord que $f(t) \in D$, puis calcule $f(t) * f(s)$.
Indice 3
Q4 : nomme le groupe de départ, l'homomorphisme et sa surjectivité.

Réponse
Q1. Soient x et y quelconques dans D. On a :

$$\begin{aligned} x * y &= (x-1)(y-1) \\ &\quad + 1. \end{aligned}$$

Or $x - 1 > 0$ et $y - 1 > 0$, donc $x * y > 1$. Ainsi $*$ est une loi de composition interne sur D. **0,5 pt**

Q2. Pour $t > 0$, $f(t) = t + 1 > 1$, donc $f(t) \in D$. Soient t et s quelconques dans $\mathbb{R}_+^*$. D'après Q1 :

$$\begin{aligned} &f(t) * f(s) \\ &= (t + 1 - 1)(s + 1 - 1) \\ &\quad + 1 \\ &= ts + 1 = f(ts). \end{aligned}$$

Donc f est un homomorphisme de $(\mathbb{R}_+^*, \times)$ dans $(D, *)$. **0,5 pt**

Q3. Soit $u \in D$. L'équation $t + 1 = u$ a une seule solution, $t = u - 1$, et $u - 1 > 0$. Donc f est une bijection de $\mathbb{R}_+^*$ sur D. **0,5 pt**

Q4. $(\mathbb{R}_+^*, \times)$ est un groupe commutatif, et f est un homomorphisme surjectif de $(\mathbb{R}_+^*, \times)$ dans $(D, *)$. Par transfert de structure, $(D, *)$ est un groupe commutatif, de neutre $f(1) = 2$. **0,5 pt**

Q5. Soit $x \in D$; on a $x = f(t)$ avec $t = x - 1$. Par transfert, son symétrique est $f(t^{-1})$:

$$\begin{aligned} f(t^{-1}) &= f\left(\frac{1}{x-1}\right) \\ &= \frac{x}{x-1}. \end{aligned}$$

0,5 pt

Anneaux

Deux lois sur un même ensemble

Devine : Les règles des nombres, chez les matrices

Ici, A, B et C désignent des matrices de $\mathcal{M}_2(\mathbb{R})$. Laquelle de ces règles est vraie pour **toutes** les matrices A, B et C ?

A. $AB = BA$

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

B. $A(B + C) = AB + AC$

Juste.
C'est la distributivité du produit par rapport à l'addition, vraie dans $\mathcal{M}_2(\mathbb{R})$.

C. Si $AB = O$, alors $A = O$ ou $B = O$.

Faux.
Avec $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, on a $AB = O$, alors que $A \neq O$ et $B \neq O$.

D. $(A + B)^2 = A^2 + 2AB + B^2$

Faux.
En développant, $(A + B)^2 = A^2 + AB + BA + B^2$. L'égalité demande $AB = BA$, faux en général.

Indice 1
Pour réfuter une règle, un seul couple de matrices suffit.
Indice 2
Essaie des matrices avec beaucoup de zéros.

Correction
Seule la distributivité est toujours vraie. Le produit des matrices n'est pas commutatif, et un produit peut être nul sans facteur nul.

Ces matrices ont donc des règles moins confortables que les nombres. Une structure à deux lois de ce type s'appelle un **anneau**.

En clair. Un anneau est un ensemble muni de deux lois. La première, notée $+$, en fait un groupe commutatif. La seconde, notée $\times$, est associative et distributive par rapport à la première.

Les sujets écrivent aussi $(E, *, \top)$: la loi $*$ y joue le rôle de $+$, et la loi $\top$ celui de $\times$. Dans cette section, A désigne un anneau, sauf mention contraire.

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. $(2\mathbb{Z}, +, \times)$ est un anneau commutatif. $(2\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$, le produit de deux entiers pairs est pair, et les règles de $\mathbb{Z}$ s'appliquent. Il n'est pas unitaire : si $u \in 2\mathbb{Z}$ était neutre pour $\times$, on aurait $u \times 2 = 2$, donc $u = 1$, qui est impair.

Contre-exemple. $(\mathbb{N}, +, \times)$ n'est pas un anneau : $(\mathbb{N}, +)$ n'est pas un groupe, car 1 n'a pas d'opposé dans $\mathbb{N}$.

Dans tout anneau, $x \times 0 = 0$. **Pourquoi est-ce vrai ?** Parce que $0 = 0 + 0$ et que $\times$ est distributive.

Calculer et reconnaître un anneau

Propriété : Règles de calcul dans un anneau

Soit $(A, +, \times)$ un anneau. Pour tous x et y de A :

1. $x \times 0 = 0 \times x = 0$;
2. $(-x) \times y = x \times (-y) = -(x \times y)$;
3. $(-x) \times (-y) = x \times y$.

Démonstration

Étape 1 (point 1). Par distributivité, $x \times 0 = x \times (0 + 0) = x \times 0 + x \times 0$. On ajoute $-(x \times 0)$ aux deux membres : $0 = x \times 0$. De même, $0 \times x = 0$.

Étape 2 (point 2). Par distributivité et le point 1, $x \times y + (-x) \times y = \big(x + (-x)\big) \times y = 0 \times y = 0$. Donc $(-x) \times y$ est l'opposé de $x \times y$ (« Symétrique pour une loi associative »). De même pour $x \times (-y)$.

