COURS ILLUSTRÉ - LYCÉE - 2ÈME BAC SCIENCES MATHÉMATIQUES A - SEMESTRE 2

Structures algébriques

Une structure algébrique associe un ensemble à une ou plusieurs opérations et à des règles précises. Le même raisonnement s'applique alors aux entiers, aux complexes, aux matrices, aux classes modulo n ou aux transformations du plan. Ce cours de structures algébriques de 2 Bac SM A montre comment vérifier une loi de composition interne, reconnaître un groupe et un sous-groupe, utiliser un morphisme pour transporter une structure, calculer avec des matrices carrées, puis distinguer anneau et corps. Six exercices corrigés reprennent les situations types de l'examen.

Mathématiques 2ème Bac Sciences Mathématiques A BIOF - Programme marocain - Mis à jour le 18/11/2026

Objectifs du chapitre

- Vérifier qu'une loi est interne et étudier ses propriétés
- Démontrer qu'un ensemble muni d'une loi est un groupe ou un sous-groupe
- Utiliser un morphisme ou un isomorphisme pour transférer une structure
- Calculer avec les matrices carrées et reconnaître anneaux, anneaux intègres et corps

Avant de commencer

- Ensembles, applications, injectivité et surjectivité
- Calcul dans $\mathbb{R}$ et $\mathbb{C}$, congruences et classes modulo n
- Composition de transformations et résolution d'équations

1. Loi de composition interne et partie stable

Loi de composition interne

Une loi de composition interne sur un ensemble E est une application de $E \times E$ dans E : elle associe à deux éléments x, y de E un élément noté $x \star y$, qui appartient encore à E.

Les exemples du programme sont nombreux : l'addition et la multiplication dans $\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$; l'addition et la multiplication des fonctions définies sur un même intervalle ; l'addition des polynômes de degré au plus n ; l'addition et la multiplication des matrices carrées d'ordre 2 ou 3 ; l'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$; la composition des transformations du plan. L'addition est une loi interne sur $\mathbb{N}$, mais la soustraction ne l'est pas, puisque $2 - 5 \notin \mathbb{N}$: une même formule peut définir une loi interne sur un ensemble et pas sur un autre.

Partie stable et loi induite

Une partie F de E est stable pour la loi $\star$ si $x, y \in F$ entraîne $x \star y \in F$. La restriction de $\star$ à $F \times F$ est alors une loi interne sur F, appelée loi induite. Par exemple, $\mathbb{U}$ est stable pour la multiplication de $\mathbb{C}$, mais l'ensemble des complexes de module 2 ne l'est pas.

Propriété	Égalité à vérifier pour tous les éléments concernés
Commutativité	$x \star y = y \star x$
Associativité	$(x \star y) \star z = x \star (y \star z)$
Élément neutre e	$e \star x = x \star e = x$
Symétrique x' de x	$x \star x' = x' \star x = e$

L'associativité permet d'enlever les parenthèses ; la commutativité permet de changer l'ordre : ce sont deux propriétés différentes. Si un élément neutre existe, il est unique ; pour une loi associative, le symétrique d'un élément, s'il existe, est unique. Pour une loi associative, on note $x^n = x \star x \star \cdots \star x$ (n facteurs) ; en notation additive, on écrit $nx = x + x + \cdots + x$.

La table d'une loi finie

Dans $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, l'addition se lit sur une table : $\overline{2} + \overline{3} = \overline{5} = \overline{1}$ et $\overline{3} + \overline{1} = \overline{0}$.

