

# Chapitre 4

## Les structures algébriques

Evariste Galois est un [mathématicien français](#), né le

[25 octobre 1811](#) à Bourg-Égalité

(aujourd'hui [Bourg-la-Reine](#)) et mort le [31 mai 1832](#) à Paris.

Son nom a été donné à une branche des mathématiques dont il a posé les prémisses,

la [théorie de Galois](#). Il est un précurseur dans la mise en

évidence de la notion de [groupe](#) et un des premiers

à expliciter la correspondance entre

[symétries](#) et [invariants](#).

Sa « théorie de l'ambiguïté » est toujours féconde au XXI<sup>e</sup> siècle.

Mort à la suite d'un [duel](#), apparemment galant, à l'âge de vingt ans, il laisse un manuscrit

élaboré trois ans plus tôt, dans lequel il établit qu'une [équation algébrique](#) est résoluble par

[radicaux](#) si et seulement si le [groupe de permutations](#) de ses [racines](#) a une certaine structure,

qu'on appellera plus tard [résoluble<sup>a</sup>](#). Ce *Mémoire sur les conditions de résolubilité des équations*

*par radicaux*, publié par [Joseph Liouville](#) quatorze ans après sa mort, ainsi qu'un article *Sur*

*la théorie des nombres* paru alors qu'il avait dix-neuf ans, ont été considérés par ses successeurs,

en particulier [Sophus Lie](#), comme le déclencheur du [point de vue structural](#) et [méthodologique](#)

des [mathématiques modernes](#).



# Chapitre 4 :Les structures algébriques

## I. Lois de composition interne

### 1. Introduction

On désigne à l'ensemble des polynômes de degrés inférieur à n par  $P_n$  ou  $\mathbb{R}_n[n]$

$P \in \mathbb{R}_n[X]$  donc  $P$  est un polynôme de degré  $\leq n$ .  $(\forall (P, Q) \in (\mathbb{R}_n[n])^2)(\forall x \in \mathbb{R})$

$$(P + Q)(x) = P(x) + Q(x) \text{ et } (P \times Q)(x) = P(x) \times Q(x)$$

On désigne à l'ensemble des polynômes de degrés inférieur à n par $P_n$ ou $\mathbb{R}_n[n]$	
$P \in \mathbb{R}_n[X]$ donc $P$ est un polynôme de degré $\leq n$ . $(\forall (P, Q) \in (\mathbb{R}_n[n])^2)(\forall x \in \mathbb{R})$	
$(P + Q)(x) = P(x) + Q(x) \text{ et } (P \times Q)(x) = P(x) \times Q(x)$	
On désigne à l'ensemble des fonctions définie sur un intervalle I de $\mathbb{R}$ par $\mathbf{F}(I, \mathbb{R})$ $\mathbf{F}(I, \mathbb{R}) = \left\{ f / f : I \rightarrow \mathbb{R} \mid x \mapsto f(x) \right\}$ $\forall (f, g) \in (\mathbf{F}(I, \mathbb{R}))^2 \quad (\forall x \in I)$ $(f + g)(x) = f(x) + g(x) \text{ et } (f \times g)(x) = f(x) \times g(x)$	On désigne à l'ensemble des classes d'équivalences modulo n. Par $\mathbb{Z}/n\mathbb{Z}$ $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ $\forall (\overline{x}, \overline{y}) \in (\mathbb{Z}/n\mathbb{Z})^2 \quad \begin{cases} \overline{x} + \overline{y} = \overline{x+y} \\ \overline{x} \times \overline{y} = \overline{x \times y} \end{cases}$
On désigne à l'ensemble des matrices carrées de taille 2 par $IM_2(\mathbb{R})$	On désigne à l'ensemble des parties de l'ensemble A par $\mathbf{P}(A)$ $X \in \mathbf{P}(A) \Leftrightarrow X \subset A$ $\forall (X, Y) \in (\mathbf{P}(A))^2$ on a : $x \in X \cap Y \Leftrightarrow x \in X \text{ et } x \in Y$ (intersection) $x \in X \cup Y \Leftrightarrow x \in X \text{ ou } x \in Y$ (union) $x \in C_A^X \Leftrightarrow x \in A \text{ et } x \notin X$ (complémentaire) $x \in X - Y \Leftrightarrow x \in X \text{ et } x \notin Y$ $X \Delta Y = (X - Y) \cup (Y - X)$
$IM_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / (a, b, c, d) \in \mathbb{R}^4 \right\}$ On définit la somme et le produit dans $IM_2(\mathbb{R})$ par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ a'c+dc' & cb'+dd' \end{pmatrix}$	
On désigne à l'ensemble des matrices carrées de taille 3 par $IM_3(\mathbb{R})$	On désigne à l'ensemble des transformations dans le plan par $\mathbf{T}$ Toute application bijective du plan $\mathbf{P}$ vers le plan $\mathbf{P}$ s'appelle transformation dans $\mathbf{P}$ . On désigne à l'ensemble des transformations dans le plan par $\mathbf{T}$ . Les translations, les homothéties et les rotations sont des transformations du plan
$IM_3(\mathbb{R}) = \left\{ \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} / (a, b, c, d, e, f, g, h, i) \in \mathbb{R}^9 \right\}$ On définit la somme et le produit dans $IM_3(\mathbb{R})$ par $\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} + \begin{pmatrix} a' & d' & g' \\ b' & e' & h' \\ c' & f' & i' \end{pmatrix} = \begin{pmatrix} a+a' & d+d' & g+g' \\ b+b' & e+e' & h+h' \\ c+c' & f+f' & i+i' \end{pmatrix}$ $\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} \times \begin{pmatrix} a' & d' & g' \\ b' & e' & h' \\ c' & f' & i' \end{pmatrix} = \begin{pmatrix} aa'+db'+gc' & ad'+de'+gf' & ag'+dh'+gi' \\ ba'+eb'+hc' & bd'+ee'+hf' & bg'+ch'+hi' \\ ca'+fb'+ic' & cd'+fe'+if' & cg'+fg'+ii' \end{pmatrix}$	