Étape 3 (point 3). Le point 2, appliqué deux fois, donne $(-x) \times (-y) = -\big(x \times (-y)\big) = -\big(-(x \times y)\big) = x \times y$, car l'opposé de l'opposé est l'élément lui-même.

> **Vérifie : Des signes modulo 12**

Dans l'anneau $(\mathbb{Z}/12\mathbb{Z}, +, \times)$, que vaut $(-\overline{3}) \times (-\overline{5})$?

A. $\overline{9}$

Faux.
C'est $-(\overline{3} \times \overline{5}) = -\overline{15} = \overline{9}$: tu as oublié que le produit de deux opposés est le produit des éléments.

B. $\overline{4}$

Faux.
Tu as additionné : $(-\overline{3}) + (-\overline{5}) = -\overline{8} = \overline{4}$. Ici, on multiplie.

C. $\overline{3}$

Juste.
$(-\overline{3}) \times (-\overline{5}) = \overline{3} \times \overline{5} = \overline{15} = \overline{3}$.

Indice 1
Une règle de calcul dans un anneau dit ce que vaut $(-x) \times (-y)$.
Indice 2
Réduis ensuite 15 modulo 12.

Correction
D'après les règles de calcul dans un anneau, point 3 :

$$\begin{aligned}(-\overline{3}) \times (-\overline{5}) &= \overline{3} \times \overline{5} \\ &= \overline{15}.\end{aligned}$$

Or $15 = 12 + 3$, donc le résultat est $\overline{3}$. Contrôle avec d'autres représentants : $-\overline{3} = \overline{9}$, $-\overline{5} = \overline{7}$, et $9 \times 7 = 63 = 5 \times 12 + 3$.

Une partie d'un anneau connu peut-elle hériter de sa structure ? **Pourquoi est-ce vrai ?** Les axiomes de $\times$ sont déjà vrais dans le grand anneau.

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 $1 \in B$.

Démonstration

Étape 1. B est un sous-groupe de $(A, +)$: $(B, +)$ est un groupe. Il est commutatif, car la loi $+$ l'est sur A (« Propriétés héritées par une loi induite »).

Étape 2. B est stable pour $\times$: la loi induite est une loi de composition interne sur B. Elle est associative, et distributive par rapport à $+$, par la même propriété.

Étape 3. Si $\times$ est commutative sur A, elle l'est sur B. Si $1 \in B$, alors $1 \times b = b \times 1 = b$ pour tout $b \in B$: 1 est l'unité de B.

Méthode : montrer qu'un ensemble est un anneau

Un anneau est à démontrer dans 6 des 14 exercices de structures consultés. **Montrer que** $(H, +, \times)$ est un anneau commutatif unitaire, avec $H = \{a + b\sqrt{3} \ / \ (a, b) \in \mathbb{Z}^2\}$.

1. **L'anneau de référence.** $H \subset \mathbb{R}$, et $(\mathbb{R}, +, \times)$ est un anneau commutatif unitaire.
2. **Le sous-groupe.** H est un sous-groupe de $(\mathbb{R}, +)$: c'est la méthode des sous-groupes.
3. **La stabilité pour $\times$.** $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$, avec $ac + 3bd$ et $ad + bc$ entiers.
4. **L'unité.** $1 = 1 + 0\sqrt{3}$, donc $1 \in H$.
5. **Conclure** : « D'après l'anneau induit sur une partie, $(H, +, \times)$ est un anneau commutatif unitaire. »

À toi : les entiers de Gauss

Montre que $(B, +, \times)$ est un anneau commutatif unitaire, avec $B = \{a + ib \ / \ (a, b) \in \mathbb{Z}^2\}$. Rédige comme dans la méthode.

Indice 1
L'anneau de référence est $(\mathbb{C}, +, \times)$.
Indice 2
Pour le sous-groupe, calcule $x - y$; pour la stabilité, développe $(a + ib)(c + id)$.
Indice 3
N'oublie pas l'unité : 1 est-il dans B ?

Réponse
$B \subset \mathbb{C}$, et $(\mathbb{C}, +, \times)$ est un anneau commutatif unitaire.

Sous-groupe. $0 = 0 + 0i$, donc $0 \in B$. Soient $x = a + ib$ et $y = c + id$ quelconques dans B. Alors $x - y = (a - c) + i(b - d)$, avec $a - c$ et $b - d$ entiers : $x - y \in B$. Donc B est un sous-groupe de $(\mathbb{C}, +)$.

Stabilité. $xy = (ac - bd) + i(ad + bc)$, avec $ac - bd$ et $ad + bc$ entiers : $xy \in B$.

Unité. $1 = 1 + 0i$, donc $1 \in B$.

Conclusion. D'après l'anneau induit sur une partie, $(B, +, \times)$ est un anneau commutatif unitaire.

Inversibles et diviseurs de zéro

Exemple : Des produits surprenants

Dans $\mathbb{Z}/14\mathbb{Z}$, $\overline{3} \times \overline{5} = \overline{15} = \overline{1}$: la classe $\overline{3}$ a un « inverse ». Mais $\overline{2} \times \overline{7} = \overline{14} = \overline{0}$, alors que $\overline{2} \neq \overline{0}$ et $\overline{7} \neq \overline{0}$.

Dans $\mathcal{M}_2(\mathbb{R})$, la matrice $A = \begin{pmatrix} 2 & -4 \\ 1 & -2 \end{pmatrix}$ n'est pas nulle, et pourtant $A \times A = O$.