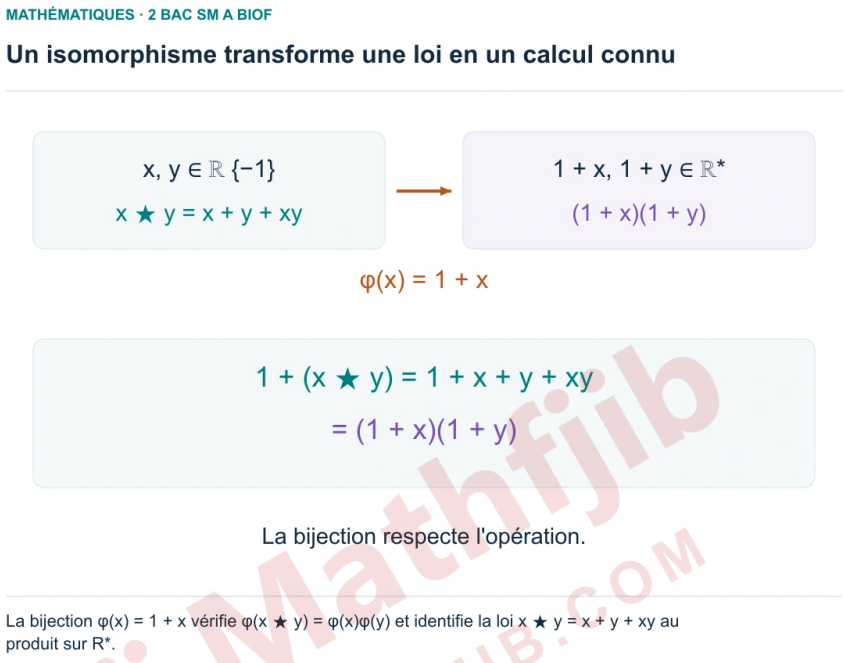
1. Chaque ligne de la table d'addition contient une seule fois chaque classe : le neutre est $\overline{0}$ et le symétrique de $\overline{3}$ est $\overline{1}$. Pour la multiplication, $\overline{2} \times \overline{2} = \overline{0}$: la classe $\overline{2}$ n'a pas d'inverse.

2. Un exemple complet de loi définie par une formule

La loi $x \star y = x + y + xy$

Sur $E = \mathbb{R} \setminus \{-1\}$, définissons $x \star y = x + y + xy$. On remarque que $1 + (x \star y) = (1 + x)(1 + y)$.

1. Si $x \neq -1$ et $y \neq -1$, ce produit est non nul, donc $x \star y \neq -1$: la loi est interne. Elle est commutative, et le développement des deux parenthésages donne $x + y + z + xy + xz + yz + xyz$: elle est associative.
2. L'élément neutre est 0. L'équation $x \star y = 0$ donne $y = -\dfrac{x}{1+x}$, qui appartient à E car $1 + y = \dfrac{1}{1+x} \neq 0$. Chaque élément a donc un symétrique : $(E, \star)$ est un groupe commutatif.



La bijection $\varphi(x) = 1 + x$ vérifie $\varphi(x \star y) = \varphi(x)\varphi(y)$ et identifie la loi $x \star y = x + y + xy$ au produit sur $\mathbb{R}^*$.

Attention

Sur tout $\mathbb{R}$, la même loi ne donnerait pas un groupe : l'élément -1 ne possède pas de symétrique pour le neutre 0. L'exclusion de -1 joue un rôle mathématique précis.

3. Groupes, calcul et puissances

Groupe et groupe commutatif

Un groupe $(G, \star)$ est un ensemble muni d'une loi interne associative, possédant un élément neutre, et dans lequel tout élément a un symétrique. Il est commutatif, ou abélien, si la loi est commutative. Par exemple, $(\mathbb{Z}, +)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont des groupes commutatifs.