## 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  $E$ . C à d  $f : E \times E \rightarrow E$**

$$(x, y) \mapsto f(x, y)$$

**Remarque :** Traditionnellement, et sans précision ou contexte particulier, une LCI est notée \* ou T ("truc"). On peut également adopter un formalisme additif (la LCI est alors notée +) ou multiplicatif ( $\times$  ou .).

## Exemples

- ❖ La somme sur  $N, N^*, Z, Q, R, C$  (mais pas sur  $Z^*, Q^*, R^*, C^*$ ).
- ❖ Le produit sur  $N, N^*, Z, Q, R, C \dots$
- ❖ La différence sur  $R$  ou  $Z$  (mais pas sur  $N$ )
- ❖ La composition des applications sur  $F$  (applications de  $F$  dans  $F$ )
- ❖ La loi  $\oplus$  d' définie sur  $R^2$  par  $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ .
- ❖ La loi  $\otimes$  d' définie sur  $R^2$  par  $(x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$
- ❖ Les lois  $\cup$ ,  $\cap$  et  $\Delta$  (réunion, intersection et différence symétrique) d' finies sur  $P(E)$  Dans  $N^*$
- ❖ L'exponentiation, c'est-à- dire l'application  $(N^*)^2 \rightarrow N^*$

$$(a, b) \rightarrow a^b$$

- ❖ le PGCD ou le PPCM sont des lois internes.
- ❖  $E$  étant un ensemble donné, l'intersection et la réunion sont des lois de composition interne dans  $P(E)$ .
- ❖ Si  $E$  est un ensemble non vide, la composition des applications de  $E$  dans  $E$  est une loi interne dans  $E^E$ .
- ❖ Dans l'ensemble  $\mathbb{Z}/n\mathbb{Z}$  l'addition et la multiplication sont des lois de compositions internes

## Application :

1) On pose  $E = ]-1; 1[$ . On définit dans  $E$  la relation \* par :  $(\forall (x, y) \in E^2) : x * y = \frac{x + y}{1 + xy}$

\* est-elle une loi de composition interne dans  $E$  ?

2) On considère l'ensemble  $E = \{f_1, f_2, f_3, f_4\}$  tel  $f_i$  et  $i \in \{1, 2, 3, 4\}$  sont des fonctions numériques de  $\mathbb{R}^*$  vers  $\mathbb{R}^*$

définies par  $f_1 : x \mapsto x$  ;  $f_2 : x \mapsto -x$  ;  $f_3 : x \mapsto \frac{1}{x}$  et  $f_4 : x \mapsto -\frac{1}{x}$

Démontrer que o ( composée de deux fonctions ) est une loi de composition interne dans  $E$

## 2) Parties stables

### Définition

Soient  $E$  un ensemble non vide puis \* une loi de composition interne sur  $E$ . Soit  $F$  une partie non vide de  $E$ .  $F$  est stable pour \*  $\Leftrightarrow \forall (x, y) \in F^2, x * y \in F$

### Exemples

- Dans  $\mathbf{Z}$ , 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) alors 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 toujours un nombre impair).
- Dans  $E^E$ , l'ensemble des injections, l'ensemble des surjections et l'ensemble des bijections sont stables pour o (la composée de deux injections (resp. deux surjections, deux bijections) est une injection (resp. une surjection, une bijection)).
- Dans  $\mathbf{C}$ , l'ensemble  $U$  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).