Dans l'anneau H de la méthode, $(2+\sqrt{3})(2-\sqrt{3}) = 4 - 3 = 1$.

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 $b = 0$.

Vérifie : Un diviseur de zéro modulo 14

Laquelle de ces classes est un diviseur de zéro dans $\mathbb{Z}/14\mathbb{Z}$?

A. $\overline{9}$

Faux.
$\overline{9} \times \overline{11} = \overline{99} = \overline{1}$: $\overline{9}$ est inversible.

B. $\overline{13}$

Faux.
$\overline{13} = -\overline{1}$, et $\overline{13} \times \overline{13} = \overline{169} = \overline{1}$: elle est son propre inverse.

C. $\overline{4}$

Juste.
$\overline{4} \times \overline{7} = \overline{28} = \overline{0}$, avec $\overline{7} \neq \overline{0}$.

Indice 1

Un diviseur de zéro $\overline{a}$ vérifie $\overline{a} \times \overline{b} = \overline{0}$ pour une classe $\overline{b} \neq \overline{0}$.

Indice 2

$14 = 2 \times 7$: cherche une classe qui partage un facteur avec 14.

Correction

$\overline{4} \neq \overline{0}$ et $\overline{7} \neq \overline{0}$, mais $\overline{4} \times \overline{7} = \overline{28} = \overline{0}$, car $28 = 2 \times 14$. Donc $\overline{4}$ est un diviseur de zéro.

Les classes $\overline{9}$ et $\overline{13}$ sont inversibles. Un inversible n'est jamais un diviseur de zéro : si $x \times b = 0$, alors $b = x^{-1} \times 0 = 0$.

Viennent ensuite les anneaux de référence. **Pourquoi est-ce vrai** que $\mathcal{M}_2(\mathbb{R})$ a des diviseurs de zéro ? Une matrice avec beaucoup de zéros suffit. Et le produit de deux inversibles x et y est inversible : **pourquoi est-ce vrai ?** Son inverse est $y^{-1} \times x^{-1}$.

Anneaux de référence

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.

Démonstration

Étape 1 (point 1). « Groupes de référence » donne les groupes commutatifs $(\mathbb{Z}, +)$, ..., $(\mathbb{C}, +)$. Les règles de calcul dans $\mathbb{C}$ donnent un produit interne, associatif, commutatif, distributif, de neutre $1 \neq 0$, et un produit nul seulement si l'un des facteurs est nul.

Étape 2 (point 2). « Groupes de référence » donne le groupe commutatif $(\mathbb{Z}/n\mathbb{Z}, +)$, et « Opérations dans $\mathbb{Z}$/n$\mathbb{Z}$ » (chapitre d'arithmétique) donne un produit associatif, commutatif, distributif, de neutre $\overline{1}$.

Étape 3 (point 3). « Groupes de référence » et « Propriétés du produit des matrices » donnent l'anneau unitaire, non commutatif. Pour $n = 2$, $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq O$ vérifie $A \times A = O$; pour $n = 3$, on complète A par des zéros.

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.

Démonstration

Étape 1. $1 \times 1 = 1$: 1 est inversible, donc $A^\times \neq \emptyset$.

Étape 2 (stabilité). Si x et y sont inversibles, « Symétrique pour une loi associative » (point 2), appliqué à la loi $\times$, donne : $x \times y$ est inversible, d'inverse $y^{-1} \times x^{-1}$.

Étape 3. La loi induite est associative (« Propriétés héritées par une loi induite ») et 1 est neutre. Si $x \in A^\times$, son inverse x^{-1} est inversible, d'inverse x (même propriété, point 1) : $x^{-1} \in A^\times$.

Exemple : Des éléments inversibles

- Dans $\mathbb{Z}$, seuls 1 et -1 sont inversibles : $\mathbb{Z}^\times = \{-1, 1\}$.
- Dans $\mathbb{Z}/14\mathbb{Z}$, les inversibles sont $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{9}$, $\overline{11}$ et $\overline{13}$. Ils forment un groupe pour $\times$: par exemple, $\overline{3} \times \overline{9} = \overline{27} = \overline{13}$ est encore inversible.
- Dans $\mathcal{M}_2(\mathbb{R})$, on vérifie un inverse par un produit égal à I, **des deux côtés** : $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} = I$, et le produit dans l'autre ordre vaut aussi I.

Méthode : réfuter par un contre-exemple

Montrer que l'anneau $(\mathcal{M}_2(\mathbb{R}), +, \times)$ n'est pas commutatif.

1. **Nier la propriété.** « Non commutatif » signifie : il **existe** deux matrices A et B telles que $AB \neq BA$.
2. **Choisir simple**, avec beaucoup de zéros : $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.
3. **Calculer en entier.** $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
4. **Conclure** : « $AB \neq BA$, donc la loi $\times$ n'est pas commutative sur $\mathcal{M}_2(\mathbb{R})$. »

Un seul contre-exemple suffit. À l'inverse, mille exemples favorables ne prouveraient rien.

Corps

Diviser dans un anneau

Devine : Où peut-on diviser ?

Dans lequel de ces anneaux toute équation $a \times x = b$, avec $a \neq 0$, a-t-elle au moins une solution ?

A. $(\mathbb{Z}, +, \times)$

Faux.
$2x = 1$ n'a aucune solution entière.