Règles valables dans tout groupe

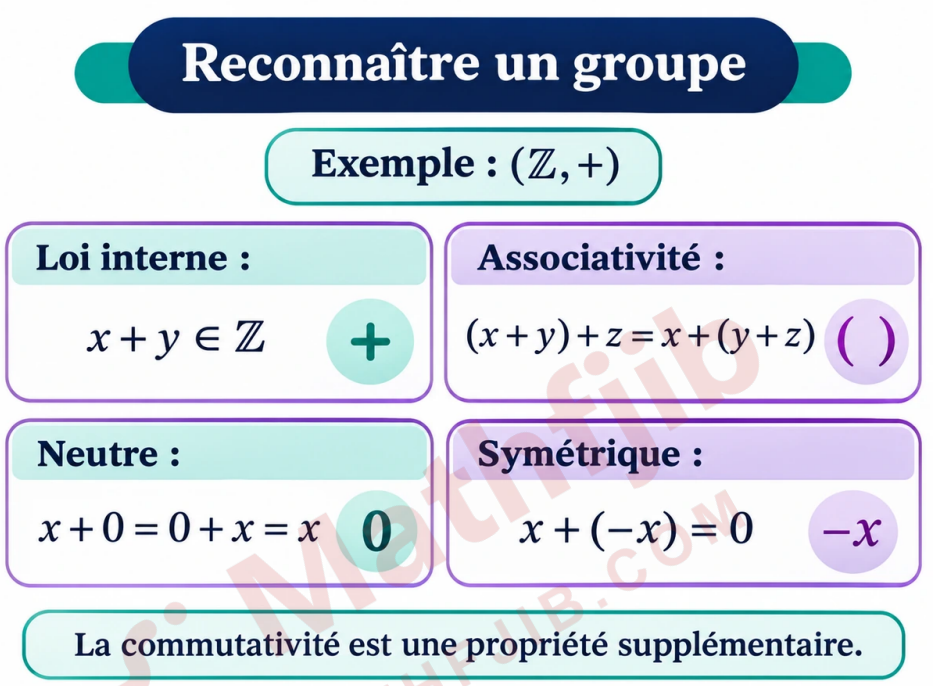
Dans un groupe noté multiplicativement, on peut simplifier à gauche et à droite : $ax = ay \Rightarrow x = y$. L'inverse d'un produit est $(ab)^{-1} = b^{-1}a^{-1}$: l'ordre est inversé. Pour $m, n \in \mathbb{Z}$: $a^m a^n = a^{m+n}$ et $(a^m)^n = a^{mn}$. L'égalité $(ab)^n = a^n b^n$ demande en général que a et b commutent.

Résoudre une équation dans un groupe

Dans un groupe noté multiplicativement, l'équation $axb = c$ admet l'unique solution $x = a^{-1}cb^{-1}$.

1. On multiplie par a^{-1} à gauche, puis par b^{-1} à droite. Changer arbitrairement l'ordre des facteurs serait faux dans un groupe non commutatif.

Les bijections d'un ensemble dans lui-même, munies de la composition, forment un groupe : le neutre est l'identité et le symétrique d'une bijection est sa réciproque. Les rotations de centre O forment aussi un groupe commutatif pour la composition, puisque la composée des rotations d'angles α et β est la rotation d'angle $\alpha + \beta$. Ces exemples relient opérations sur les nombres et opérations sur les transformations.



Pour former un groupe, la loi doit être interne, associative, posséder un élément neutre et donner un symétrique à chaque élément.

4. Sous-groupes : une vérification plus courte

Sous-groupe

Un sous-groupe H d'un groupe $(G, \star)$ est une partie de G qui est elle-même un groupe pour la loi induite.

Caractérisation d'un sous-groupe

Une partie H de G est un sous-groupe de $(G, \star)$ si et seulement si H est non vide et, pour tous $x, y \in H$, $x \star y' \in H$, où y' est le symétrique de y. En notation additive, le critère devient $x - y \in H$; en notation multiplicative, $xy^{-1} \in H$.

Les multiples d'un entier

Pour un entier $n \geq 1$, $n\mathbb{Z}$ contient 0. Si $x = na$ et $y = nb$, alors $x - y = n(a - b) \in n\mathbb{Z}$.

1. C'est donc un sous-groupe de $(\mathbb{Z}, +)$. On démontre que tous les sous-groupes de $(\mathbb{Z}, +)$ sont de cette forme.

Les racines de l'unité

Dans $(\mathbb{C}^*, \times)$, $\mathbb{U}_n = \{z : z^n = 1\}$ contient 1. Si $z, w \in \mathbb{U}_n$, alors $\left(\frac{z}{w}\right)^n = \frac{z^n}{w^n} = 1$.

1. Ainsi $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$; il contient exactement n éléments.

5. Morphismes, noyau, image et isomorphismes

Morphisme

Soient $(E, \star)$ et $(F, \top)$ deux ensembles munis de lois internes. Une application $f : E \to F$ est un morphisme si $f(x \star y) = f(x) \top f(y)$ pour tous $x, y \in E$. Un morphisme bijectif est un isomorphisme ; les deux ensembles munis de leurs lois sont alors dits isomorphes.

Transfert de structure

Si f est un morphisme surjectif de $(E, \star)$ sur $(F, \top)$, il transporte l'associativité, la commutativité, l'élément neutre et les symétriques : si $(E, \star)$ est un groupe, alors $(F, \top)$ est un groupe, de neutre $f(e)$, et le symétrique de $f(x)$ est $f(x')$. Plus généralement, l'image d'un groupe par un morphisme est un groupe.