### Application :

on considère  $(\mathcal{F}(\mathbb{R}, \mathbb{R}), o)$  l'ensemble des fonctions numériques de la loi de composition des fonctions. Et on considère la partie  $\mathcal{A}(\mathbb{R}, \mathbb{R})$  des fonction affines

Démontrer que  $\mathcal{A}(\mathbb{R}, \mathbb{R})$  est une partie stable de  $(\mathcal{F}(\mathbb{R}, \mathbb{R}), o)$

### Correction

Soit  $f_{(a,b)} \in \mathcal{A}$  donc  $f_{(a,b)} : x \rightarrow ax + b$  et  $f_{(c,d)} \in \mathcal{A}$

donc  $f_{(c,d)} : x \rightarrow cx + d$ . On a  $\forall x \in \mathbb{R}$

$$\begin{aligned} (f_{(c,d)} \circ f_{(a,b)})(x) &= f_{(c,d)}(ax + b) \\ &= c(ax + b) + d \\ &= cax + cb + d \\ &= f_{(ca,cb+d)}(x) \end{aligned}$$

C à d  $f_{(c,d)} \circ f_{(a,b)} = f_{(ca,cb+d)}$  donc ( $\forall f_{(a,b)} \in \mathcal{A}$

$(\forall f_{(c,d)} \in \mathcal{A})$  on a  $f_{(c,d)} \circ f_{(a,b)} \in \mathcal{A}$

## Exercice corrigé

On considère l'ensemble  $E = \left\{ \begin{pmatrix} a+b & -b \\ b & a \end{pmatrix}, (a, b) \in \mathbb{R}^2 \right\}$

Démontrer que E stable pour la loi  $\times$  dans  $\mathcal{M}_2(\mathbb{R})$

## Corrigé

Soit  $(a, b)$  et  $(x, y)$  de éléments de  $\mathbb{R}^2$  tel que

$$\mathcal{M}_{(a,b)} = \begin{pmatrix} a+b & -b \\ b & a \end{pmatrix} \in E$$

$$\text{et } \mathcal{M}_{(x,y)} = \begin{pmatrix} x+y & -y \\ y & x \end{pmatrix} \in E$$

$$\mathcal{M}_{(a,b)} \times \mathcal{M}_{(x,y)}$$

$$= \begin{pmatrix} (a+b)(x+y) - by & -y(a+b) - bx \\ b(x+y) + ay & -by + ax \end{pmatrix}$$

$$= \begin{pmatrix} (ax - by) + (bx + by + ay) & -(bx + by + ay) \\ bx + by + ay & ax - by \end{pmatrix}$$

$$= \mathcal{M}_{(ax - by, bx + by + ay)} \in E$$

Donc E stable pour la loi  $\times$  dans  $\mathcal{M}_2(\mathbb{R})$

## Exercice

1) On considère N muni de deux lois de composition internes :

$$\forall (a, b) \in \mathbb{N}^{*2} : a \wedge b = p \gcd(a, b) \text{ et } a \vee b = p \operatorname{lcm}(a, b)$$

Etudier la stabilité de  $E = \{1; 2; 3; 6\}$  par rapport à  $(\mathbb{N}^*; \wedge)$  et  $(\mathbb{N}^*; \vee)$

2) On considère l'ensemble  $E = \{2^n, n \in \mathbb{Z}\}$ . Etudier la stabilité de  $E$  par rapport à  $(\mathbb{Z}; +)$  et  $(\mathbb{Z}; \times)$

## Définition

Soient E un ensemble non vide puis \* une loi de composition interne sur E. Soit F une partie non vide de E, stable pour \*. L'application  $F \times F \rightarrow F$  est appelée loi induite par \* sur F.

$$(x, y) \mapsto x * y$$

## 3) Propriétés des lois de composition interne

Soient E un ensemble non vide et \* une loi de composition interne sur E. \* peut avoir ou non une ou plusieurs des propriétés suivantes :

### Commutativité et Associativité

## Définition

\* est commutative  $\Leftrightarrow \forall (x, y) \in E^2, x * y = y * x$

\* est associative  $\Leftrightarrow \forall (x, y, z) \in E^3, (x * y) * z = x * (y * z)$ .

**Remarque :** si la loi  $*$  est associative dans  $E$  on écrit :  $\forall (a, b, c) \in E^3 \quad (a * b) * c = a * (b * c) = a * b * c$

## Exemples et contres exemples :

- L'addition et la multiplication dans  $\mathbf{C}$  sont commutatives. La loi  $\circ$  dans  $\mathbf{E}^E$  fournit l'exemple le plus important de loi non commutative (en général  $\mathbf{f} \circ \mathbf{g} \neq \mathbf{g} \circ \mathbf{f}$ ).
- L'addition et la multiplication dans  $\mathbf{C}$  ou la composition dans  $\mathbf{E}^E$  sont des lois associatives  $((\mathbf{f} \circ \mathbf{g}) \circ \mathbf{h} = \mathbf{f} \circ (\mathbf{g} \circ \mathbf{h})$  et on peut écrire plus simplement  $\mathbf{f} \circ \mathbf{g} \circ \mathbf{h}$ ). La division dans  $\mathbf{C}^*$  est interne mais n'est pas associative.
- De même, l'exponentiation dans  $\mathbf{N}^*$  n'est pas associative