B. $(\mathbb{Z}/4\mathbb{Z}, +, \times)$

Faux.
$\overline{2} \times x = \overline{1}$ n'a pas de solution : $\overline{2} \times x$ vaut toujours $\overline{0}$ ou $\overline{2}$.

C. $(\mathcal{M}_2(\mathbb{R}), +, \times)$

Faux.

Avec $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, on a $A \times A = O$. Si $A \times X = I$, alors $A = A \times (A \times X) = (A \times A) \times X = O$, ce qui est faux.

D. $(\mathbb{Q}, +, \times)$

Juste.

Si $a \neq 0$, alors $x = \dfrac{b}{a}$ est rationnel et convient.

Indice 1

Teste l'équation $a \times x = 1$ avec un a bien choisi.

Indice 2

Dans un anneau de matrices, souviens-toi des diviseurs de zéro.

Correction

Dans $\mathbb{Q}$, tout $a \neq 0$ a un inverse $\dfrac{1}{a}$, et $x = \dfrac{1}{a} \times b$ convient.

Dans les trois autres, un élément non nul n'a pas d'inverse : 2 dans $\mathbb{Z}$, $\overline{2}$ dans $\mathbb{Z}/4\mathbb{Z}$, $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ dans $\mathcal{M}_2(\mathbb{R})$.

Un anneau où l'on peut toujours diviser par un élément non nul s'appelle un **corps**.

Un corps n'a d'ailleurs aucun diviseur de zéro. **Pourquoi est-ce vrai ?** Si $a \neq 0$ et $a \times b = 0$, on multiplie par a^{-1}.

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 $K^* = K \setminus \{0\}$.

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 $\times$.

Démonstration

Étape 1. Supposons $a \times b = 0$ et $a \neq 0$. Alors a est inversible, car K est un corps.

Étape 2. Par associativité et « Règles de calcul dans un anneau » : $b = 1 \times b = (a^{-1} \times a) \times b = a^{-1} \times (a \times b) = a^{-1} \times 0 = 0$.

Conclusion. $a = 0$ ou $b = 0$. Par contraposée, le produit de deux éléments non nuls est non nul : K^* est stable pour $\times$.

Exemple : **Exemple et contre-exemple**

Exemple. $(\mathbb{Q}, +, \times)$ est un corps : par exemple, l'inverse de $-\dfrac{3}{5}$ est $-\dfrac{5}{3}$, encore rationnel.

Contre-exemple. $(\mathcal{M}_2(\mathbb{R}), +, \times)$ n'est pas un corps : $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ vérifie $A \times A = O$ avec $A \neq O$, et un corps n'a pas de diviseur de zéro.

Un corps est à démontrer ou à discuter dans 8 des 14 exercices de structures consultés. Pour $\mathbb{Q}$, tout vérifier à la main est long. L'énoncé suivant montre qu'il suffit de deux groupes et de la distributivité. **Pourquoi est-ce vrai ?** Parce que les calculs où 0 intervient se règlent à part.

Caractériser un corps commutatif

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.

Démonstration

Étape 1. Pour tout $x \in K$, $x \times 0 = 0 \times x = 0$: la preuve du point 1 de « Règles de calcul dans un anneau » n'emploie que la distributivité et le groupe $(K, +)$.

Étape 2 (associativité, commutativité). Pour x, y, z dans K : si aucun n'est nul, les égalités $(x \times y) \times z = x \times (y \times z)$ et $x \times y = y \times x$ sont vraies dans le groupe $(K^*, \times)$. Si l'un d'eux est nul, chaque membre vaut 0, par l'étape 1.

Étape 3 (unité). Le neutre 1 de $(K^*, \times)$ vérifie $1 \times 0 = 0 \times 1 = 0$: il est neutre sur K, et $1 \neq 0$ car $1 \in K^*$.

Conclusion. $(K, +, \times)$ est un anneau commutatif unitaire, et tout $x \neq 0$ a un inverse dans K^*.

À retenir : **Ce qu'il faut retenir de la preuve**

Le groupe $(K^*, \times)$ donne tout, sauf les calculs où 0 intervient. Ceux-là se règlent par $x \times 0 = 0 \times x = 0$, qui ne demande que la distributivité et le groupe $(K, +)$. Retiens ce découpage : les éléments non nuls d'un côté, 0 de l'autre.

Vérifie : Le cas d'un facteur nul

À l'étape 2, comment prouve-t-on $(x \times y) \times z = x \times (y \times z)$ lorsque $y = 0$?

A. Par l'étape 1 : chaque membre vaut 0.

Juste.

$(x \times 0) \times z = 0 \times z = 0$ et $x \times (0 \times z) = x \times 0 = 0$.

B. Par le groupe $(K^*, \times)$.

Faux.

$0 \notin K^*$: ce groupe ne dit rien des calculs où 0 intervient.

C. Ce cas n'arrive jamais.

Faux.

y est un élément quelconque de K : il peut être nul.

D. Par la commutativité de $\times$.

Faux.

Elle n'est pas encore établie sur K : c'est justement l'objet de l'étape 2.

Indice 1

Rappelle ce que l'étape 1 établit.

Indice 2

Calcule séparément les deux membres avec $y = 0$.

Correction

Avec $y = 0$, l'étape 1 donne $(x \times 0) \times z = 0 \times z = 0$ et $x \times (0 \times z) = x \times 0 = 0$. Les deux membres sont égaux. Le groupe $(K^*, \times)$ ne sert que lorsque x, y et z sont tous non nuls.

