Prof : Mohamed iaalou

Cours de Mathématiques

Deuxième année du baccalauréat

Author: Mohamed iaalou

Institute: inspection de Mathématiques, direction provinciale - Tantan

Date: April 25, 2020

Version: 2.0 covid - 19

Nous Contacter: M.iaalou

Taalimona.com
Soutien Scolaire

Séries : Sciences Mathématiques A et B

Contents

Capacités attendues

- *Maitriser les techniques d'opérations sur les différentes structures usuelles ;*
- *Utiliser les structures des ensembles usuels pour étudier les structures d'autres ensembles ;*
- *Comparer deux structures algébriques transposer une structure algébrique d'un ensemble à un autre en utilisant la notion d'homomorphisme et d'isomorphisme.*

Recommandations pédagogiques

- *On se limitera à l'ensemble des fonctions définies sur un intervalle ; l'ensemble des polynômes de degré n ; l'ensemble des matrices carrées ; les ensembles $\mathbb{Z}/n\mathbb{Z}$ et les divers ensembles de transformations munis de la composition des transformations ;*
- *On insistera sur les opérations fondamentales dans l'ensemble des matrices carrées ;*
- *On présentera les différentes définitions illustrées par des exemples usuels ;*
- *On insistera sur le sous-groupe et le sous-espace vectoriel dans leur relation avec les groupes et les espaces vectoriels usuels ;*
- *On traitera plusieurs modèles d'opérations sur différents ensembles du programme (les nombres ; les transformations ; les matrices ; les applications ; $\mathbb{Z}/n\mathbb{Z}$; U_n ..);*
- *On traitera la structure de $(M_n, +, \times)$; et la structure de $(M_n, +, .)$ pour $n = 2$ et pour $n = 3$*

Prof : Mohamed iaalou

Chapter 1 Lois de composition interne - Morphisme

1.1 Lois de composition interne

1.1.1 Définition et exemples

Définition 1.1

Soit E un ensemble non vide. Une loi de composition interne sur E (ou encore une opération dans E) est une application de $E \times E$ dans E.

Notation

Soient f une application de $E \times E$ vers E, avec E un ensemble non vide et $(a, b) \in E^2$.

- L'élément $f(a, b)$ est appelé le composé ou la composée de a et b dans cet ordre dans E, on le note souvent $a \star b$, aTb , $a \perp b \dots$.
- Si $\star$ est une loi de composition interne sur un ensemble E, on dit que E est muni de la loi $\star$ et on écrit $(E, \star)$. L'ensemble $(E, \star)$. est appelé un magma.

Exemples usuels

1. Dans $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ ou $\mathbb{C}$, l'addition et la multiplication sont des lois de composition interne.
2. Dans $\mathbb{N}$, la soustraction n'est pas une loi interne, mais elle l'est dans $\mathbb{Z}$. La division dans $\mathbb{R}$ n'est pas une loi interne mais la division dans $\mathbb{R}^\star$ l'est.
3. Dans $\mathbb{N}^\star$, l'exponentiation a^b, le PGCD ou le PPCM sont des lois internes.
4. Si E est un ensemble, on a sur $\mathscr{P}(E)$ les lois de composition internes suivantes:
   - L'intersection : $(A, B) \mapsto A \cap B$
   - La réunion : $(A, B) \mapsto A \cup B$
   - La différence : $(A, B) \mapsto A \backslash B$.
   - La différence symétrique : $(A; B) \mapsto A \Delta B$.
5. L'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ (voir le chapitre : Arithmétique dans $\mathbb{Z}$) sont des lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$.
6. Soit $\mathscr{F}(I; \mathbb{R})$ l'ensemble des fonctions réelles définies sur un intervalle I. L'addition et la multiplication sont des lois de composition interne sur $\mathscr{F}(I; \mathbb{R})$
7. Pour $I = \mathbb{R}$, la composition $\circ$ est une loi de composition interne sur $\mathscr{F}(\mathbb{R}; \mathbb{R})$
8. Si E est un ensemble non vide, la composition des applications de E dans E est une loi interne dans E^E.
9. Le produit scalaire dans le plan vectoriel $\mathcal{V}_2$ n'est pas une loi de composition interne car $\vec{u}.\vec{v} \in \mathbb{R}$, et donc $\vec{u}.\vec{v} \notin \mathcal{V}_2$
10. Le produit vectoriel dans l'espace des vecteurs $\mathcal{V}_3$ est une loi de composition interne.
11. L'ensemble $(\mathcal{T}, \circ)$ des translations du plan est un magma. $(t_{\vec{u}} \circ t_{\vec{v}} = t_{\vec{u}+\vec{v}})$

N.B : La liste précédente est très loin d'être exhaustive.

1.1.2 Ensemble des matrices carrées d'ordre 2 à coefficients réels

Définition 1.2

Tout tableau de la forme $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ où a, b, c et d sont des réels est appelé matrice carrée d'ordre 2.

L'ensemble des matrices carrées d'ordre 2 à coefficients réels est noté $\mathscr{M}_2(\mathbb{R})$.

On écrit : $\mathscr{M}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix}, (a, b, c, d) \in \mathbb{R}^4 \right\}$

1.1.2.1 l'addition et la multiplication dans $\mathscr{M}_2(\mathbb{R})$

On définit sur $\mathscr{M}_2(\mathbb{R})$ la somme et le produit de deux matrices comme suit :

Soient $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ et $N = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$ deux matrices de $\mathscr{M}_2(\mathbb{R})$.

- Somme de deux matrices:

$$M + N = \begin{pmatrix} a & c \\ b & d \end{pmatrix} + \begin{pmatrix} x & z \\ y & t \end{pmatrix} = \begin{pmatrix} a+x & c+z \\ b+y & d+t \end{pmatrix}.$$

- le produit de deux matrices :

$$M \times N = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \times \begin{pmatrix} x & z \\ y & t \end{pmatrix} = \begin{pmatrix} ax+cy & az+ct \\ bx+dy & bz+dt \end{pmatrix}.$$

L'addition et la multiplication matricielles sont des lois de composition interne sur $\mathscr{M}_2(\mathbb{R})$.

Exemples

Soient $A = \begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix}$ deux matrices de $\mathscr{M}_2(\mathbb{R})$.