Noyau et image d'un morphisme de groupes

Si $f : (G, \star) \to (H, \top)$ est un morphisme de groupes, f envoie le neutre sur le neutre. Le noyau $\ker f = \{x \in G : f(x) = e_H\}$ est un sous-groupe de G et l'image $f(G)$ est un sous-groupe de H. Le morphisme est injectif si et seulement si $\ker f = \{e_G\}$.

Transporter une loi vers une loi connue

Pour la loi $x \star y = x + y + xy$ sur $E = \mathbb{R} \setminus \{-1\}$, l'application $\varphi(x) = 1 + x$ est une bijection de E sur $\mathbb{R}^*$.

1. Comme $\varphi(x \star y) = (1+x)(1+y) = \varphi(x)\varphi(y)$, c'est un isomorphisme de $(E, \star)$ sur $(\mathbb{R}^*, \times)$: les propriétés du produit se transportent à cette loi, et le symétrique de x est $\varphi^{-1}\left(\frac{1}{1+x}\right) = \frac{1}{1+x} - 1$.

Un morphisme non injectif

L'application $z \mapsto |z|$ de $(\mathbb{C}^*, \times)$ vers $(\mathbb{R}_+^*, \times)$ est un morphisme surjectif.

1. Son noyau est le cercle unité $\mathbb{U}$, et non le seul complexe 1 : elle n'est pas injective. On retrouve au passage que $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

6. Matrices carrées : un calcul associatif et souvent non commutatif

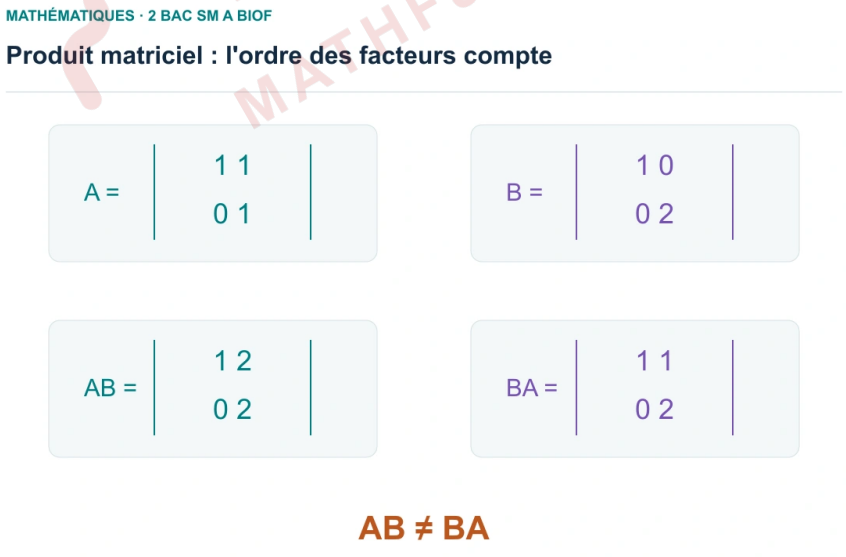
Opérations sur les matrices carrées

Pour des matrices carrées d'ordre $n = 2$ ou $n = 3$, l'addition se fait coefficient par coefficient, et le coefficient de la ligne i et de la colonne j du produit AB est $\sum_{k=1}^{n} a_{ik}b_{kj}$. Le produit est associatif, distributif par rapport à l'addition, et admet pour neutre la matrice identité I_n, mais il n'est pas commutatif en général. On note $\mathcal{M}_n(\mathbb{R})$ l'ensemble de ces matrices.

Deux produits différents

Pour $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $AB = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$ tandis que $BA = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$.

1. On a bien $AB \neq BA$: dans un calcul matriciel, l'ordre des facteurs doit être conservé.



Pour $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, les coefficients en haut à droite de AB et BA sont 2 et 1 : $AB \neq BA$.

Un produit de matrices d'ordre 3

Pour $C = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, on obtient $C^2 = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

1. Par récurrence, C^n a la même forme avec $2n$ à la place de 2 : le coefficient de la première ligne et de la troisième colonne vaut $1 \times 2 + 0 \times 0 + 2 \times 1 = 4$ pour C^2.