<u>Exemples</u>	<u>Contres exemples</u>
L'addition et la multiplication sont commutatives et associatives dans $\mathbf{N}, \mathbf{Q}, \mathbf{Z}, \mathbf{R}$ et $\mathbf{C}$	La soustraction n'est pas commutative dans $\mathbf{R}$ ( car $1-5 \neq 5-1$ )
L'intersection et l'union sont associatives et commutatives dans $\mathcal{P}(E)$	La soustraction n'est pas associative dans $\mathbf{Z}$ (car $((1-3)-4) \neq 1-(3-4)$ )
La somme et la multiplication sont associatives et commutatives dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$	Le produit vectoriel dans $\mathcal{V}_3$ n'est pas commutatif ( car $\vec{i} \wedge \vec{j} = -\vec{j} \wedge \vec{i}$ )
La somme de deux vecteurs dans $\mathcal{V}_2$ et $\mathcal{V}_3$ est associative et commutative	La composée de deux fonctions n'est pas commutative La multiplication dans $M_2(\mathbb{R})$ n'est pas commutative
La composée de deux fonctions est associative dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$	

## 4) Éléments particuliers

### a) Elément neutre

#### Définition

Soient  $E$  un ensemble non vide et  $*$  une loi interne sur  $E$ .

Soit  $e \in E$ .  $e$  est élément neutre pour  $*$   $\Leftrightarrow \forall x \in E, e * x = x * e = x$ .

\* admet un élément neutre dans  $E \Leftrightarrow \exists e \in E / \forall x \in E, x * e = e * x = x$

## Remarque

- ◊ Notez bien l'ordre des quantificateurs  $\exists e \in E / \forall x \in E, \dots$  qui dit que  $e$  est précis et ne dépend pas de  $x$ , et non pas  $\forall x \in E, \exists e \in E / \dots$  Qui permettrait à  $e$  de changer quand  $x$  change.
- ◊ Si on sait que la loi  $*$  est commutative, une et une seule des deux égalités ( $\forall x \in E, x * e = x$  ou  $\forall x \in E, e * x = x$ ) ci-dessus suffit

## Théorème

Si  $*$  admet un élément neutre, celui-ci est unique

## Exemples

- ✓ Dans  $\mathbf{C}$ ,  $0$  est élément neutre pour l'addition et  $1$  est élément neutre pour la multiplication.
- ✓ Dans  $P(E)$ ,  $E$  est élément neutre pour l'intersection et  $\emptyset$  est élément neutre pour la réunion.
- ✓ la fonction nulle  $\theta : x \rightarrow 0$  est un élément neutre pour l'addition dans  $\mathcal{F}(I, \mathbb{R})$
- ✓ la fonction nulle  $I_1 : x \rightarrow 1$  est un élément neutre pour la multiplication dans  $\mathcal{F}(I, \mathbb{R})$
- ✓ la fonction nulle  $I_E : x \rightarrow x$  est un élément neutre pour la composée des fonctions dans  $\mathcal{F}(I, \mathbb{R})$
- ✓ la matrice nulle  $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$  est un élément neutre pour la loi  $+$  dans  $\mathcal{M}_2(\mathbb{R})$  et la matrice identité  $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  est l'élément neutre pour la loi  $\times$  dans  $\mathcal{M}_2(\mathbb{R})$
- ✓ la matrice nulle  $O_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$  est un élément neutre pour la loi  $+$  dans  $\mathcal{M}_3(\mathbb{R})$  et la matrice identité  $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$  est l'élément neutre pour la loi  $\times$  dans  $\mathcal{M}_3(\mathbb{R})$

## b) Elément absorbant

### Définition

Soient  $E$  un ensemble non vide et  $*$  une loi interne sur  $E$ .

Soit  $a \in E$ .  $a$  est élément absorbant pour  $*$   $\Leftrightarrow \forall x \in E, a * x = x * a = a$ .

## Exemples

- Dans  $\mathbf{C}$ , 0 est absorbant pour la multiplication.
- Dans  $P(E)$ ,  $\mathbf{E}$  est absorbant pour la réunion et  $\emptyset$  est absorbant pour l'intersection.
- Dans  $\mathcal{M}_3(\mathbb{R})$ ,  $O_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$  est l'élément neutre pour la loi  $\times$

### c) Elément symétrisable

#### Définition

Soient  $E$  un ensemble non vide et  $*$  une loi interne sur  $E$  possédant un élément neutre  $e$ .

Soit  $x \in E$ .

- **x admet un** symétrique à gauche **pour  $*$**   $\Leftrightarrow \exists x' \in E / x * x' = e$ .
- **x admet un** symétrique à droite **pour  $*$**   $\Leftrightarrow \exists x' \in E / x * x' = e$ .
- **x admet un** symétrique **pour  $*$**   $\Leftrightarrow \exists x' \in E / x * x' = x' * x = e$ .
- **x est** symétrisable à gauche **pour  $*$**  si et seulement si **x admet un symétrique à gauche pour  $*$** .
- **x est** symétrisable à droite **pour  $*$**  si et seulement si **x admet un symétrique à droite pour  $*$** .
- **x est** symétrisable **pour  $*$**  si et seulement si **x admet un symétrique pour  $*$** .