- Calculons $A + B$:

$$\begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 5+2 & 1+0 \\ 3+4 & -2+3 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 7 & 1 \end{pmatrix}$$

- Calculons $A \times B$ et $B \times A$

$$\begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 5\times 2 + 1\times 4 & 5\times 0 + 1\times 3 \\ 3\times 2 + (-2)\times 4 & 3\times 0 + (-2)\times 3 \end{pmatrix} = \begin{pmatrix} 14 & 3 \\ -2 & -6 \end{pmatrix}$$

De la même façon : $B \times A = \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 10 & 2 \\ 29 & -2 \end{pmatrix}$

1.1.3 Ensemble des matrices carrées d'ordre 3 à coefficients réels.

Définition 1.3

On appelle matrice carrée d'ordre 3, tout tableau de nombres réels de la forme :

$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ où $a_{ij} \in \mathbb{R}, \forall i, j \in \{1, 2, 3\}$.

Chaque coefficient a_{ij} se trouve à l'intersection de la i^{me} ligne et la j^{me} colonne .

Définition 1.3

L'ensemble des matrices carrées d'ordre 3 est noté $\mathscr{M}_3(\mathbb{R})$

1.1.3.1 l'addition et la multiplication dans $\mathscr{M}_3(\mathbb{R})$

On définit sur $\mathscr{M}_3(\mathbb{R})$ la somme et le produit de deux matrices par :

Soient $M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ et $N = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}$ deux matrices de $M_3(\mathbb{R})$

- **Somme de deux matrices :**

$$\begin{aligned} M+N &= \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & a_{13}+b_{13} \\ a_{21}+b_{21} & a_{22}+b_{22} & a_{23}+b_{23} \\ a_{31}+b_{31} & a_{32}+b_{31} & a_{33}+b_{33} \end{pmatrix} \end{aligned}$$

.

- **Produit de deux matrices :**

$$\begin{aligned} M\times N &= \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \times \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31} & a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32} & a_{11}b_{13}+a_{12}b_{23}+a_{13}b_{33} \\ a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31} & a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32} & a_{21}b_{13}+a_{22}b_{23}+a_{23}b_{33} \\ a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31} & a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32} & a_{31}b_{13}+a_{32}b_{23}+a_{33}b_{33} \end{pmatrix} \end{aligned}$$

L'addition et la multiplication matricielles sont des lois de composition interne sur $\mathscr{M}_3(\mathbb{R})$.

Remarque

Si $M\times N = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}$, alors $c_{ij} = a_{i1}\times b_{1j} + a_{i2}\times b_{2j} + a_{i3}\times b_{3j}$

exemples

- $\begin{pmatrix} 1 & 3 & 2 \\ 2 & 0 & 1 \\ -1 & -2 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 1 & -2 \\ -2 & 5 & -1 \\ -4 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 4 & 0 \\ 0 & 5 & 0 \\ -5 & -2 & 4 \end{pmatrix}$
- $\begin{pmatrix} 1 & 1 & 2 \\ 2 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} -1 & 1 & -2 \\ 1 & 2 & -1 \\ 1 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 7 & -1 \\ -2 & 2 & -2 \\ 3 & 3 & 2 \end{pmatrix}$

1.2 Partie stable pour une L.C.I - loi induite

1.2.1 Partie stable

Définition 1.4

Soit $(E, *)$ un ensemble non vide muni d'une loi de composition interne $*$ et S une partie de E.
On dit que S est une partie stable $(E, *)$ si $\forall (x, y) \in S^2, x * y \in S$.

Exemples

- Dans $\mathbb{Z}$, l'ensemble des nombres pairs est stable pour l'addition (la somme de deux nombres pairs est un nombre pair) ou pour la multiplication (le produit de deux nombres pairs est un nombre pair)
- Dans $\mathbb{Z}$,, l'ensemble des nombres impairs est stable pour la multiplication (le produit de deux nombres impairs est un nombre impair) mais n'est pas stable pour l'addition (la somme de deux nombres impairs n'est pas un nombre impair).
- Dans E^E, l'ensemble des injections, l'ensemble des surjections et l'ensemble des bijections sont stables pour $\circ$ (la composée de deux injections (resp. deux surjections, deux bijections) est une injection (resp. une surjection, une bijection)).
- Dans $\mathbb{C}$, l'ensemble $\mathbb{U}$ des nombres complexes de module 1 est stable pour la multiplication (un produit de deux nombres complexes de module 1 est un nombre complexe de module 1 .
- l'ensemble : $E = \left\{ M(a, b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad /(a, b) \in \mathbb{R}^2 \right\}$ est une partie stable dans $(\mathscr{M}_2(\mathbb{R}), \times)$

  En effet : Soient $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ et $B = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$ deux éléments de E. On a:

  $$A \times B = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(bc + ad) \\ bc + ad & ac - bd \end{pmatrix}$$

  Donc $M(a, b) \times M(c, d) = M(ac - bd, bc + ad) \in E$

1.2.2 Loi induite

Définition 1.5

Soient E un ensemble non vide muni d'une loi de composition interne $*$. Soit F une partie non vide de E stable pour $*$

L'application $\begin{array}{ccc} \mathrm{F} \times \mathrm{F} & \longrightarrow & \mathrm{F} \\ (\mathrm{x}, \mathrm{y}) & \longmapsto & x * y \end{array}$ est appelée loi induite par $*$ sur F.

Exemples

- la multiplication dans $\mathbb{Z}$ induit une loi sur l'ensemble $\{1; -1\}$
- la multiplication dans $\mathbb{R}$ induit une loi sur l'intervalle $]0, +\infty[$

1.3 Propriétés usuelles d'une loi de composition interne

1.3.1 Commutativité

Définition 1.6

Soit $\star$ une loi interne sur un ensemble E.

On dit que la loi $\star$ est commutative dans E si, $\forall(x, y) \in \mathrm{E}^2 : x \star y = y \star x$

1.3.2 Associativité

Définition 1.7

Soit $\star$ une loi interne sur un ensemble E.