Matrices inversibles d'ordre 2

Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc \neq 0$, A est inversible et $A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Les matrices inversibles d'ordre fixé forment un groupe pour le produit. Toutes les matrices ne sont pas inversibles : la matrice nulle en est un contre-exemple.

7. Anneaux et corps : deux opérations à distinguer

Anneau

Un anneau $(A, +, \times)$ est un ensemble muni de deux lois internes telles que $(A, +)$ soit un groupe commutatif, que $\times$ soit associative et distributive par rapport à $+$. Il est unitaire si $\times$ admet un élément neutre, et commutatif si $\times$ est commutative.

Règles de calcul dans un anneau

Dans un anneau, $a \times 0 = 0 \times a = 0$, $(-a) \times b = a \times (-b) = -(a \times b)$ et $(-a) \times (-b) = a \times b$. Si a et b commutent, la formule du binôme de Newton s'applique à $(a+b)^n$.

Anneau intègre et diviseurs de zéro

Un élément non nul a est un diviseur de zéro s'il existe $b \neq 0$ tel que $ab = 0$ ou $ba = 0$. Un anneau commutatif unitaire, avec $1 \neq 0$ et sans diviseur de zéro, est dit intègre : $ab = 0$ y entraîne $a = 0$ ou $b = 0$.

Des diviseurs de zéro

Dans $\mathcal{M}_2(\mathbb{R})$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ alors qu'aucun des deux facteurs n'est nul.

1. De même, $\overline{2} \times \overline{3} = \overline{0}$ dans $\mathbb{Z}/6\mathbb{Z}$. Ces deux anneaux ne sont pas intègres, tandis que $\mathbb{Z}$ l'est.

Corps

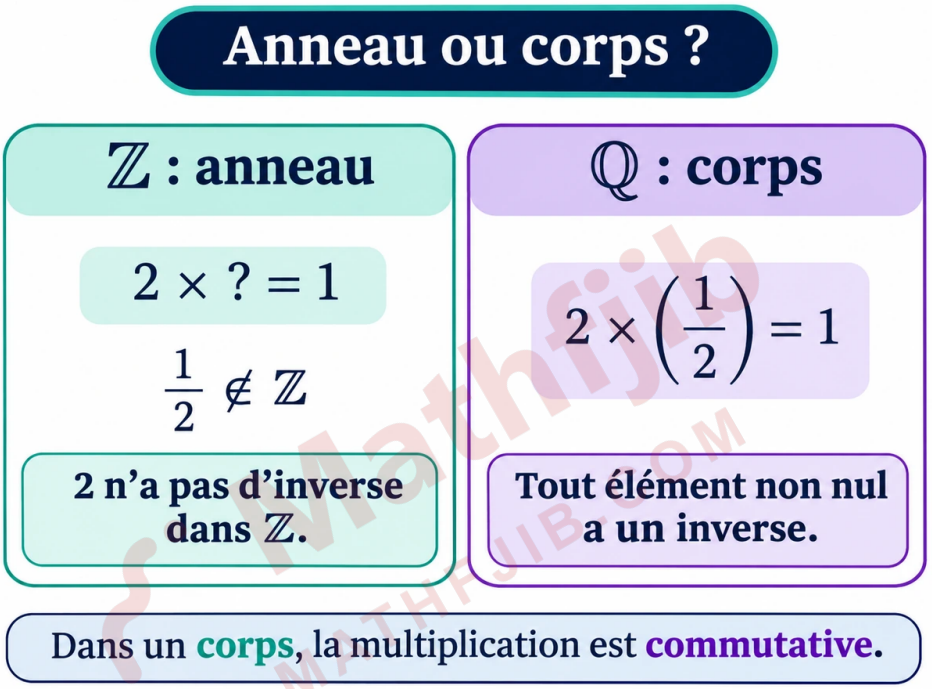
Un corps est un anneau unitaire, avec $1 \neq 0$, dans lequel tout élément non nul possède un inverse pour la multiplication. Un corps commutatif est intègre, et l'équation $ax = b$ y admet l'unique solution $x = a^{-1}b$ si $a \neq 0$. Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs ; $\mathbb{Z}$ n'est pas un corps, car 2 n'y a pas d'inverse.