#### Remarque

- ◊ Notez que ici, on fournit  $x'$  après avoir fourni  $x$  (soit  $x \in E \dots \exists x' \in E \dots$ ) et donc bien sûr,  $x'$  varie quand  $x$  varie.
- ◊ Si on sait que la loi  $*$  est commutative, une et une seule des deux égalités ci-dessus suffit.

#### Théorème

Soit  $x$  un élément de  $E$ . Si  $*$  est associative, possède un élément neutre  $e$  et si  $x$  admet un symétrique pour  $*$ , celui-ci est unique.

#### Démonstration.

Soit  $x$  un élément de  $E$ . Soient  $x'$  et  $x''$  deux éléments symétriques de  $x$  (pas nécessairement distincts).

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

## Exemples :

- Si  $*$  est l'addition dans  $\mathbf{C}$ , le symétrique (défini ci-dessus de manière très générale) d'un complexe  $z$  n'est autre que  $-z$  et s'appelle l'**opposé** de  $z$ .
- Si  $*$  est la multiplication dans  $\mathbf{C} \setminus \{0\}$ , le symétrique d'un complexe non nul  $z$  n'est autre que  $1/z$  et s'appelle l'**inverse** de  $z$ .
- Si  $*$  est la composition des applications, les éléments de  $E^E$  qui admettent un symétrique pour la loi  $\circ$  sont les **bijections** de  $E$  sur  $E$ . Le symétrique d'une bijection  $f$  pour la loi  $\circ$  n'est autre que sa **réciproque**  $f^{-1}$ .
- Dans  $(\mathcal{R}_\Omega, \circ)$  le symétrique de  $r(\Omega, -\theta)$  est  $r(\Omega, \theta)$

## **Théorème**

Soient  $E$  un ensemble non vide puis  $*$  une loi de composition interne sur  $E$ , associative et possédant un élément neutre  $e$ .

Soient  $x$  et  $y$  deux éléments de  $E$ . Si  $x$  et  $y$  sont symétrisables, alors  $x * y$  est symétrisable et  $(x * y)' = y' * x'$ .

## Démonstration.

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

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

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

Donc,  $x * y$  est symétrisable et son symétrique est  $y' * x'$ .

## Exemples :

- dans  $\mathbf{C}$ , l'opposé  $-(z_1 + z_2)$  de  $z_1 + z_2$  est  $-z_1 - z_2$ ,
- dans l'ensemble des bijections d'un ensemble  $E$  sur lui-même, la réciproque  $(g \circ f)^{-1}$  de  $g \circ f$  est  $f^{-1} \circ g^{-1}$  (et pas  $g^{-1} \circ f^{-1}$ ).

## Application :

On considère l'ensemble  $E = ]-1, 1[$  et soit la loi de composition interne  $*$  définie par  $x * y = \frac{x+y}{1+xy}$

- 1) Démontrer que  $*$  est une loi de composition interne sur  $E$
- 2) Démontrer que  $*$  est commutative et associative dans  $E$
- 3) Déterminer l'élément neutre  $e$  pour la loi  $*$  dans  $E$
- 4) Démontrer que pour tous  $x$  de  $E$  admet un élément symétrique dans  $E$  à déterminer

## Solution :

1) Soit  $x$  et  $y$  deux éléments de  $E$  on a

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

$$\text{et } \begin{cases} -2 < x - 1 < 0 \\ 0 < 1 - y < 2 \\ 0 < 1 + xy < 2 \end{cases} \text{ donc } x * y - 1 < 0$$

et par suite  $x * y < 1$

$$\text{On a } x * y + 1 = \frac{x+y}{1+xy} + 1 = \frac{x+y+xy+1}{1+xy}$$

$$= \frac{x+1+y(x+1)}{1+xy} = \frac{(x+1)(y+1)}{1+xy}$$

$$\text{et } \begin{cases} 0 < x + 1 < 2 \\ 0 < y + 1 < 2 \\ 0 < 1 + xy < 2 \end{cases} \quad \text{Donc } x * y + 1 > 0 \text{ et par suite } x * y > -1$$

Et par suite  $-1 < x * y < 1$  donc la loi  $*$  est une loi de composition interne dans  $E$

2) Soient  $x, y$  et des éléments de  $E$

$$\text{On a } x * y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y * x \text{ donc la loi } * \text{ est commutative}$$

$$\text{et } (x * y) * z = \frac{(x * y) + z}{1 + (x * y)z} = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy}z}$$

$$= \frac{x + y + z + xyz}{1 + xy + xz + yz} = \frac{\frac{y+z}{1+yz} + x}{1 + \frac{y+z}{1+yz}x}$$

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

donc la loi  $*$  est associative

3) Soit  $e$  l'élément neutre pour la loi  $*$  dans  $E$

$$\text{donc } \forall x \in E \quad x * e = e * x = x$$

$$\text{Donc } \frac{x+e}{1+ex} = x \Rightarrow x + e = x + ex^2$$

$$\Rightarrow e(1 - x^2) = 0$$

On sait que  $1 - x^2 \neq 0$  car  $x \in E$  donc  $e = 0$

4) Si  $x'$  est l'élément symétrique de  $x$  alors

$$\forall x \in E \quad x * x' = x' * x = 0 \text{ donc}$$

$$x * x' = \frac{x+x'}{1+xx'} = 0 \Rightarrow x' = -x$$

Comme  $x \in E$  alors  $x' = -x \in E$  et par suite tout

élément  $x$  de  $E$  admet un élément symétrique dans  $E$  :

$$x' = -x$$

## d) Elément régulier ( simplifiable )

### Définition

Soient  $E$  un ensemble non vide et  $*$  une loi interne sur  $E$ .