On dit que la loi $\star$ est associative dans E si $\forall(x, y, z) \in \mathrm{E}^3 : (x \star y) \star z = x \star (y \star z)$

Exemples

- L'addition et la multiplication sont commutatives et associatives dans $\mathbb{Z}$. Mais ce n'est pas le cas pour la soustraction.
- La composition des applications dans $\mathcal{F}(X, X)$ est associative, mais elle n'est pas commutative (trouver un contre-exemple).
- Soit $n \in \mathbb{N}^{\star}$, on définit la somme et le produit dans $\mathbb{Z}/n\mathbb{Z}$ par :
  $\forall \bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} \dot{+} \bar{b} = \overline{a+b}$ et $\bar{a} \dot{\times} \bar{b} = \overline{a \times b}$
  Les lois $\dot{+}$ et $\dot{\times}$ sont commutatives et associatives dans $\mathbb{Z}/n\mathbb{Z}$.
- l'addition est associative et commutative dans $(\mathscr{M}_2(\mathbb{R}), +)$ et dans $(\mathscr{M}_3(\mathbb{R}), +)$.
- la multiplication est associative dans $(\mathscr{M}_2(\mathbb{R}), \times)$ et dans $(\mathscr{M}_3(\mathbb{R}), \times)$, mais elle n'est pas commutative.
  En effet $\begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix} \times \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 14 & 3 \\ -2 & -6 \end{pmatrix}$ et $\begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix} \times \begin{pmatrix} 5 & 1 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 10 & 2 \\ 29 & -2 \end{pmatrix}$
- Soient $\mathcal{T}$ l'ensemble des translations du plan, $\mathcal{R}_{\Omega}$ l'ensemble des rotations de centre Ω et $\mathcal{H}_{\Omega}$ l'ensemble des homothéties de centre Ω.
  Les ensembles $(\mathcal{T}, \circ)$, $(\mathcal{R}_{\Omega}, \circ)$ et $(\mathcal{H}_{\Omega}, \circ)$ sont des magmas associatifs commutatifs.

1.3.3 Distributivité

Définition 1.8

Soit E un ensemble muni de deux lois de composition internes $\star$ et $\top$.

- On dit que $\top$ est distributive à gauche sur $\star$ si : $\forall(x, y, z) \in E^3, x\top(y \star z) = (x\top y) \star (x\top z)$
- On dit que $\top$ est distributive à droite sur $\star$ si : $\forall(x, y, z) \in E^3, (x \star y)\top z = (x\top z) \star (y\top z)$
- On dit que $\top$ est distributive sur $\star$ si $\top$ est distributive à gauche **et** à droite sur $\star$ dans E.

Remarque

Si la loi $\top$ est commutative, alors, $\top$ est distributive sur $\star$ dans E si $\top$ est distributive à gauche **ou** à droite sur $\star$ dans E.

Exemples

- Dans $\mathbb{C}$, la multiplication est distributive sur l'addition mais l'addition n'est pas distributive sur la multiplication.
- Dans $\mathbb{Z}/n\mathbb{Z}$, la multiplication $\dot{\times}$ est distributive sur l'addition $\dot{+}$ mais l'addition n'est pas distributive sur la multiplication.
- Dans $\mathscr{M}_2(\mathbb{R})$ et dans $\mathscr{M}_3(\mathbb{R})$, la multiplication matricielle est distributive sur l'addition mais l'addition n'est pas distributive sur la multiplication.
- Dans $\mathcal{P}(\mathrm{E})$, l'intersection est distributive sur la réunion et la réunion est distributive sur l'intersection.
- Dans $(\mathbb{R}^R, \circ)$, la loi $\circ$ est distributive à droite sur $+$, mais pas à gauche $((g+h)\circ f = g\circ f + h\circ f$, mais en général, $f\circ(g+h) \neq f\circ g + f\circ h$.

1.3.4 Éléments particuliers d'une l.c.i.

1.3.4.1 Élément neutre

Définition 1.9

Soit E un ensemble non vide muni d'une loi de composition interne $\star$ et $e \in E$.
On dit que e est un élément neutre pour $\star$ dans E si: $\forall x \in E:\ e\star x = x\star e = x$.

Remarque

Si $\star$ est commutative alors : e est un élément neutre pour $\star$ dans $E \Leftrightarrow \forall x \in E : e\star x = x$

Proposition : Unicité de l'élément neutre

Soit $(E,\star)$ un ensemble muni d'une loi de composition interne $\star$.
Si la loi $\star$ admet un élément neutre dans E alors il est unique.

Démonstration

Soient e et e' deux éléments neutres distincts de la loi $\star$.
On a : e est neutre pour $\star$, donc $e\star e' = e'$ De même e' est neutre pour $\star$, donc $e\star e' = e$.
D'où $e = e'$

Exemples

- 0 est un élément neutre de $(\mathbb{N};+)$, $(\mathbb{Z};+)$, $(\mathbb{Q};+)$, $(\mathbb{R};+)$ et $(\mathbb{C};+)$
- 1 est un élément neutre de $(\mathbb{N};\times)$, $(\mathbb{Z};\times)$, $(\mathbb{Q};\times)$, $(\mathbb{R};\times)$ et $(\mathbb{C};\times)$
- Dans l'ensemble $\mathscr{P}(E)$, $\varnothing$ est neutre pour $\cup$ et E est neutre pour $\cap$.
- Dans $\mathscr{F}(\mathbb{R};\mathbb{R})$, la fonction identique $Id : x \mapsto x$ est neutre pour la composition.
- La matrice nulle $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est neutre dans $(\mathscr{M}_2(\mathbb{R});+)$ et on a:
$$(\forall M \in \mathscr{M}_2(\mathbb{R}))\ M + O_2 = O_2 + M = M$$
- La matrice identité $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est neutre dans $(\mathscr{M}_2(\mathbb{R});\times)$ et on a :
$$(\forall M \in \mathscr{M}_2(\mathbb{R}))\ M \times I_2 = I_2 \times M = M$$

- De même, la matrice identité $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est neutre dans $(\mathscr{M}_3(\mathbb{R}); \times)$.
- La loi soustraction définie sur $\mathbb{R}$ ne possède pas d'élément neutre.

1.3.4.2 Éléments symétrisables :

Définition 1.10

Soit $(E, \star)$ un ensemble non vide muni d'une loi de composition interne $\star$ d'élément neutre e.