Les corps de référence $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ arrivent ensuite. **Pourquoi est-ce vrai ?** Tout nombre non nul y a un inverse : $\frac{1}{x}$, ou $\frac{\overline{z}}{|z|^2}$ pour un complexe z.

Propriété : Corps de référence

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps commutatifs. L'anneau $(\mathbb{Z}, +, \times)$ n'est pas un corps.

Démonstration

Étape 1. Ce sont des anneaux commutatifs unitaires avec $1 \neq 0$ (« Anneaux de référence »).

Étape 2. Un rationnel ou un réel x non nul a pour inverse $\frac{1}{x}$, rationnel si x l'est. Un complexe non nul z a pour inverse $\frac{\overline{z}}{|z|^2}$, car $z\overline{z} = |z|^2 \neq 0$.

Étape 3. S'il existait un entier y tel que $2y = 1$, le nombre 1 serait pair. Donc 2 n'est pas inversible dans $\mathbb{Z}$, qui n'est pas un corps.

Exemple : Contre-exemple : des non nuls qui ne restent pas non nuls

Dans $\mathbb{Z}/6\mathbb{Z}$, les classes non nulles ne forment pas un groupe pour $\times$: $\overline{2} \times \overline{3} = \overline{6} = \overline{0}$. L'hypothèse 2 de la caractérisation échoue. D'ailleurs, $\mathbb{Z}/6\mathbb{Z}$ n'est pas un corps, puisqu'un corps n'a pas de diviseur de zéro.

Dans $\mathbb{Z}/7\mathbb{Z}$, au contraire, chaque classe non nulle a un inverse : $\overline{2} \times \overline{4} = \overline{1}$, $\overline{3} \times \overline{5} = \overline{1}$ et $\overline{6} \times \overline{6} = \overline{1}$. **Pourquoi est-ce vrai** pour 7 et pas pour 6 ? Parce que 7 est premier : c'est l'énoncé suivant.

Les corps $\mathbb{Z}$/p$\mathbb{Z}$

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.

Démonstration

Étape 1 (n premier). $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire (« Anneaux de référence »). $\overline{1} \neq \overline{0}$, car $n \nmid 1$. Toute classe non nulle est inversible (« Le cas de $\mathbb{Z}$/p$\mathbb{Z}$, p premier », chapitre d'arithmétique). C'est donc un corps commutatif.

Étape 2 (n non premier). Comme $n \geq 2$ n'est pas premier, $n = ab$ avec a et b entiers, $1 < a < n$ et $1 < b < n$. Les classes $\overline{a}$ et $\overline{b}$ ne sont pas nulles, car n ne divise ni a ni b. Pourtant $\overline{a} \times \overline{b} = \overline{n} = \overline{0}$.

Conclusion. L'anneau a des diviseurs de zéro : ce n'est pas un corps (« Un corps n'a pas de diviseur de zéro »).

À retenir : Ce qu'il faut retenir de la preuve

Les deux sens utilisent deux outils différents. Si n est premier, l'arithmétique fournit l'inverse de chaque classe non nulle. Sinon, on écrit $n = ab$, et $\overline{a} \times \overline{b} = \overline{0}$ fabrique un diviseur de zéro. Pour réfuter « corps », exhiber un diviseur de zéro est l'arme la plus rapide.

Vérifie : Une classe qui n'est pas nulle

À l'étape 2, on a $n = ab$ avec $1 < a < n$ et $1 < b < n$. Pourquoi a-t-on $\overline{a} \neq \overline{0}$?

A. Parce que a est un diviseur premier de n.
Faux.
Rien ne l'impose : pour $n = 12$, on peut prendre $a = 4$ et $b = 3$.

B. Parce que $a \neq 0$, et la classe d'un entier non nul n'est jamais nulle.
Faux.

Ce n'est pas suffisant : $14 \neq 0$, et pourtant $\overline{14} = \overline{0}$ dans $\mathbb{Z}/14\mathbb{Z}$.

C. Parce que $0 < a < n$: n ne divise pas a.

Juste.

Un multiple strictement positif de n vaut au moins n : n ne divise pas a, donc $\overline{a} \neq \overline{0}$.

Indice 1

$\overline{a} = \overline{0}$ signifie que n divise a.

Indice 2

Quel multiple de n pourrait être compris entre 1 et $n-1$?

Correction

$\overline{a} = \overline{0}$ signifierait que n divise a. Or $1 < a < n$: aucun multiple de n n'est strictement compris entre 0 et n. Donc $\overline{a} \neq \overline{0}$, et de même $\overline{b} \neq \overline{0}$.

Le produit $\overline{a} \times \overline{b} = \overline{n} = \overline{0}$ montre alors un diviseur de zéro.

Exemple : Contre-exemple : intègre, mais pas un corps

L'anneau $(\mathbb{Z}, +, \times)$ n'a aucun diviseur de zéro. Pourtant ce n'est pas un corps : $3x = 1$ n'a pas de solution entière. L'absence de diviseur de zéro ne donne donc pas les inverses en général. Pour $\mathbb{Z}/p\mathbb{Z}$, la preuve les tire de l'arithmétique.

Il reste une dernière voie : transporter un corps connu, comme on a transporté un groupe. **Pourquoi est-ce vrai ?** Une bijection qui respecte les deux lois recopie chaque calcul.

Transférer un corps

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 :

$$f(x+y) = f(x) * f(y) \quad \text{et} \quad f(x \times y) = f(x) \top f(y).$$

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 $f(x^{-1})$.

