Chapitre

Structures algébriques

I Lois de compositions interne - Morphisme

1 Lois de comosition interne

a Définition et exemples

D — **Définition**

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 $a * b$, aTb, $a \perp b, \ldots$
♣ Si $*$ est une loi de composition interne sur un ensemble E, on dit que E est muni de la loi $*$ et on écrit $(E,*)$. L'ensemble $(E,*)$ est appelé un **magma**.

Exemple

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 $\mathbb{R}^*$ l'est.
3. Dans $\mathbb{N}^*$, 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 : $(A,B) \longrightarrow A \cap B$
   - La réunion : $(A,B) \longrightarrow A \cup B$
   - La différence : $(A,B) \longrightarrow A \setminus B$
   - La différence symétrique : $(A,B) \longrightarrow A \Delta B$
5. L'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ (voir le chapitre : **Arithmétique dans** $\mathbb{Z}$) sont des lois de composition 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 $\mathscr{V}_2$ n'est pas une loi de composition interne car pour tout $\vec{u}; \vec{v} \in \mathscr{V}_\in$, on a : $\vec{u}.\vec{v} \notin \mathscr{V}_2$ ($\vec{u}.\vec{v} \in \mathbb{R}$)

10. Le produit vectoriel dans l'espace des vecteurs $\mathscr{V}_3$ est une loi de composition interne

11. L'ensemble $(\mathscr{T},\circ)$ des translation du plan est un magma. $\left(t_{\vec{u}}\circ t_{\vec{v}}=t_{\vec{u}+\vec{v}}\right)$

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

2 Ensemble des matrices carrées d'ordre 2 à coefficient réels

D Définition

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

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

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

a 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 :**

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

♣ **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 sont des lois de compositions interne sur $\mathscr{M}_2(\mathbb{R})$.

Exemple

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 $A+B$:

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

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

$$A\times B=\begin{pmatrix}5 & 1\\ 3 & -2\end{pmatrix}\times\begin{pmatrix}2 & 0\\ 4 & 3\end{pmatrix}=\begin{pmatrix}5\times2+1\times4 & 5\times0+1\times3\\ 3\times2+(-2)\times4 & 3\times0+(-2)\times3\end{pmatrix}=\begin{pmatrix}14 & 3\\ -2 & -6\end{pmatrix}$$

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

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

D Définition

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

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

Chaque coefficient a_{ij} se trouve de la $i^{\text{éme}}$ ligne et la $j^{\text{éme}}$ colonne.
L'ensemble des matrices carrées d'ordre 3 est noté par $\mathscr{M}_3(\mathbb{R})$

a 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 $\mathscr{M}_3(\mathbb{R})$

♣ **Somme de deux matrices :**

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

♣ **Produit de deux matrices :**

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

L'addition et la multiplication sont des lois de compositions 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 $c_{ij} = a_{i1} \times b_{1j} + a_{i2} \times b_{2j} + a_{i3} \times b_{3j}$

Exemple

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

4 Partie stable pour une $l.c.i$ - loi induite

a Partie stable

D **Définition**

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 de $(E,*)$ si $\forall (x,y)\in S^2$; $x*y\in S$

Exemple

1. Dans $\mathbb{Z}$, l'ensemble des nombres pairs $2\mathbb{N}$ 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)
2. Dans $\mathbb{Z}$, l'ensemble des nombres impairs $2\mathbb{N}+1$ 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).
3. 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)).
4. 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).
5. L'ensemble $E=\left\{M(a,b)=\begin{pmatrix}a&-b\\b&a\end{pmatrix}/\ (a,b)\in\mathbb{R}^2\right\}$ 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 $M(a,b)\times M(c,d)=M(ac-bd,bc+ad)\in E$

b Loi induite

D **Définition**

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

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

Exemple

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

II Propriétés usuelles d'une loi de composition interne

1 Commutativité

D **Définition**

Soit $*$ une loi de composition interne sur en ensemble E.
On dit que la loi $*$ est commutative dans E si, $\forall (x,y)\in E^2$; $x*y=y*x$

2 Associativité

D **Définition**

Soit $*$ une loi de composition interne sur un ensemble E.
On dit que la loi $*$ est associative dans E si, $\forall (x,y,z)\in E^3$; $(x*y)*z=x*(y*z)$

Exemple

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

3 Distributivité

D **Définition**

Soit E un ensemble muni de deux lois de compositions internes $*$ et $\top$.
♣ On dit que $\top$ est distributive à gauche sur $*$ si : $\forall (x,y,z)\in E^3$; $x\top(y*z)=(x\top y)*(x\top z)$
♣ On dit que $\top$ est distributive à droite sur $*$ si : $\forall (x,y,z)\in E^3$; $(x*y)\top z=(x\top z)*(y\top z)$
♣ On dit que $\top$ est distributive sur $*$ si $\top$ est distributive à gauche et à droite sur $*$ dans E.