On dit que x (élément de E) est symétrisable pour $\star$ dans E si $\exists x' \in E \ : \ x \star x' = x' \star x = e$.

Remarque

- si x' est un symétrique de x pour la loi $\star$, alors x est un symétrique de x' pour la même loi. on dit alors que x et x' sont symétriques (ou symetrisables) dans $(E;^\star)$.
- Si la loi $\star$ est commutative, alors on peut se contenter de l'une des relations $x \star x' = e$ ou $x' \star x = e$

Exemples

- Dans $(\mathbb{Z}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{R}; +)$ et $(\mathbb{C}; +)$, tout élément a admet un symétrique noté $-a$, appelé opposé de a
- Dans $(\mathbb{Q}^\star; \times)$, $(\mathbb{R}^\star; \times)$ et $(\mathbb{C}^\star; \times)$, tout élément a admet un symétrique noté a^{-1} ou $\frac{1}{a}$, appelé inverse de a.
- Dans $(\mathscr{P}(E); \cap)$, l'unique élément symétrisable est E et dans $(\mathscr{P}(E); \cup)$, l'unique élément symétrisable est $\varnothing$.
- Dans $(\mathbb{Z}/n\mathbb{Z}; +)$, tout élément $\bar{a}$ admet un symétrique qui est $-\bar{a}$ (ou encore $\overline{(-a)}$).
- Dans $(\mathbb{Z}/5\mathbb{Z}; \times)$, tout élément $\bar{a}$ différent de $\bar{0}$ admet un inverse.
- Dans $(\mathbb{Z}/4\mathbb{Z}; \times)$, l'élément $\bar{2}$ n'admet pas d'inverse.
- Dans $(\mathscr{M}_2(\mathbb{R}); +)$, toute matrice $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ admet comme symétique la matrice notée $-A$ et on a : $-A = \begin{pmatrix} -a & -c \\ -b & -d \end{pmatrix}$.
- Dans $(\mathscr{M}_2(\mathbb{R}); \times)$, si $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ et $\delta = ad - bc \neq 0$, alors A est inversible et on a:

  $A^{-1} = \begin{pmatrix} \frac{d}{\delta} & \frac{-c}{\delta} \\ \frac{-b}{\delta} & \frac{a}{\delta} \end{pmatrix}$ (On vérifie aisément que : $A \times A^{-1} = A^{-1} \times A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$).

  Par exemple La matrice $A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ est inversible et on a: $A^{-1} = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}$.

Proposition

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

Si un élément a de E admet un symétrique dans E, alors ce symétrique est unique.

Démonstration

Supposons qu'il existe deux éléments b et c dans E tels que : $a \star b = b \star a = e$ et $a \star c = c \star a = e$

L'associativité de la loi $\star$ permet alors d'écrire: $b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c$

Donc $b = c$.

1.3.4.3 Symétrique de la composée de deux éléments par une L.C.I :

Proposition

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

Si x et y sont deux éléments de E symétrisables , alors $(x \star y)' = y' \star x'$.

Démonstration

Soient x et y deux éléments symétrisables de E de symétriques respectifs x' et y'

$$(x \star y) \star (y' \star x') = x \star (y \star y') \star x' = x \star e \star x' = x \star x' = e$$
$$(y' \star x') \star (x \star y) = y' \star (x' \star x) \star y = y' \star e \star y = y' \star y = e$$

Donc, $x \star y$ est symétrisable et $(x \star y)' = y' \star x'$.

Notons que l'associativité de $\star$ est nécessaire.

Exemples

- Dans $\mathbb{C}^\star$, l'inverse $\dfrac{1}{z_1 \times z_2}$ de $z_1 \times z_2$ est $\dfrac{1}{z_1} \times \dfrac{1}{z_2}$
- Dans l'ensemble des bijections d'un ensemble E sur lui-même, la bijection réciproque $(g \circ f)^{-1}$ de $g \circ f$ est $f^{-1} \circ g^{-1}$. (qui est en général différent de $g^{-1} \circ f^{-1}$)
- Si A et B sont deux matrices inversibles dans $(\mathscr{M}_2(\mathbb{R}), \times)$ alors la matrice $A \times B$ est également inversible et on a: $(A \times B)^{-1} = B^{-1} \times A^{-1}$

1.3.4.4 Éléments réguliers ou simplifiables pour une L.C.I :

Définition 1.11

Soit $(E, \star)$ un magma et $a \in E$.

On dit que a est régulier pour $\star$ dans E si : $\forall (x, y) \in E^2$: $\begin{cases} x \star a = y \star a & \Rightarrow & x = y & (1) \\ a \star x = a \star y & \Rightarrow & x = y & (2) \end{cases}$

Si (1) est vérifié on dit que a est régulier à droite.

Si (2) est vérifié on dit que a est régulier à gauche.

Exemples :

- Dans $\mathbb{C}$, tout élément est simplifiable pour l'addition : $\forall (z, z', z'') \in \mathbb{C}^3 : (z + z' = z + z'' \Rightarrow z' = z'')$
- Dans $\mathbb{C}$, les éléments simplifiables pour la multiplication sont les complexes non nuls : $\forall (z, z', z'') \in \mathbb{C}^\star \times \mathbb{C} \times \mathbb{C}\, (z \times z' = z \times z'' \Rightarrow z' = z'')$. Mais attention, on ne simplifie pas par $0 (0 \times 1 = 0 \times 2$ mais $1 \neq 2)$.
  Donc, $az = az' \# z = z'$ mais $(az = az'$ et $a \neq 0) \Rightarrow z = z'$
- On considère dans $\mathscr{M}_2(\mathbb{R})$ les matrices suivantes:

$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, B = \begin{pmatrix} 2 & -6 \\ -1 & 3 \end{pmatrix}, C = \begin{pmatrix} -2 & 10 \\ 1 & -5 \end{pmatrix}$

Calculons: $A \times B$ et $A \times C$

$A \times B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \times \begin{pmatrix} 2 & -6 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 2-2 & -6+6 \\ 4-4 & -12+12 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$A \times C = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} -2 & 10 \\ 1 & -5 \end{pmatrix} = \begin{pmatrix} 2-2 & 10-10 \\ 4-4 & -20+20 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Donc l'égalité $A \times B = A \times C$ n'entraine pas nécessairement $B = C$

- Dans E^E, les éléments simplifiables à gauche sont les injections, les éléments simplifiables à droite sont les surjections et les éléments simplifiables sont les bijections.