Démonstration

Comme f est surjective, tout élément de E s'écrit $f(x)$ avec $x \in A$.

Étape 1. f est un homomorphisme surjectif de $(A, +)$ dans $(E, *)$: par « Transfert de structure de groupe », $(E, *)$ est un groupe commutatif de neutre $f(0)$.

Étape 2. Comme dans la preuve du transfert de structure de groupe : $\big(f(x)\top f(y)\big)\top f(z) = f\big((x\times y)\times z\big) = f\big(x\times(y\times z)\big) = f(x)\top\big(f(y)\top f(z)\big)$, et $f(x)\top\big(f(y)*f(z)\big) = f\big(x\times(y+z)\big) = \big(f(x)\top f(y)\big)*\big(f(x)\top f(z)\big)$; de même à droite.

Étape 3. Commutativité et unité $f(1)$ se transfèrent de la même façon. Si A est un corps : $f(1)\neq f(0)$ car f est injective, et si $f(x)\neq f(0)$, alors $x\neq 0$ et $f(x)\top f(x^{-1}) = f(x^{-1})\top f(x) = f(1)$.

À retenir : Ce qu'il faut retenir de la preuve

On calcule dans A, puis on revient par f, comme pour un groupe. La bijectivité sert deux fois. La surjectivité écrit tout élément de E sous la forme $f(x)$. L'injectivité garantit $f(1)\neq f(0)$.

Les sujets notent $(E,*,\top)$: $*$ joue le rôle de $+$, et $\top$ celui de $\times$. Le zéro est le neutre de $*$, ici $f(0)$; l'unité est le neutre de $\top$, ici $f(1)$. Ce ne sont pas forcément les nombres 0 et 1.

Vérifie : Le rôle de l'injectivité

Dans la preuve, pour transférer une structure de corps, à quoi sert l'injectivité de f ?

A. À garantir $f(1)\neq f(0)$.

Juste.
Un corps exige $1\neq 0$. Comme $1\neq 0$ dans A et que f est injective, $f(1)\neq f(0)$.

B. À écrire tout élément de E sous la forme $f(x)$.

Faux.
C'est le rôle de la surjectivité.

C. À obtenir l'associativité de $\top$.

Faux.
L'associativité se transfère par le calcul, avec la surjectivité seulement.

Indice 1
Un corps demande $1\neq 0$.
Indice 2
Que dit l'injectivité de deux éléments distincts ?

Correction
La définition d'un corps exige que l'unité diffère du zéro. Dans E, l'unité est $f(1)$ et le zéro est $f(0)$. Comme $1\neq 0$ dans le corps A et que f est injective, $f(1)\neq f(0)$. La surjectivité, elle, sert à écrire tout élément de E sous la forme $f(x)$.

Exemple : Contre-exemple : sans injectivité

Prends $E = \{0\}$, muni de $+$ et de $\times$, et l'application nulle $f : x \mapsto 0$, de $\mathbb{R}$ dans E. Pour tous réels x et y, elle vérifie $f(x+y) = 0 = f(x) + f(y)$ et $f(xy) = 0 = f(x) \times f(y)$.

Elle est surjective, mais pas injective : $f(1) = f(0)$. L'ensemble $(\{0\}, +, \times)$ est bien un anneau, et pourtant ce n'est pas un corps : son unité $f(1)$ est égale à son zéro $f(0)$. L'hypothèse « bijection » ne se remplace pas par « surjection ».

La suite est en synthèse : la méthode pour montrer qu'un anneau est un corps, puis un transfert de corps à rédiger.

La chaîne d'examen : un ensemble de matrices

Te voilà au bout du chapitre. Un exercice de structures figure dans 14 des 16 sujets consultés (2017-2022 et 2024-2025). Les matrices y servent de support dans 11 des 14 exercices de structures consultés.

À maîtriser : la chaîne entière, de la partie stable au corps. On la parcourt sur un ensemble neuf. On pose $J = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}$ et, pour a et b réels :

$$\begin{aligned} M(a,b) &= aI + bJ \\ &= \begin{pmatrix} a+b & -2b \\ b & a-b \end{pmatrix}. \end{aligned}$$

On note ici $E = \{M(a,b) \;/\; (a,b) \in \mathbb{R}^2\}$.

Méthode : montrer qu'un ensemble est un groupe

Pour **montrer que** $(E, *)$ est un groupe, choisis l'une de ces trois voies, de la plus rapide à la plus longue.

1. **Un sous-groupe.** Si E est contenu dans un groupe connu, pour la même loi, applique la caractérisation d'un sous-groupe.
2. **Un transfert.** Sinon, cherche un homomorphisme surjectif depuis un groupe connu, comme $(\mathbb{R}, +)$ ou $(\mathbb{C}^*, \times)$.
3. **Les axiomes.** En dernier recours : loi interne, associativité, neutre, symétrique de chaque élément, des deux côtés si la loi n'est pas commutative.

Dans les trois cas, **conclus** en nommant l'ensemble, la loi et la structure : « $(E, *)$ est un groupe commutatif ».

À toi : Coin examen : partie stable, homomorphisme, transfert

La structure d'anneau de $\mathcal{M}_2(\mathbb{R})$ est en général rappelée par l'énoncé. Rédige chaque réponse avant d'ouvrir la correction. Barème indicatif BURHAN.