Remarque

Si la loi $\top$ est commutative, alors $\top$ est distributive sur $*$ dans E si :

$\top$ est distributive à gauche **ou** à droite sur $*$ dans E

.

Exemple

1. Dans $\mathbb{C}$, la multiplication est distributive sur l'addition mais l'addition n'est pas distributive sur la multiplication.
2. Dans $\mathbb{Z}/n\mathbb{Z}$, la multiplication est distributive sur l'addition mais l'addition n'est pas distributive sur la multiplication.
3. 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.
4. Dans $\mathscr{P}(E)$, l'intersection est distributive sur la réunion et la réunion est distributive sur l'intersection.
5. Dans $(\mathbb{R}^{\mathbb{R}}, \circ)$, 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, $f\circ(g+h) \neq f\circ g + f\circ h$.

4 Éléments particuliers d'une $l.c.i$

a Élément neutre

D **Définition**

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

Remarque

Si $*$ est commutative alors : e est un élément neutre pour $*$ dans $E \iff \forall x \in E$; $e*x = x$

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

• Preuve

Soient e et e′ deux élément neutres distincts de la loi $*$
On a : e est l'élément neutre pour $*$, donc $e*e' = e'$. De même e′ est l'élément neutre pour $*$, donc $e*e' = e$
D'où : $e = e'$

Exemple

1. 0 est un élément neutre de $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$
2. 1 est un élément neutre de $(\mathbb{N},\times)$, $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ et $(\mathbb{C},\times)$
3. Dans l'ensemble $\mathscr{P}(E)$, $\emptyset$ est un élément neutre pour $\cup$ et E est l'élément neutre pour $\cap$
4. Dans $\mathscr{F}(\mathbb{R},\mathbb{R})$, la fonction identique $Id : x \longmapsto x$ est l'élément neutre pour la composition.
5. La matrice nulle $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est l'élément neutre dans $(\mathscr{M}_2(\mathbb{R}),+)$ et on a :
$$(\forall M \in \mathscr{M}_2(\mathbb{R})) \; ; \; M + O_2 = O_2 + M = M$$
6. La matrice identité $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est l'élément neutre dans $(\mathscr{M}_2(\mathbb{R}),\times)$ et on a :
$$(\forall M \in \mathscr{M}_2(\mathbb{R})) \; ; \; M \times I_2 = I_2 \times M = M$$
7. De même, la matrice identité $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est l'élément neutre dans $(\mathscr{M}_3(\mathbb{R}),\times)$
8. La loi soustraction définie sur $\mathbb{R}$ ne possède pas d'élément neutre.

b Éléments symétrisables

D **Définition**

Soit $(E,*)$ un ensemble non vide muni d'une loi de composition interne $*$ d'élément neutre e.
On dit que x (élément de E) est symétrisable pour $*$ dans E si : $\exists\, x' \in E$; $x*x' = x'*x = \mathrm{e}$

Remarque

♣ Si x' est un symétrique de x pour la loi $*$, alors x est un symétrique de x' pour la loi $*$. On dit alors que x et x' sont symétriques (ou symétrisables) dans $(E,*)$.
♣ Si la loi $*$ est commutative, alors on peut se contenter de l'une des relations :
$$x*x' = \mathrm{e} \quad \text{ou} \quad x'*x = \mathrm{e}$$

Exemple

1. Dans $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$, tout élément a admet un symétrique noté $-a$, appelé opposé de a.
2. Dans $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$, tout élément a admet un symétrique noté a^{-1} ou $\dfrac{1}{a}$, appelé inverse de a.
3. Dans $(\mathscr{P}(E),\cap)$, l'unique élément symétrisable est E et dans $(\mathscr{P}(E),\cup)$, l'unique élément symétrisable est $\emptyset$.