Ensemble et lois usuelles	Structure à retenir
$(\mathbb{Z}, +, \times)$	Anneau commutatif unitaire intègre, pas un corps
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$	Anneau commutatif unitaire ; corps si et seulement si n est premier
$(\mathcal{M}_n(\mathbb{R}), +, \times)$, $n = 2$ ou 3	Anneau unitaire non commutatif et non intègre
$(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$	Corps commutatifs

Si p est premier, chaque classe non nulle modulo p est première avec p et possède donc un inverse par Bézout : $\mathbb{Z}/p\mathbb{Z}$ est un corps. Si n est composé, $n = ab$ avec $1 < a, b < n$, alors $\overline{a} \times \overline{b} = \overline{0}$: $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro et n'est pas un corps.

Méthode : Lire un problème de structure

1. Identifier l'ensemble, les lois et leurs neutres respectifs.
2. Vérifier la stabilité, puis les propriétés demandées, une par une.
3. Chercher un groupe ou un anneau déjà connu, un sous-groupe ou un isomorphisme qui évite des calculs.
4. Pour montrer qu'une propriété est fausse, donner un contre-exemple explicite dans l'ensemble.



Les entiers forment un anneau mais pas un corps, car 2 n'a pas d'inverse dans $\mathbb{Z}$; dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, tout élément non nul est inversible.

Je retiens

- Une loi interne reste dans l'ensemble ; associativité et commutativité sont deux propriétés distinctes.
- Un groupe demande une loi associative, un élément neutre et un symétrique pour chaque élément.
- H est un sous-groupe si H est non vide et stable par $x \star y'$, où y' est le symétrique de y.
- Un morphisme surjectif transporte la structure ; un isomorphisme identifie deux structures.
- Le produit matriciel est associatif mais pas commutatif : l'ordre des facteurs se conserve.
- Un anneau intègre n'a pas de diviseur de zéro ; un corps exige l'inverse de tout élément non nul.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Exercices - À chercher avant la correction

Cherchez chaque exercice sur votre cahier avant de lire sa correction. Justifiez chaque étape et citez le théorème utilisé, avec ses hypothèses.

Exercice 1. Une loi isomorphe à l'addition

Facile

Sur $\mathbb{R}$, on définit $x \star y = x + y - 2$.

1. Montrer que $\star$ est une loi interne, commutative et associative.
2. Déterminer son élément neutre et le symétrique de tout réel x. Conclure.
3. Montrer que $f(x) = x - 2$ définit un isomorphisme de $(\mathbb{R}, \star)$ sur $(\mathbb{R}, +)$.

Exercice 2. Comparer $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$

Facile

1. Dresser la table de multiplication des classes non nulles de $\mathbb{Z}/5\mathbb{Z}$ et donner l'inverse de chacune.
2. Dans $\mathbb{Z}/4\mathbb{Z}$, calculer $\overline{2} \times \overline{2}$. La classe $\overline{2}$ a-t-elle un inverse ?
3. Conclure sur la structure de ces deux anneaux.

Exercice 3. Un groupe de matrices isomorphe à $(\mathbb{R}, +)$

Intermédiaire

Pour x réel, on pose $M(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ et $G = \{M(x) : x \in \mathbb{R}\}$.

1. Calculer $M(x)M(y)$ et en déduire que G est stable pour la multiplication des matrices.
2. Montrer que $\varphi : x \mapsto M(x)$ est un isomorphisme de $(\mathbb{R}, +)$ sur $(G, \times)$.
3. En déduire que $(G, \times)$ est un groupe commutatif, puis calculer $M(x)^n$ pour $n \in \mathbb{N}$ et $M(x)^{-1}$.

Exercice 4. Un morphisme de groupes et son noyau

Intermédiaire

Soit $f : \mathbb{R} \to \mathbb{C}^*$ définie par $f(\theta) = e^{i\theta}$.

1. Montrer que f est un morphisme de $(\mathbb{R}, +)$ vers $(\mathbb{C}^*, \times)$.
2. Déterminer son noyau et son image.
3. En déduire deux sous-groupes, l'un de $(\mathbb{R}, +)$, l'autre de $(\mathbb{C}^*, \times)$. Le morphisme est-il injectif ?