1.4 Morphismes :

1.4.1 Définitions et exemples

Définition 1.12

Soient $(E, *)$ et $(F, \perp)$ deux ensembles munis de deux l.c.i et f une application de E dans F.

- On dit que f est un morphisme (ou homomorphisme) de $(E, *)$ dans $(F, \top)$ si on a:

$$\forall (x, y) \in E^2 : f(x * y) = f(x) \top f(y)$$

- Si de plus f est bijective, on dit que f est un isomorphisme de $(E, *)$ dans $(F, \top)$ et les ensembles E et F sont dits isomorphes.
- un morphisme de $(E, *)$ dans lui même s'appelle un endomorphisme de $(E, *)$.
- un endomorphisme bijectif de $(E, *)$ s'appelle un automorphisme de $(E, *)$.

Exemples

1. Soit l'application $\begin{array}{rccc} f : & (\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}^*, \times) \\ & x & \longmapsto & 2^x \end{array}$

   On a pour tout $(x; y) \in \mathbb{Z}^2$: $\quad f(x+y) = 2^{x+y} = 2^x \times 2^y = f(x) \times f(y)$

   Par conséquent, f est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}^*, \times)$
2. On considère l'application: $\begin{array}{rccc} g : & (]0; +\infty[, \times) & \longrightarrow & (\mathbb{R}, +) \\ & x & \longmapsto & ln(x) \end{array}$

   on a pour tout $(x; y) \in (]0; +\infty[)^2 : g(xy) = \ln(xy) = \ln x + \ln y = g(x) + g(y)$

   Par conséquent, g est un morphisme de $]0; +\infty[$ dans $\mathbb{R}$.
3. On considère l'application: $\begin{array}{rccc} h : & (\mathbb{C}, \times) & \longrightarrow & (\mathbb{R}, \times) \\ & z & \longmapsto & |z| \end{array}$

   On a : $\forall (z_i; z_2) \in \mathbb{C}^2$: $\quad h(z_1 \times z_2) = |z_1 \times z_2| = |z_1| \times |z_2| = h(z_1) \times h(z_2)$

   Par conséquent, h est un morphisme de $(\mathbb{C}, \times)$ dans $(\mathbb{R}; \times)$

4. On considère l'application: $K: \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathscr{M}_2(\mathbb{R}),\times) \\ x & \longmapsto & \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \end{array}$

   On a $\forall(x;y)\in\mathbb{R}^2: k(x+y)=\begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$.

   D'autre part: $k(x)\times k(y)=\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\times\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$.

   Donc $k(x)\times k(y)=k(x+y)$. Par conséquent, k est un morphisme de $(\mathbb{R};+)$ dans $(\mathscr{M}_2(\mathbb{R});\times)$

5. On considère l'application: $\varphi: \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{C}^*,\times) \\ \theta & \longmapsto & e^{i\theta} \end{array}$

   On a pour tout $(\theta_1;\theta_2)\in\mathbb{R}^2: \varphi(\theta_1+\theta_2)=e^{i(a+a_2)}=e^{i\theta_1}\times e^{i\theta_2}=\varphi(\theta_1)\times\varphi(\theta_2)$

   Par conséquent. φ est un morphisme de $(\mathbb{R};+)$ dans $(\mathbb{C}^*;\times)$

1.4.2 Propriétés d'un morphisme

Propriétés

Soit f un morphisme de $(E,*)$ dans $(F,\top)$

1. $f(E)$ est une partie stable de $(F,\top)$
2. Si $*$ est associative dans E, alors $\top$ est associative dans $f(E)$.
3. Si $*$ est commutative dans E, alors $\top$ est commutative dans $f(E)$.
4. Si e est l'élément neutre dans $(E,*)$ alors $f(e)$ est l'élément neutre dans $(f(E),\top)$.
5. Si e est l'élément neutre dans $(E,*)$ et x est symetrisable de symétrique x' dans $(E,*)$, alors $f(x)$ est symetrisable dans $(f(E),\top)$ et a pour symétrique $f(x')$.

Démonstration

1. Soient y_1 et y_2 deux éléments de $f(E)$. Donc il existe $(x_1;x_2)\in E^2$ tels que : $y_1=f(x_1)$ et $y_2=f(x_2)$.
   Puisque f est un morphisme de $(E;*)$ dans $(F;T)$, alors:
   $y_1Ty_2=f(x_1)Tf(x_2)=f(x_1*x_2)$
   Comme $*$ est une loi interne sur E, alors $x_1*x_2\in E$, et donc $f(x_1*x_2)\in f(E)$. par suite, $y_1\top y_2\in f(E)$.
   D'où, $f(E)$ est une partie stable de $(F;T)$.
2. Soient $(u;v;w)\in(f(E))^3$. Donc il existe $(x;y;z)\in E^3$ tels que : $u=f(x)$ et $v=f(y)$ et $w=f(z)$.
   puisque f est un morphisme de $(E;*)$ dans $(F;T)$ alors:
   $(uTv)Tw=(f(x)Tf(y))Tf(z)=f(x*y)Tf(z)=f[(x*y)*z]$
   Et si la loi * est associative dans $(E;*)$, alors :
   $(uTv)Tw=f[x*(y*z)]=f(x)Tf(y*z)=f(x)T[f(y)Tf(z)]=uT(vTw)$
   par suite, la loi T est associative dans $(f(E);T)$.
3. Supposons que la loi * est commutative dans $(E;*)$. En conservant les notations de la question précédente, on obtient:
   $y_1\top y_2=f(x_1)\top f(x_2)=f(x_1*x_2)=f(x_2*x_1)=f(x_2)\top f(x_1)=y_2\top y_1$

ce qui montre bien que la loi T est commutative dans $(f(E); \text{T})$.