4. Dans $(\mathbb{Z}/n\mathbb{Z},+)$, tout élément $\overline{a}$ admet un symétrique qui est $-\overline{a}$ (ou encore $\overline{(-a)}$.
5. Dans $(\mathbb{Z}/5\mathbb{Z},\times)$, tout élément $\overline{a}$ différent de $\overline{0}$ admet un inverse.
6. $(\mathbb{Z}/4\mathbb{Z},\times)$, l'élément $\overline{2}$ n'admet pas d'inverse.
7. Dans $(\mathscr{M}_2(\mathbb{R}),+)$, toute matrice $A=\begin{pmatrix}a & c\\ b & d\end{pmatrix}$ admet comme symétrique la matrice notée $-A$ et on a :
$$-A=\begin{pmatrix}-a & -c\\ -b & -d\end{pmatrix}$$
8. 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 : $A^{-1}=\begin{pmatrix}\frac{d}{\delta} & \frac{-c}{\delta}\\ \frac{-b}{\delta} & \frac{a}{\delta}\end{pmatrix}$
$\left(\text{On vérifie aisément que : } A\times A^{-1}=A^{-1}\times A=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)$
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 $(E,*)$ 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.

• Preuve

Supposons qu'il existe deux éléments b et c dans E tels que : $a*b=b*a=\text{e}$ et $a*c=c*a=\text{e}$
L'associativité de la loi $*$ permet alors d'écrire : $b=b*\text{e}=b*(a*c)=(b*a)*c=\text{e}*c=\text{e}$
Donc : $b=c$

c Symétrique de la composée de deux éléments par une $l.c.i$

Proposition

Soit $(E,*)$ un ensemble muni d'une loi de composition interne associative $*$ et d'élément neutre e.
Si x et y sont deux éléments de E symétrisables, alors $(x*y)'=y'*x'$

• Preuve

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

$$(x*y)*(y'*x')=x*(y*y')*x'=x*\text{e}*x'=x*x'=\text{e}$$

$$(y'*x')*(x*y)=y'*(x'*x)*y=y'*\text{e}*y=y'*y=\text{e}$$

Donc, $x*y$ est symétrisable et $(x*y)' = y'*x'$
Notons que l'associativité de $*$ est nécessaire.

Exemple

1. Dans $\mathbb{C}^*$, l'inverse $\dfrac{1}{z_1 \times z_2}$ de $z_1 \times z_2$ est $\dfrac{1}{z_1} \times \dfrac{1}{z_2}$
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 $g^{-1} \circ f^{-1}$)
3. 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 : $(A \times B)^{-1} = B^{-1} \times A^{-1}$

d Éléments réguliers ou simplifiables pour une *l.c.i*

D Définition

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

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

Si (1) est vérifier, on dit que a est régulier à droite.
Si (2) est vérifier, on dit que a est régulier à gauche.

Exemple

1. Dans $\mathbb{C}$, tout élément est simplifiable pour l'addition : $\forall (z,z',z'') \in \mathbb{C}^3$; $(z+z' = z+z'' \implies z' = z'')$
2. Dans $\mathbb{C}$, les éléments simplifiables pour la multiplication sont les complexes non nuls : $\forall (z,z',z'') \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}$; $(z \times z' = z \times z'' \implies z' = z'')$.
   Mais **attention**, on ne simplifie pas par 0 ($0 \times 1 = 0 \times 2$ mais $1 \neq 2$)
   Donc : $az = az' \not\Rightarrow z = z'$ mais $(az = az' \text{ et } a \neq 0) \implies z = z'$
3. 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 $A \times C$
   $A \times B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \times \begin{pmatrix} 2 & -6 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 2-2 & -6+6 \\ 4-4 & -12+12 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
   $A \times C = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \times \begin{pmatrix} -2 & 10 \\ 1 & -5 \end{pmatrix} = \begin{pmatrix} 2-2 & 10-10 \\ 4-4 & -20+20 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
   Donc l'égalité $A \times B = A \times C$ n'entraîne pas nécessairement $B = C$
4. 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.

III Morphisme

D Définition

Soient $(E,*)$ et $(F,\top)$ deux ensembles muni 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 $(E,*)$.

Exemple

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

   On a pour tout $(x,y)\in\mathbb{Z}^2$; $f(x+y)=2^{x+y}=2^x\times 2^y=f(x)\times f(y)$
   Par conséquent, f est un morphisme de $(\mathbb{Z},+)$ vers $(\mathbb{Z}^*,\times)$

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 $(]0;+\infty[,\times)$ 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 pour tout $(z_1,z_2)\in\mathbb{C}^2$; $h(z_1\times z_2)=|z_1\times z_2|=|z_1|\times|z_2|=h(z_1)\times h(z_2)$
   Par conséquent, h est un morphisme de $(\mathbb{C},\times)$ dans $(\mathbb{R},\times)$.