Soit  $x \in E$ .

- **$x$  est régulier** ( simplifiable ) à gauche pour  $*$   $\Leftrightarrow \forall (y, z) \in E^2, x * y = x * z \Rightarrow y = z$ .
- **$x$  est régulier** ( simplifiable ) à droite pour  $*$   $\Leftrightarrow \forall (y, z) \in E^2, y * x = z * x \Rightarrow y = z$ .
- **$x$  est régulier** ( simplifiable ) si et seulement si  $x$  est simplifiable à gauche et à droite.

## Théorème

Si  $*$  est associative et possède un élément neutre  $e$ , tout élément symétrisable est régulier ( simplifiable ).

**Démonstration .** Soit  $x$  un élément de  $\mathbf{E}$ , symétrisable pour  $*$ . Soit  $x'$  son symétrique pour  $*$ . Pour  $(y, z) \in \mathbf{E}^2$ ,  
 $x * y = x * z \Rightarrow x' * (x * y) = x' * (x * z) \Rightarrow (x' * x) * y = (x' * x) * z \Rightarrow e * y = e * z \Rightarrow y = z$ .

## Exemples :

- $\mathbb{N}^*$  n'a pas d'élément neutre pour l'addition.
  - Dans  $\mathbb{C}$ , tout élément est régulier ( 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 :  $\forall (z, z', z'') \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}$  ( $z \times z' = z \times z'' \Rightarrow z' = z''$ ). Mais attention, on ne simplifie pas par 0 ( $0 \times 1 = 0 \times 2$  mais  $1 \neq 2$ ).
- Donc,  $az = az'$  n'implique pas  $z = z'$  mais ( $az = az'$  et  $a \neq 0$ )  $\Rightarrow z = z'$ .

**Remarque :** L'élément neutre est toujours régulier.

## Exercices corrigés :

### Exercice 1

On définit une loi de composition interne  $*$  sur  $\mathbb{R}$  par :  $\forall (a, b) \in \mathbb{R}^2, a * b = \ln(e^a + e^b)$

Quelles en sont les propriétés ? Possède-t-elle un élément neutre ? Y a-t-il des éléments réguliers ?

### Correction :

$\forall a, b \in \mathbb{R}, b * a = \ln(e^b + e^a) = \ln(e^a + e^b) = a * b$ .  $*$  est commutative.

$a * \varepsilon = a \Leftrightarrow \ln(e^a + e^\varepsilon) = a \Leftrightarrow e^\varepsilon = 0$ . Il n'y a donc pas de neutre.

$\forall a, b, c \in \mathbb{R}, (a * b) * c = \ln(e^{a+b} + e^c) = \ln(e^a + e^b + e^c) = a * (b * c)$ .  $*$  est associative.

$a * b = a * c \Rightarrow \ln(e^a + e^b) = \ln(e^a + e^c) \Rightarrow e^b = e^c \Rightarrow b = c$ . Tout élément est régulier

### Exercice 2

Soit  $E = [0 ; 1]$ . On définit une loi  $*$  sur  $E$  par  $\forall x, y \in E, x * y = x + y - xy$

(a) Montrer que  $*$  est une loi de composition interne commutative et associative.

(b) Montrer que  $*$  possède un neutre.

(c) Quels sont les éléments symétrisables ? réguliers ?

## Correction :

a)  $1 - (x + y - xy) = (1 - x)(1 - y)$  donc

si  $x \leq 1$  et  $y \leq 1$  alors  $x * y \leq 1$ .

Par suite  $*$  est bien une loi de composition interne sur

\* est clairement commutative et associative.

b) 0 est élément neutre de  $E$ .

c) Si  $x \in [0 ; 1]$  alors pour tout  $y \in [0 ; 1]$ ,

$$x * y = x$$

$(1 - y) + y > 0$  et donc  $x$  n'est pas inversible

(dans  $[0 ; 1]$ ). Ainsi, seul 0 est inversible.

Pour tout  $x, y, z \in [0 ; 1]$ ,

$$x * y = x * z \iff y(1 - x) = z(1 - x).$$

Par suite, tout  $x \in [0 ; 1]$  est régulier tandis que 1 ne

l'est visiblement pas.

## II) Morphisme de $(E, *)$ vers $(F, T)$

### Définition

Soient  $E$  et  $F$  deux ensembles,  $*$  une loi de composition interne sur  $E$ , et  $T$  une loi de composition interne sur  $F$ .