Exercice 5. Le corps des matrices $M(a, b)$

Approfondissement

Pour a, b réels, on pose $M(a, b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ et $E = \{M(a, b) : (a, b) \in \mathbb{R}^2\}$.

1. Montrer que E est stable pour l'addition et la multiplication des matrices.

2. Soit $\varphi : \mathbb{C} \to E$ définie par $\varphi(a+ib) = M(a,b)$. Montrer que φ est bijective et que $\varphi(z+z') = \varphi(z) + \varphi(z')$ et $\varphi(zz') = \varphi(z)\varphi(z')$.
3. En déduire que $(E, +, \times)$ est un corps commutatif, et calculer $M(0,1)^2$.

Exercice 6. Transporter une structure par un isomorphisme

Approfondissement

Sur $I =]1, +\infty[$, on définit $x \star y = xy - x - y + 2$.

1. Vérifier que $x \star y = (x-1)(y-1) + 1$ et en déduire que $\star$ est une loi interne sur I.
2. Montrer que $\varphi(x) = x - 1$ définit un isomorphisme de $(I, \star)$ sur $(]0, +\infty[, \times)$.
3. En déduire que $(I, \star)$ est un groupe commutatif, son élément neutre et le symétrique de x.
4. On note $x^{(n)} = x \star x \star \cdots \star x$ (n termes). Exprimer $x^{(n)}$ en fonction de x et n.

Mathfjib MATHFJIB.COM
Mathfjib MATHFJIB.COM

Corrections expliquées des exercices

Exercice 1. Une loi isomorphe à l'addition

1. Pour x, y réels, $x+y-2$ est réel : la loi est interne. Elle est commutative, car $x+y-2 = y+x-2$, et associative, car $(x \star y) \star z = x+y+z-4 = x \star (y \star z)$.

2. $x \star e = x \iff x+e-2 = x \iff e = 2$: le neutre est 2. Puis $x \star x' = 2 \iff x' = 4-x$. Ainsi $(\mathbb{R}, \star)$ est un groupe commutatif.

3. f est bijective, de réciproque $y \mapsto y+2$, et $f(x \star y) = x+y-4 = (x-2)+(y-2) = f(x)+f(y)$: c'est un isomorphisme. On vérifie que $f(2) = 0$, le neutre de $(\mathbb{R}, +)$.

Exercice 2. Comparer $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$

1. Les produits non nuls modulo 5 donnent : $\overline{1} \times \overline{1} = \overline{1}$, $\overline{2} \times \overline{3} = \overline{1}$, $\overline{4} \times \overline{4} = \overline{16} = \overline{1}$. Les inverses sont donc $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$ et $\overline{4}^{-1} = \overline{4}$. Le reste de la table se complète de même, par exemple $\overline{2} \times \overline{4} = \overline{3}$ et $\overline{3} \times \overline{3} = \overline{4}$.

2. $\overline{2} \times \overline{2} = \overline{4} = \overline{0}$. Si $\overline{2}$ avait un inverse $\overline{a}$, on aurait $\overline{2} = \overline{2} \times (\overline{2} \times \overline{a}) = \overline{0} \times \overline{a} = \overline{0}$, ce qui est faux.

3. $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ est un corps, car 5 est premier. $(\mathbb{Z}/4\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire non intègre, donc pas un corps.

Exercice 3. Un groupe de matrices isomorphe à $(\mathbb{R}, +)$

1. $M(x)M(y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = M(x+y)$, qui appartient à G.

2. φ est surjective par définition de G, et injective car $M(x) = M(y)$ impose $x = y$. La question 1 s'écrit $\varphi(x+y) = \varphi(x)\varphi(y)$: φ est un isomorphisme.

3. $(\mathbb{R}, +)$ est un groupe commutatif, et l'isomorphisme transporte la structure : $(G, \times)$ est un groupe commutatif de neutre $M(0) = I_2$. On en déduit $M(x)^n = M(nx)$ et $M(x)^{-1} = M(-x)$.

Exercice 4. Un morphisme de groupes et son noyau

1. $f(\theta+\theta') = e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'} = f(\theta)f(\theta')$.

2. $f(\theta) = 1 \iff \theta \equiv 0\ [2\pi]$: $\ker f = 2\pi\mathbb{Z}$. Tout complexe de module 1 s'écrit $e^{i\theta}$: $f(\mathbb{R}) = \mathbb{U}$.