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

   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 : $\begin{array}{rccc} \varphi: & (\mathbb{R},+) & \longrightarrow & (\mathbb{C}^*,\times) \\ & \theta & \longmapsto & \mathrm{e}^{i\theta} \end{array}$

   On a pour tout $(\theta_1,\theta_2)\in\mathbb{R}^2$; $\varphi(\theta_1+\theta_2)=\mathrm{e}^{i(\theta_1+\theta_2)}=\mathrm{e}^{i\theta_1}\times\mathrm{e}^{i\theta_2}=\varphi(\theta_1)\times\varphi(\theta_2)$
   Par conséquent, φ est un morphisme de $(\mathbb{R},+)$ dans $(\mathbb{C}^*,\times)$

1 Propriétés d'un morphisme

Propriété

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 $f(\mathrm{e})$ est l'élément neutre dans $(f(E),\top)$.
5. Si e est l'élément neutre dans $(E,*)$ et x est symétrisable de symétrie x' dans $(E,*)$, alors $f(x)$ est symétrisable dans $(f(E),\top)$ et a pour symétrique $f(x')$.

• Preuve

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 $(F,\top)$, alors $y_1\top y_2 = f(x_1)\top f(x_2) = f(x_1 * x_2)$ Comme $*$ est une loi de composition 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 $(F;\top)$
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 $(F,\top)$ alors :
   $(u\top v)\top w = (f(x)\top f(y))\top f(z) = f(x*y)\,f(z) = f[(x*y)*z]$
   Et si la loi $*$ est associative dans $(E,*)$, alors :
   $(u\top v)\top w = f[x*(y*z)] = f(x)\top f(y*z) = f(x)\top[f(y)\top f(z)] = u\top(v\top w)$
   Par suite, la loi $\top$ est associative dans $(f(E),\top)$
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 $\top$ est commutative dans $(f(E),\top)$
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 : $u\top f(\mathrm{e}) = f(x)\top f(\mathrm{e}) = f(x*\mathrm{e}) = f(x) = u$
   On montre de même que $f(\mathrm{e})\top u = u$, ce qui entraîne que $f(\mathrm{e})$ est neutre dans $(f(E),\top)$
5. Soit x' le symétrique d'un élément x dans $(E,*)$
   On a : $x*x' = \mathrm{e}$ et $x'*x = \mathrm{e}$ et f un morphisme de $(E,*)$ dans $(f(E),\top)$
   donc $f(x)\top f(x') = f(x*x') = f(\mathrm{e})$ et $f(x')\top f(x) = f(x'*x) = f(\mathrm{e})$
   Comme $f(\mathrm{e})$ est neutre dans $(f(E),\top)$, alors $f(x)$ a pour symétrique $f(x')$ dans $(f(E),\top)$

Remarque

• Si f est un morphisme de $(E,*)$ dans $(F,\top)$, alors f transforme les propriétés de $(E,*)$ à $(f(E),\top)$.

• Si de plus f est surjective ($f(E)=F$)alors f transfert les propriétés de $(E,*)$ à $(F,\top)$

IV Groupe

1 Définition et exemples

D **Définition**

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

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

Si de plus, la loi $*$ est commutative, on dit que $(\mathbb{C},*)$ est un groupe commutatif ou abélien.

Exemple

1. Les ensembles $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs.
2. Les ensembles $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ 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 $\left(\mathbb{Q}_+^*,\times\right)$ 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 inversible dans $(\mathscr{M}_2(\mathbb{R}),\times)$
6. Les ensembles $(\mathscr{V}_2,+)$ et $(\mathscr{V}_3,+)$ 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'est pas un groupe car $\overline{2}$ n'est pas inversible dans $(\mathbb{Z}/4\mathbb{Z},\times)$.
8. La composée de deux rotation 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 : $R(\Omega,\theta)\circ R(\Omega,\theta')=R(\Omega,\theta')\circ R(\Omega,\theta)$ et le symétrique de la rotation $R(\Omega,\theta)=R(\Omega,-\theta)$
   L'ensemble des rotations de centre Ω, muni de la loi de composition est donc un groupe commutatif.

Proposition

Soit $(G,*)$ 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 $(x,y)\in G^2$; $(x')'=x$ et $(x*y)'=y'*x'$

5. Tout élément $a \in G$ est régulier. Autrement dit, pour tout $(a,x,y) \in G^3$:

$$(a*x = a*y \Longrightarrow x = y) \quad et \quad (x*a = y*a \Longrightarrow x = y)$$

Proposition

Soit $(E,*)$ un groupe d'élément neutre e et $(a,b) \in G^2$ et a' le symétrique de a dans $(G,*)$:
♣ L'équation $a*x = b$ admet une solution unique dans E qui est $x = a'*b$
♣ L'équation $x*a = b$ admet une solution unique dans E qui est $x = b*a'$
En d'autre termes : Pour tout $(a,b,x) \in G^3$:

$$\left(a*x = b \Longleftrightarrow x = a'*b\right) \quad et \quad \left(x*a = b \Longleftrightarrow x = b*a'\right)$$

Exercice

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

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 $(\mathbb{R},*)$
3. Calculer $\underbrace{x*x*\ldots*x}_{n\ fois}$ pour $n \geqslant 1$
4. $(\mathbb{R}\backslash\{1\},*)$ est-il un groupe commutatif ?