- **Q1.** Montrer que $J^2 = -I$, puis que E est stable pour $\times$.
- **Q2.** On pose $f(a+ib) = M(a,b)$ pour tout complexe $a+ib$. Montrer que f est un homomorphisme de $(\mathbb{C}^*, \times)$ dans $(E, \times)$.
- **Q3.** On note $E^* = E \setminus \{O\}$. Montrer que $(E^*, \times)$ est un groupe commutatif.

Indice 1
Q1 : développe $(aI + bJ)(cI + dJ)$.
Indice 2
Q2 : compare avec le produit $(a+ib)(c+id)$.
Indice 3
Q3 : nomme le groupe de départ et l'homomorphisme, puis montre que l'image est exactement E^*.

Réponse
Q1. Par le calcul ligne par colonne :

$$\begin{aligned} J^2 &= \begin{pmatrix} 1-2 & -2+2 \\ 1-1 & -2+1 \end{pmatrix} \\ &= -I. \end{aligned}$$

Soient $M(a,b)$ et $M(c,d)$ quelconques dans E. Comme $IJ = JI = J$:

$$\begin{aligned} &M(a,b) \times M(c,d) \\ &= acI + (ad+bc)J + bdJ^2 \\ &= M(ac-bd, ad+bc). \end{aligned}$$

Donc E est stable pour $\times$. **0,75 pt**

Q2. Soient $z = a+ib$ et $z_1 = c+id$ quelconques dans $\mathbb{C}^*$. On a $(a+ib)(c+id) = (ac-bd) + i(ad+bc)$, donc, d'après Q1 :

$$\begin{aligned} f(zz_1) &= M(ac-bd, ad+bc) \\ &= f(z) \times f(z_1). \end{aligned}$$

Ainsi f est un homomorphisme de $(\mathbb{C}^*, \times)$ dans $(E, \times)$. **0,5 pt**

Q3. Le coefficient de la ligne 2, colonne 1 de $M(a,b)$ est b, et celui de la ligne 1, colonne 1 est $a+b$. Donc $M(a,b) = O$ si et seulement si $a = b = 0$, et $f(\mathbb{C}^*) = E^*$.

Comme $(\mathbb{C}^*, \times)$ est un groupe commutatif, par transfert de structure, $(E^*, \times)$ est un groupe commutatif, de neutre $f(1) = I$. **0,75 pt**

Vérifie : L'inverse d'une matrice de E

D'après Q3, quel est l'inverse de $M(1,1) = \begin{pmatrix} 2 & -2 \\ 1 & 0 \end{pmatrix}$ dans $(E^*, \times)$?

A. $M(-1,-1)$
Faux.

C'est l'opposé de $M(1,1)$, son symétrique pour $+$. Pour $\times$, $M(1,1)\times M(-1,-1)=M(0,-2)\neq I$.

B. $M\left(\frac{1}{2},-\frac{1}{2}\right)$

Juste.
$\frac{1}{1+i}=\frac{1-i}{2}$, et l'inverse de $f(z)$ est $f(z^{-1})$.

C. $M(1,-1)$

Faux.
$M(1,1)\times M(1,-1)=M(2,0)=2I$: tu as pris le conjugué sans diviser par $|1+i|^2=2$.

D. $M\left(\frac{1}{2},\frac{1}{2}\right)$

Faux.
$M(1,1)\times M\left(\frac{1}{2},\frac{1}{2}\right)=M(0,1)=J\neq I$.

Indice 1

$M(1,1)=f(1+i)$, et le symétrique de $f(z)$ est $f(z^{-1})$.

Indice 2

Calcule $\frac{1}{1+i}$ en multipliant par le conjugué.

Correction

Par transfert, l'inverse de $f(1+i)$ est $f\left(\frac{1}{1+i}\right)$. Or $\frac{1}{1+i}=\frac{1-i}{2}$, donc l'inverse est :

$$M\left(\frac{1}{2},-\frac{1}{2}\right)=\begin{pmatrix}0 & 1\\ -\frac{1}{2} & 1\end{pmatrix}.$$

Contrôle.

$$\begin{pmatrix}2 & -2\\ 1 & 0\end{pmatrix}\times\begin{pmatrix}0 & 1\\ -\frac{1}{2} & 1\end{pmatrix}=I,$$

et le produit dans l'autre ordre vaut aussi I.

Exemple **: Coin examen : sous-groupe et anneau**

- **Q4. Montrer que E est un sous-groupe de $(\mathcal{M}_2(\mathbb{R}),+)$.** $E\subset\mathcal{M}_2(\mathbb{R})$ et $O=M(0,0)\in E$. Soient $M(a,b)$ et $M(c,d)$ quelconques dans E : $M(a,b)-M(c,d)=M(a-c,b-d)\in E$. Donc E est un sous-groupe de $(\mathcal{M}_2(\mathbb{R}),+)$. **0,5 pt**

- **Q5. Montrer que $(E,+,\times)$ est un anneau commutatif unitaire.** E est un sous-groupe de $(\mathcal{M}_2(\mathbb{R}),+)$, stable pour $\times$ (Q1). D'après l'anneau induit sur une partie, $(E,+,\times)$ est un anneau. La formule de Q1 ne change pas si l'on échange (a,b) et (c,d), et $I=M(1,0)\in E$. Donc $(E,+,\times)$ est un anneau commutatif unitaire. **0,75 pt**

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

Pour **montrer que** $(K,+,\times)$ est un corps commutatif, trois voies :

1. **La caractérisation.** $(K,+)$ et $(K^*,\times)$ sont des groupes commutatifs, et $\times$ est distributive par rapport à $+$.
2. **Un transfert** depuis un corps connu, par une bijection qui respecte les deux lois.
3. **À la main.** $1\neq 0$, puis un inverse **dans** K pour chaque $x\neq 0$.