4. Soit $u \in f(E)$. Il existe alors $x \in E$ tel que $u = f(x)$.
   On suppose que la loi $*$ admet un élément neutre e dans $(E; *)$.
   Donc : $u \top f(e) = f(x) T f(e) = f(x * e) = f(x) = u$
   On montre de même que $f(e) \top u = u$, ce qui entraine que $f(e)$ est neutre dans $(f(E); \top)$
5. Soit x' le symétrique d'un élément x dans $(E; *)$.
   on a : $x * x' = e$ et $x' * x = e$, et f un morphisme de $(E; *)$ dans $(F; \top)$,
   donc $f(x) T f\left(x'\right) = f\left(x * x'\right) = f(e)$ et $f\left(x'\right) T f(x) = f\left(x' * x\right) = f(e)$.
   Comme $f(e)$ est neutre dans $(f(E); T)$, alors $f(x)$ a pour symétrique $f\left(x'\right)$ dans $(f(E); T)$.

Remarque

- Si f est un morphisme de $(E, *)$ dans $(F, \top)$, alors f transfert les propriétés de $(E, *)$ à $(f(E), \top)$.
- Si de plus f est surjectif alors f transfert les propriétés de $(E, *)$ à $(F, \top)$.

Chapter 2 Structure de groupe

2.1 Groupe :

2.1.1 Définition et exemples

Définition 2.1

Soit G un ensemble muni d'une loi de composition interne $*$.

On dit que $(G, \star)$ est un groupe si, $\begin{cases} \star \text{ est associative dans} G \\ \star \text{ admet un élément neutre dans} G. \\ \text{Tout élément de } G \text{ est symétrisable pour } (G, \star). \end{cases}$.

Si de plus, la loi $\star$ est commutative, on dit que $(G, \star)$ est un groupe commutatif ou abélien.

Exemples

1. Les ensembles $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs.
2. les ensembles $(Q^*; \times) \cdot (\mathbb{R}^*; \times)$ et $(C^*; \times)$ sont des groupes abéliens,
3. $(\mathbb{Z}^*; \times)$ n'est pas un groupe, car les seuls éléments symétrisables de $(\mathbb{Z}^*; \times)$ sont 1 et -1.
4. Les ensembles $\left(Q_+^*; \times\right)$ et $\left(\mathbb{R}_+^*; \times\right)$ sont des groupes commutatifs.
5. Les ensembles $(\mathscr{M}_2(\mathbb{R}); +)$ et $(\mathscr{M}_3(\mathbb{R}); +)$ sont des groupes commutatifs, mais $(\mathscr{M}_2(\mathbb{R}); \times)$ n'est pas un groupe car les matrices $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, par exemple, ne sont pas inversibles dans $(\mathscr{M}_2(R); \times)$
6. Les ensembles $(\mathcal{V}_2; +)$ et $(\mathcal{V}_3; +)$ sont des groupes commutatifs.
7. $(\mathbb{Z}/6\mathbb{Z}; +)$ et $(\mathbb{Z}/5\mathbb{Z}; \times)$ sont des groupes commutatifs, cependant $(\mathbb{Z}/4\mathbb{Z}; \times)$ n'en est pas un car $\overline{2}$ n'est pas inversible dans $(\mathbb{Z}/4\mathbb{Z}; \times)$.
8. La composée de deux rotations de même centre Ω et d'angles respectifs θ et θ' est une rotation de même centre Ω et d'angle $\theta + \theta'$. et on a : $R(\Omega; \theta) o R\left(\Omega; \theta'\right) = R\left(\Omega; \theta'\right) o R(\Omega; \theta)$ et le symétrique de la rotation $R(\Omega; \theta)$ est $R(\Omega; -\theta)$.

   L'ensemble des rotations de centre Ω, muni de la loi de composition est donc un groupe commutatif.

Proposition

Soit $(G; \star)$ un groupe. Alors :

1. G est non vide car il contient au moins son élément neutre.
2. L'élément neutre e de G est unique.
3. Le symétrique de tout élément de G est unique.
4. Pour tout $(x; y) \in G^2 \quad (x')' = x$ et $(x \star y)' = y' \star x'$.
5. Tout élément $a \in G$ est régulier. Autrement dit, pour tout $(a; x; y) \in G^3$:

$$(a \star x = a \star y \Rightarrow x = y) \quad \text{et} \quad (x \star a = y \star a \Rightarrow x = y)$$

Proposition

Soit $(G;\star)$ un groupe d'élément neutre e et $(a;b) \in G^2$ et a' le symétrique de a dans $(G;\star)$:

l'équation $a \star x = b$ admet une solution unique dans E qui est $x = a' \star b$.

l'équation $x \star a = b$) admet une solution unique dans E qui est $x = b \star a'$.

En d'autres termes: Pour tout $(a;b;x) \in G^3$: $(a \star x = b \Leftrightarrow x = a' \star b)$ et $(x \star a = b \Leftrightarrow x = b \star a')$

Exercice

Soit $\star$ la loi de composition définie sur $\mathbb{R}$ par : $\forall (x,y) \in \mathbb{R}^2$: $\quad x \star y = x + y - xy$

1. L'ensemble $\mathbb{R}$, muni de cette loi est-il un groupe commutatif?
2. Montrer que $a = 1$ n'est pas un élément régulier de $(\mathbb{R},\star)$
3. Calculer $\underbrace{x \star x \star \ldots \star x}_{n}$ pour $n \geq 1$
4. ($\mathbb{R}\backslash\{1\},\star$) est-il un groupe commutatif?

2.1.2 Sous groupe d'un groupe

Définition 2.2

Soit $(G;\star)$ un groupe et H une partie de G.

on dit que $(H;\star)$ est un sous-groupe de $(G;\star)$ lorsque:

- H est une partie stable de $(G;\star)$, c'est-à-dire: $\left(\forall (x;y) \in H^2 : x \star y \in H\right)$
- $(H;\star)$ est un groupe.

Exemples

1. ($\mathbb{Z};+$) est un sous-groupe de $(\mathbb{R};+)$
2. $\left(\mathbb{R}_+^*;\times\right)$ est un sous-groupe de $(\mathbb{R}^*;\times)$.
3. L'ensemble $\mathbb{U}$ constitué des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*;\times)$.
4. L'ensemble des racines n-ièmes de l'unité est un sous-groupe de $(\mathbb{C}^*;\times)$.
5. $(\mathbb{Z};\times)$ n'est pas un sous-groupe de $(\mathbb{R};\times)$.