2 Sous-groupe d'un groupe

D **Définition**

Soit $(G,*)$ un groupe et H une partie de G.
On dit que $(H,*)$ est un sous-groupe de $(G,*)$ lorsque :
• H est une partie stable de $(G,*)$, c'est-à-dire : $\left(\forall (x,y) \in H^2 \ ; \ x*y \in H\right)$
• $(H,*)$ est un groupe

Exemple

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 $(\mathbb{R},\times)$

Remarque

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

Proposition

Soit $(H,*)$ un sous-groupe d'un groupe $(G,*)$ d'élément neutre e.

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

3 Propriété caractéristique d'un sous-groupe

Proposition

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

$$H \text{ est un sous-groupe de } (G,*) \iff \begin{cases} H \neq \emptyset \\ \left(\forall (x,y) \in H^2\right)\ ;\ x*y' \in H \end{cases} \text{ où } y' \text{ est le symétrique de } y \text{ dans } (G,*)$$

Remarque

La propriété caractéristique précédente s'écrit :

• En notation additive, $\begin{cases} H \neq \emptyset \\ \left(\forall (x,y) \in H^2\right)\ ;\ x-y \in H \end{cases}$

• En notation multiplicative, $\begin{cases} H \neq \emptyset \\ \left(\forall (x,y) \in H^2\right)\ ;\ x.y^{-1} \in H \end{cases}$

• 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.

4 Morphisme de groupes

Proposition

Soit f un morphisme d'un groupe $(G,*)$ dans un groupe $(H,\top)$. On a alors :
• $f(e_G) = e_H$
• $\forall x \in G\ ;\ f(x') = (f(x))'$

Remarque

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

Proposition

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

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

Remarque

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

V Structure d'anneaux

1 définitions et exemples

D Définition

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

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

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

Notation

♣ Lorsqu'il n'y a pas d'ambiguïté, on note les lois $*$ et $\top$ respectivement par $+$ (notation additive) et $\times$ (notation multiplicative).
• On note 0 ou (0_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 $(A,*,\top)$.
• 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 :

$$nx=\underbrace{x+x+\ldots+x}_{n\ fois}\ si\ n\geqslant 1\quad ;\quad nx=\underbrace{(-x)+(-x)+\ldots+(-x)}_{-n\ fois}\ si\ n\leqslant -1\quad ;\quad 0_A x=0_A$$

• La notation x^n dans l'anneau $(A,+,\times)$ est définie par :

$$x^n=\underbrace{x\times x\times\ldots\times x}_{n\ fois}\ si\ n\geqslant 1\quad ;\quad x^n=\underbrace{x^{-1}\times x^{-1}\times\ldots\times x^{-1}}_{-n\ fois}\ si\ n\leqslant -1\quad ;\quad x^0=1_A$$

♣ Ces conditions sont très utiles dans les calculs numériques (réels et complexes) et matriciels.

Exemple

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 $I_3=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$

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 Diviseurs de zéro dans un anneau

D Définition

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

Exemple

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 :

$$\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \neq O_2 \quad et \quad \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = O_2$$

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 $(A, +, \times)$.

Remarque

• 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 $(A, +, \times)$.

Exemple

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

4 Anneau intègre

D Définition

Soit $(A, +, \times)$ un anneau.
On dit que $(A, +, \times)$ est un anneau intègre si A n'est pas réduit à $\{O_A\}$ et n'admet pas de diviseur de zéro.

Exemple

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.

VI Structure de corps

D Définition

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 loi $\times$ est commutative.

Exemple

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

T Théorème

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

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

T Théorème

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

1. Tout élément de $\mathbb{K}^*$ est régulier pour $\top$.
2. $(\mathbb{K},*,\top)$ est un anneau intègre. ie $(\forall x,y\in\mathbb{K}\ ;\ x\top y=0_\mathbb{K}\iff x=0_\mathbb{K}\ ou\ y=0_\mathbb{K})$
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 $x=a'\top b$

T Théorème

Pour tout entier relatif non nul n, on a :
• $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k\wedge n=1$
• $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps si et seulement si n est premier.