Pour réfuter, exhibe deux éléments non nuls de produit nul, ou un élément non nul sans inverse dans l'ensemble. **Conclus** en nommant la structure : « $(K,+,\times)$ est un corps commutatif », ou « n'est pas un corps ».

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

$(\mathbb{Z}/21\mathbb{Z},+,\times)$ est un anneau commutatif unitaire. Ce n'est pas un corps : $\overline{3}\times\overline{7}=\overline{21}=\overline{0}$, alors que $\overline{3}\neq\overline{0}$ et $\overline{7}\neq\overline{0}$.

Avant d'écrire « corps », vérifie l'absence de diviseur de zéro et l'existence de chaque inverse. Un seul diviseur de zéro suffit à tout refuser.

À toi : Coin examen : le corps

- **Q6.** Montrer que $(E,+,\times)$ est un corps commutatif.

Rédige avec la caractérisation d'un corps commutatif, puis compare avec l'autre voie, par transfert depuis $\mathbb{C}$.

Indice 1
Les trois hypothèses de la caractérisation sont presque établies : cite Q4, Q3, puis la distributivité.
Indice 2
Pour l'autre voie, il faut une bijection de $\mathbb{C}$ sur E : vérifie aussi l'injectivité.

Réponse
Q6. On vérifie les trois hypothèses de la caractérisation d'un corps commutatif.

- $(E,+)$ est un groupe commutatif, d'après Q4.
- $(E^*,\times)$ est un groupe commutatif, d'après Q3.

- La loi $\times$ est distributive par rapport à $+$ dans $\mathcal{M}_2(\mathbb{R})$, donc dans E.

Conclusion. D'après la caractérisation d'un corps commutatif, $(E, +, \times)$ est un corps commutatif. **0,75 pt**

Autre voie. f est surjective par définition de E. Elle est injective : $M(a,b) = M(c,d)$ donne $b = d$ (ligne 2, colonne 1), puis $a = c$. C'est donc une bijection de $\mathbb{C}$ sur E, avec $f(z + z_1) = f(z) + f(z_1)$ et $f(zz_1) = f(z) \times f(z_1)$. Par transfert, E est un corps commutatif, comme $\mathbb{C}$.

Total indicatif de la chaîne Q1 à Q6 : 4 points.

À toi : Coin examen : un corps par transfert

Point important : un transfert de corps sur des lois ad hoc. Sur $\mathbb{R}$, on pose $x * y = x + y - 3$ et $x \top y = xy - 3x - 3y + 12$. Dans $(\mathbb{R}, *, \top)$, la loi $*$ joue le rôle de $+$ et la loi $\top$ celui de $\times$. Barème indicatif BURHAN.

- **T1.** Montrer que $f : t \mapsto t + 3$ est une bijection de $\mathbb{R}$ sur $\mathbb{R}$.
- **T2.** Montrer que $f(t + s) = f(t) * f(s)$ pour tous réels t et s.
- **T3.** Montrer que $f(ts) = f(t) \top f(s)$ pour tous réels t et s.
- **T4.** En déduire que $(\mathbb{R}, *, \top)$ est un corps commutatif ; préciser son zéro et son unité.

Avant de rédiger : le zéro de ce corps est-il le réel 0 ?

Indice 1
T1 : résous $t + 3 = u$.
Indice 2
T2 et T3 : calcule $f(t) * f(s)$ et $f(t) \top f(s)$, puis compare.
Indice 3
T4 : le zéro est le neutre de $*$, c'est-à-dire $f(0)$; l'unité est $f(1)$.

Réponse
T1. Pour tout réel u, l'équation $t + 3 = u$ a une seule solution, $t = u - 3$: f est une bijection de $\mathbb{R}$ sur $\mathbb{R}$. **0,25 pt**

T2. Soient t et s deux réels quelconques.

$$\begin{aligned} & f(t) * f(s) \\ & = (t + 3) + (s + 3) - 3 \\ & = t + s + 3 \\ & = f(t + s). \end{aligned}$$

0,5 pt

T3. Avec les mêmes t et s :

$$\begin{aligned} & f(t) \top f(s) \\ & = (t+3)(s+3) - 3(t+3) \\ & \quad - 3(s+3) + 12 \\ & = ts + 3 = f(ts). \end{aligned}$$

0,75 pt

T4. $(\mathbb{R}, +, \times)$ est un corps commutatif, et f est une bijection qui vérifie T2 et T3. Par transfert d'une structure de corps, $(\mathbb{R}, *, \top)$ est un corps commutatif. Son zéro est $f(0) = 3$ et son unité est $f(1) = 4$. **0,5 pt**

Le zéro n'est donc pas le réel 0 : c'est le neutre de $*$, ici 3. L'unité est le neutre de $\top$, ici 4. Total indicatif : 2 points. Tu sais maintenant parcourir la chaîne en entier.

SOURCES

Référentiel BURHAN du chapitre « Structures algébriques : groupes, anneaux, corps » (2bac · sciences-mathematiques · mathematiques)