3. Le noyau $2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$ et l'image $\mathbb{U}$ un sous-groupe de $(\mathbb{C}^*, \times)$. Comme $\ker f \neq \{0\}$, f n'est pas injective : par exemple $f(0) = f(2\pi)$.

Exercice 5. Le corps des matrices $M(a, b)$

1. $M(a,b) + M(c,d) = M(a+c, b+d)$ et $M(a,b)M(c,d) = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = M(ac-bd, ad+bc)$: les deux résultats sont dans E.

2. φ est surjective par définition de E, et injective car $M(a,b) = M(c,d)$ impose $a = c$ et $b = d$. Pour $z = a+ib$ et $z' = c+id$, $z+z' = (a+c)+i(b+d)$ et $zz' = (ac-bd)+i(ad+bc)$: la question 1 donne exactement $\varphi(z+z') = \varphi(z)+\varphi(z')$ et $\varphi(zz') = \varphi(z)\varphi(z')$.

3. φ est un isomorphisme qui transporte les deux lois : $(E, +, \times)$ a la même structure que $(\mathbb{C}, +, \times)$, c'est un corps commutatif, de neutres $M(0,0)$ et $M(1,0) = I_2$. Comme $\varphi(i) = M(0,1)$ et $i^2 = -1$, on a $M(0,1)^2 = M(-1,0) = -I_2$.

Exercice 6. Transporter une structure par un isomorphisme

1. $(x-1)(y-1)+1 = xy-x-y+1+1 = x \star y$. Si $x > 1$ et $y > 1$, alors $(x-1)(y-1) > 0$ et $x \star y > 1$: la loi est interne sur I.

Mathfjib MATHFJIB.COM

2. φ est une bijection de I sur $]0,+\infty[$, de réciproque $t \mapsto t+1$, et $\varphi(x \star y) = (x-1)(y-1) = \varphi(x)\varphi(y)$: c'est un isomorphisme.

3. $(]0,+\infty[, \times)$ est un groupe commutatif ; la structure se transporte. Le neutre est $\varphi^{-1}(1) = 2$ et le symétrique de x est $\varphi^{-1}\left(\dfrac{1}{x-1}\right) = 1 + \dfrac{1}{x-1} = \dfrac{x}{x-1}$. Contrôle : $x \star \dfrac{x}{x-1} = (x-1) \times \dfrac{1}{x-1} + 1 = 2$.

4. $\varphi\left(x^{(n)}\right) = \varphi(x)^n = (x-1)^n$, donc $x^{(n)} = 1 + (x-1)^n$.

Questions fréquentes

Comment démontrer qu'une loi définit un groupe ?

Vérifier qu'elle est interne et associative, trouver un élément neutre valable des deux côtés, puis un symétrique de chaque élément. La commutativité est une propriété supplémentaire, pas une obligation du groupe.

Comment montrer qu'une partie est un sous-groupe ?

Montrer qu'elle est non vide, souvent en vérifiant qu'elle contient le neutre, puis que $x \star y'$ lui appartient pour tous x et y de la partie, où y' est le symétrique de y.

À quoi sert un isomorphisme en structures algébriques ?

Il identifie deux structures par une bijection qui respecte les lois. On peut alors transporter calculs et propriétés d'un ensemble connu, comme $\mathbb{R}$, $\mathbb{C}$ ou les matrices, vers un ensemble muni d'une loi moins familière.

Quelle différence entre anneau et corps ?

Dans un corps, tout élément non nul possède un inverse pour la multiplication. Un anneau peut en manquer : les entiers et les matrices carrées donnent deux exemples différents.

Pourquoi $\mathbb{Z}/n\mathbb{Z}$ est-il un corps seulement si n est premier ?

Si n est premier, toute classe non nulle est première avec n et Bézout fournit son inverse. Si $n = ab$ avec $1 < a, b < n$, alors $\overline{a} \times \overline{b} = \overline{0}$: il existe des diviseurs de zéro, ce qui est impossible dans un corps.

MATHFJIB - Mathématiques 2 Bac SM A
Suivez les consignes et la progression de votre professeur.
Retrouver le cours, ses illustrations et les exercices corrigés en ligne.