On dit qu'une application  $f$  de  $E$  dans  $F$  est un morphisme de  $(E, *)$  dans  $(F, T)$  si:

$$\forall (a, b) \in E^2 \quad f(a * b) = f(a)Tf(b)$$

- Un morphisme bijectif est appelé isomorphisme.
- Un morphisme de  $(E, *)$  dans lui-même est appelé endomorphisme de  $E$ .
- Un endomorphisme bijectif est appelé automorphisme.

### Exemples :

✓ On considère l'application  $f : \mathbb{N} \rightarrow 2\mathbb{N}$

$$x \mapsto 2x \quad (\text{ } 2\mathbb{N} \text{ est l'ensemble des entiers pairs})$$

On a  $a \mapsto 2a$  et  $b \mapsto 2b$  et  $a + b \mapsto 2(a + b)$

On sait que  $2(a + b) = 2a + 2b$  et par suite  $f(a + b) = f(a) + f(b) \quad \forall (a, b) \in \mathbb{N}^2$

Donc  $f$  est un morphisme de  $(\mathbb{N}, +)$  dans  $(2\mathbb{N}, +)$

✓ Soient les deux ensembles  $\mathbb{N}^*$  et  $2\mathbb{N}^*$  muni respectivement par l'addition et la multiplication

On considère l'application  $f : \mathbb{N}^* \rightarrow 2\mathbb{N}^*$

$$x \mapsto 2^x \quad f(\mathbb{N}^*) = \{2^1; 2^2; 2^3; 2^4; \dots \rightarrow\} \text{ est une partie de } 2\mathbb{N}^*$$

On a  $a \mapsto 2^a$  et  $b \mapsto 2^b$  et  $a+b \mapsto 2^{a+b}$

On sait que  $2^{a+b} = 2^a \times 2^b$  et par suite  $f(a+b) = f(a) \times f(b) \quad \forall (a,b) \in \mathbb{N}^{*2}$  donc  $f$  est un morphisme de  $(\mathbb{N}^{*}; +)$  dans  $(2\mathbb{N}^{*}; \times)$

- ✓ L'application  $f : (\mathbb{R}^{+*}, \times) \rightarrow (\mathbb{R}, +)$  définie par  $f(x) = \ln x$  est un isomorphisme de  $(\mathbb{R}^{+*}, \times)$  dans  $(\mathbb{R}, +)$

:

$$f(x \times y) = \ln(x \times y) = \ln x + \ln y = f(x) + f(y), \quad \forall x, y \in \mathbb{R}^{+*}$$

- ✓ Soit  $a \in \mathbb{R}$ . L'application  $f_a : (\mathbb{R}, +) \rightarrow (\mathbb{R}^{+*}, \times)$  définie par  $f_a(x) = a^x$  est un isomorphisme de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}^{+*}, \times)$  :

on a  $f_a(x+y) = a^{x+y} = a^x \times a^y = f_a(x) \times f_a(y), \quad \forall x, y \in \mathbb{R}$ .

- ✓ L'application  $f : (\mathbb{C}^{*}, \times) \rightarrow (\mathbb{R}^{+*}, \times)$  définie par  $f(z) = |z|$  pour tout  $z \in \mathbb{C}^{*}$  est un morphisme de  $(\mathbb{C}^{*}, \times)$  dans  $(\mathbb{R}^{+*}, \times)$

$$\text{car } f(z \times w) = |z \times w| = |z| \times |w| = f(z) \times f(w), \quad \forall z, w \in \mathbb{C}^{*}.$$

- ✓ L'application  $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}^{+*}, \times)$  définie par  $f(x) = e^x$  pour tout  $x \in \mathbb{R}$  est un isomorphisme de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}^{+*}, \times)$  car elle est bijective et  $f(x+y) = e^{x+y} = e^x \times e^y = f(x) \times f(y), \quad \forall x, y \in \mathbb{R}$ .

- ✓ L'application  $f : (\mathbb{R}, +) \rightarrow (\mathbb{C}^{*}, \times)$  définie par  $f(x) = e^{2i\pi x}$  pour tout  $x \in \mathbb{R}$  est un morphisme de  $(\mathbb{R}, +)$  dans  $(\mathbb{C}^{*}, \times)$  car  $f(x+y) = e^{2i\pi(x+y)} = e^{2i\pi x} \times e^{2i\pi y} = f(x) \times f(y), \quad \forall x, y \in \mathbb{R}$ .