Remarques

- Si $(G;\star)$ est un groupe, alors G et $\{e\}$ sont des sous-groupes de $(G;\star)$, appelés sous-groupes triviaux de G.
- Un sous groupe H d'un groupe $(G;\star)$ tel que $H \neq \{e\}$ et $H \neq G$, s'appelle sous groupe propre de $(G;\star)$.

Proposition

Soit $(H;\star)$ un sous groupe d'un groupe $(G;\star)$ d'élément neutre e.

1. $H \neq \varnothing$
2. e est l'élément neutre dans $(H;\star)$.
3. $\forall x \in H$: $x' \in H$, où x' le symétrique de x dans $(G;\star)$.
4. $\left(\forall (x;y) \in H^2\right)$: $x \star y \in H$.
5. $\left(\forall (x;y) \in H^2\right)$: $x \star y' \in H$, où y' le symétrique de y dans $(G;\star)$.

2.1.3 Propriété caractéristique d'un sous groupe

Proposition

Soit $(G;*)$ un groupe d'élément neutre e, et H une partie de G.

H est un sous-groupe de $(G;\star) \Leftrightarrow \begin{cases} H \neq \varnothing \\ \left(\forall (x;y) \in H^2\right) : x \star y' \in H \end{cases}$ où y' est le symétrique de y dans $(G;\star)$

Remarque importante

la propriété caractéristique précédente s'écrit:

- En notation additive, $\begin{cases} H \neq \varnothing \\ \left(\forall (x;y) \in H^2\right) \quad x - y \in H \end{cases}$
- En notation multiplicative, $\begin{cases} H \neq \varnothing \\ \left(\forall (x;y) \in H^2\right) \quad x.y^{-1} \in H \end{cases}$
- Muni de la loi induite, un sous-groupe est un groupe, pour montrer que l'on a affaire à un groupe : on démontre en général que c'est un sous-groupe d'un groupe usuel. Le lecteur est donc invité à bien connaitre les exemples classiques cités précédemment.

2.1.4 Morphisme de groupes

Proposition

Soit f un morphisme d'un d'un groupe $(G,\star)$ dans un groupe $(H,\top)$. On a alors:

- $f\left(e_G\right) = e_H$
- $\forall x \in G, \quad f\left(x'\right) = [f(x)]'$.

Remarque

Un morphisme de groupe transforme le neutre de $(G,\star)$ en le neutre de $(H,\top)$ et le symétrique dans $(G,\star)$ en symétrique dans $(H,\top)$.

Proposition

Soit f un morphisme de $(G,\star)$ dans $(H,\top)$.

1. Si $(G,\star)$ est un groupe, alors $(f(G),\top)$ est un groupe.
2. Si $(G,\star)$ est un groupe abélien, alors $(f(G),\top)$ est un groupe abélien.

Remarques

- Si le morphisme f est surjectif ou est un isomorphisme de groupes alors $f(G) = F$, et dans ce cas, l'image du groupe $(G;\star)$ par f est le groupe $(F;\top)$. On dit alors que le morphisme f transfère " la structure du groupe $(G;\star)$, en celle du groupe $(F;\top)$
- Si $(G,\star)$ et $(H,\top)$ sont deux ensembles isomorphes, alors $(G,\star)$ et $(H,\top)$ ont la même structure.

Chapter 3 Anneau - corps

3.1 Structure d'anneaux

3.1.1 Définition et exemples

Définition 3.1

Soit $(A, \star, \top)$ un ensemble muni de deux lois de compositions interne $\star$ et $\top$.

On dit que $(A, \star, \top)$ est un anneau Si : $\begin{cases} (A, \star) \text{ est un groupe commutatif} \\ \top \text{ est distributive par rapport à } \star \\ \top \text{ est associative} \end{cases}$

Si de plus la loi $\top$ est commutative, alors l'anneau $(A, \star, \top)$ est dit anneau commutatif.

Si de plus la loi $\top$ admet un élément neutre , alors l'anneau $(A, \star, \top)$ est dit anneau unitaire.

Notation

- Lorsqu'il n'y a pas d'ambiguïté, on note les lois $\star$ et $\top$ respectivement par $+$ (notation additive) et $\times$ (notation multiplicative).
  - On note 0 (ou o_A), l'élément neutre pour $+$, appelé le zéro de l'anneau A et on note 1 ou (1_A) l'élément neutre pour $\times$, appelé l'élément unité de l'anneau $(A, +, \times)$.
  - on note couramment le composé $x.y$ ou même xy au lieu de $x \times y$
  - Le symétrique de $x \in A$ pour l'addition (opposé de x) est noté $-x$
  - Le symétrique de $x \in A$ pour la multiplication (inverse de x), s'il existe, est noté x^{-1}.
- Soit $(A; +; \times)$ un anneau unitaire et Soient $x \in A$ et $n \in \mathbb{Z}$.
  La notation nx dans l'anneau $(A; +; \times)$ est définie par :

$$nx = \underbrace{x + x + \ldots + x}_{nfois} \text{ si } n \geq 1 \quad ; \quad nx = \underbrace{(-x) + (-x) + \ldots + (-x)}_{-n \text{ fois}} \quad \text{si } n \leq -1 \quad ; \quad 0_A x = 0_A$$

- De même, la notation x^n dans l'anneau $(A; +; \times)$ est définie par :

$$x^n = \underbrace{x \times x \times \ldots \times x}_{n/ \text{ fois}} \text{ si } n \geq 1 \quad ; \quad x^n = \underbrace{x^{-1} \times \ldots \times x^{-1}}_{-n \text{ fois}} \quad \text{si } x \text{ est inversible et } n \leq -1; \quad x^0 = 1_A$$

- Ces notations sont très utiles dans les calculs numériques (réels et complexes) et matriciels.

Exemples

1. $(\mathbb{Z}; +; \times)$, $(\mathbb{Q}; +; \times)$, $(\mathbb{R}; +; \times)$ et $(\mathbb{C}; +; \times)$ sont des anneaux commutatifs unitaires, mais $(\mathbb{N}; +; \times)$ n'est pas un anneau car ($\mathbb{N}; +$) n'est pas un groupe.
2. Pour $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}; +; \times)$ est un anneau commutatif unitaire. Son zéro est $\overline{0}$ et son élément unité est $\overline{1}$
3. $(\mathscr{M}_2(\mathbb{R}); +; \times)$ et $(\mathscr{M}_3(\mathbb{R}); +; \times)$ sont des anneaux unitaires non commutatifs. L'élément unité pour $(\mathscr{M}_2(\mathbb{R}); +; \times)$ est $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et l'élément unité pour l'anneau $(\mathscr{M}_3(\mathbb{R}); +; \times)$ est $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

3.1.2 Règles de calcul dans un anneau

Proposition

Soit $(A;+;\times)$ un anneau unitaire. Pour tout x, y de A, on a les propriétés suivantes:

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

3.1.3 Diviseurs de zéro dans un anneau

Définition 3.2

Soit $(A;+;\times)$ un anneau et $a \in A - \{0_A\}$.
On dit que a est un diviseur de zéro dans A s'il existe $b \in A - \{0_A\}$ tel que $a \times b = 0$ ou $b \times a = 0$.

Exemples

1. Dans l'anneau $\mathbb{Z}/6\mathbb{Z}$, l'élément $\overline{2}$ est un diviseur de zéro car : $\overline{2} \neq \overline{0}$ et $\overline{2} \times \overline{3} = \overline{3} \times \overline{2} = \overline{0}$.
   De même, $\overline{3}$ est un diviseur de zéro dans cet anneau.
2. Dans l'anneau $(\mathscr{M}_2(\mathbb{R});+;\times)$, l'élément $\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$ est un diviseur de zéro car:
$$\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \neq O_2 \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = O_2$$

Proposition

Soit $(A;+;\times)$ un anneau unitaire et $a \in A$.
Si a est un diviseur de zéro dans $(A;+;\times)$, alors a n'est pas inversible dans $(A;+;\times)$.

Remarques

- La réciproque de la proposition précédente n'est pas vraie. (un élément qui n'est pas diviseur de zéro dans un anneau $(A;+;\times)$, n'est pas forcement inversible).
- Si a est inversible dans un anneau $(A;+;\times)$, alors a n'est pas un diviseur de zéro.

Proposition

Soit $(A;+;\times)$ un anneau unitaire et $\mathbb{U}$ l'ensemble des éléments inversibles pour $\times$ dans A.
L'ensemble $(\mathbb{U};\times)$ est un groupe, appelé groupe des éléments inversibles de l'anneau $(A;+;\times)$

Exemples

1. les ensembles $(Q^*;\times) \cdot (\mathbb{R}^*;\times)$ et $(C^*;\times)$ sont les groupes d'éléments inversibles respectivement des anneaux $(\mathbb{Q};+;\times)$, $(\mathbb{R};+;\times)$ et $(\mathbb{C};+;\times)$.
2. L'ensemble $(\mathbb{U} = \{1,-1\};\times)$ est le groupe des éléments inversibles de l'anneau $((\mathbb{Z};+;\times)$.

3.1.4 Anneau intègre

Définition 3.3

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

On dit que $(A;+;\times)$ est un anneau intègre si A n'est pas réduit à $\{0_A\}$ et n'admet pas de diviseurs de zéro.

Exemples

1. $(\mathbb{Z};+;\times)$, $(\mathbb{Q};+;\times)$, $(\mathbb{R};+;\times)$ et $(\mathbb{C};+;\times)$ sont des anneaux commutatifs unitaires intègres.
2. $(\mathbb{Z}/5\mathbb{Z};+;\times)$ est un anneau commutatif unitaire intègre, mais $(\mathbb{Z}/6\mathbb{Z};+;\times)$ est un anneau commutatif unitaire non intègre. ($\overline{2}$ est un diviseur de zéro).
3. $(\mathscr{M}_2(\mathbb{R});+;\times)$ et $(\mathscr{M}_3(\mathbb{R});+;\times)$ sont deux anneaux unitaires non intègres.

3.2 Structure de corps

Définition 3.4

Soit $(\mathbb{K},+,\times)$ un anneau unitaire.

$(\mathbb{K},+,\times)$ est un corps si, et seulement si, tout élément non nul de $\mathbb{K}$ admet un inverse (pour $\times$) dans $\mathbb{K}$.

Un corps $(\mathbb{K},+,\times)$ est dit commutatif si la deuxième $\times$ est commutative.

Exemples

1. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps commutatifs.
2. $(\mathbb{Z},+,\times)$ est un anneau unitaire, mais qui n'est pas un corps, car le nombre 2 par exemple n'est pas inversible .

Théorème

Soit $\mathbb{K}$ un ensemble muni de deux lois de composition interne $\star$ et $\top$.

$$(\mathbb{K},\star,\top) \text{ est un corps si, et seulement si, } \begin{cases} (\mathbb{K},\star) \text{ est un groupe commutatif} \\ (\mathbb{K}^*,\top) \text{ est un groupe} \quad (\text{ avec } \mathbb{K}^* = \mathbb{K}-\{0_\mathbb{K}\}) \,. \\ \top \text{ est distributive par rapport à } \star \,. \end{cases}$$

Théorème

Soit $(\mathbb{K},\star,\top)$ un corps d'élément neutre $0_\mathbb{K}$ et d'unité $1_\mathbb{K}$. On pose $\mathbb{K}^* = \mathbb{K}-\{0_\mathbb{K}\}$

1. Tout élément de $\mathbb{K}^*$ est régulier pour $\top$.
2. $(\mathbb{K},*,\top)$ est un anneau intègre. ie $(\forall x,y \in \mathbb{K}: \; x\top y = 0_\mathbb{K} \Leftrightarrow x = 0_\mathbb{K}$ ou $y = 0_\mathbb{K})$.
3. Soit $a \in \mathbb{K}^*$ et a' son symétrique pour la loi $\top$ et $b \in \mathbb{K}$.
   Les équations $x\top a = b$ et $a\top x = b$ admettent les uniques solutions respectives $x = b\top a'$ et $x = a'\top b$.

Théorème

Pour tout entier relatif non nul n, on a :

- $\bar{k}$ est inversible dans $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ si et seulement $k \wedge \boldsymbol{n} = \mathbf{1}$
- $(\mathbb{Z}/\boldsymbol{n}\mathbb{Z},\overline{+},\overline{\times})$ est un corps si et seulement si $\boldsymbol{n}$ est premier.