- ✓ On considère l'application  $L : \mathbb{R} \rightarrow IM_2(\mathbb{R})$

$$x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

$$\text{Pour tout } x \text{ et } y \text{ de } \mathbb{R} \text{ on a } L(x+y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \text{ et } L(x) \times L(y) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$

Donc  $L(x+y) = L(x) \times L(y)$  et par suite  $L$  est un morphisme de  $(\mathbb{R}, +)$  dans  $(IM_2(\mathbb{R}); \times)$

## Propriétés

Soit  $f$  un morphisme de  $(E, *)$  dans  $(F, T)$  on a :

- 1)  $f(E)$  est une partie stable dans  $(F, T)$
- 2) Si la loi  $*$  est associative dans  $E$  alors  $T$  est associative dans  $f(E)$
- 3) Si la loi  $*$  est commutative dans  $E$  alors  $T$  est commutative dans  $f(E)$
- 4) Si  $e$  est élément neutre pour la loi  $*$  dans  $E$  alors  $f(e)$  est l'élément neutre pour la loi  $T$  dans  $f(E)$
- 5) Si la loi  $*$  admet un élément neutre  $e$  et si pour tout élément  $x$  de  $E$  admet un symétrique  $x'$

Alors l'élément  $y = f(x)$  admet un symétrique  $y' = f(x')$

## Démonstration :

1) On a  $f(E) \subset F$  on démontre que  $yTz \in f(E)$        $\forall (y, z) \in f^2(E)$

$$\begin{cases} y \in f(E) \Leftrightarrow \exists x_1 \in E \quad f(x_1) = y \\ z \in f(E) \Leftrightarrow \exists x_2 \in E \quad f(x_2) = z \end{cases} \text{ et } yTz = f(x_1)Tf(x_2) = f(x_1 * x_2)$$

Et comme la loi  $*$  est une loi de composition interne dans  $E$  alors  $x_1 * x_2 \in E$  et par suite  $f(x_1 * x_2) \in f(E)$  donc  $f(E)$  est une partie stable dans  $(F, T)$

2) Soit  $y, z$  et  $w$  des éléments de  $f(E)$

$$\begin{cases} y \in f(E) \Leftrightarrow \exists x_1 \in E \quad f(x_1) = y \\ z \in f(E) \Leftrightarrow \exists x_2 \in E \quad f(x_2) = z \\ w \in f(E) \Leftrightarrow \exists x_3 \in E \quad f(x_3) = w \end{cases}$$

$$(yTz)Tw = (f(x_1)Tf(x_2))Tf(x_3) = f(x_1 * x_2)Tf(x_3) = f((x_1 * x_2) * x_3)$$

Comme la loi  $*$  est associative alors  $(yTz)Tw = f(x_1 * (x_2 * x_3)) = f(x_1)Tf(x_1 * x_3) = yT(zTw)$

Et par suite  $T$  est associative dans  $F$ .

3) De même on montre que  $T$  est commutative dans  $f(E)$

4) On a  $f(e) \in f(E)$ . Soit  $y$  un élément de  $f(E)$  on sait que  $y \in f(E) \Leftrightarrow \exists x_1 \in E; f(x_1) = y$  donc

(car  $e$  élément neutre dans  $(E, *)$ )     $f(e)Ty = f(e)Tf(x_1) = f(e * x_1) = f(x_1)$  et par suite  $f(e)$  est l'élément neutre dans  $(f(E), T)$

5) Soit  $x'$  le symétrique de  $x$  dans  $(E, *)$  on a  $x * x' = e$  et  $x' * x = e$  donc  $f(x * x') = f(e)$

et  $f(x' * x) = f(e)$

Comme  $f$  est morphisme alors  $f(x)Tf(x') = f(x * x') = f(e)$  et par suite  $f(x')$  est le symétrique de  $f(x)$  dans  $(f(E), T)$ .

**Remarque :** si  $f$  est un isomorphisme (ou morphisme bijectif) alors  $f(E) = F$

➤ **Application :** montrer que  $f : \mathbb{R} \rightarrow IM_2(\mathbb{R})$  est un morphisme de  $(\mathbb{R}, +)$  dans  $(IM_2(\mathbb{R}), \times)$

$$\theta \mapsto \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

Puis calculer  $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}^n$  pour tout  $n$  de  $\mathbb{N}$

### III) groupes

#### 1) Définition d'un groupe

##### Définition

Soit  $G$  un ensemble non vide muni d'une loi de composition interne (notée  $*$ ).

$(G, *)$  est un **groupe** si et seulement si

1)  $*$  est **associative**,

2)  $*$  possède un **élément neutre** dans  $G$

3) tout élément de  $G$  possède un **symétrique** pour  $*$  dans  $G$ .

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

##### Exemples et contres exemples :

Voici des ensembles et des opérations bien connus qui ont une structure de groupe.

❖  $(R^*, \times)$  est un groupe commutatif,  $\times$  est la multiplication habituelle. Vérifions chacune des propriétés :

1. Si  $x, y \in R^*$  alors  $x \times y \in R^*$ .

2. Pour tout  $x, y, z \in R^*$  alors  $x \times (y \times z) = (x \times y) \times z$ , c'est l'associativité de la multiplication des nombres réels.

3. 1 est l'élément neutre pour la multiplication, en effet  $1 \times x = x$  et  $x \times 1 = x$ , ceci quel que soit  $x \in R^*$ .

4. L'inverse d'un élément  $x \in R^*$  est  $x' = \frac{1}{x}$  (car  $x \times \frac{1}{x}$  est bien égal à l'élément neutre 1).

L'inverse de  $x$  est donc  $x^{-1} = \frac{1}{x}$

. Notons au passage que nous avions exclu 0 de notre groupe, car il n'a pas d'inverse.

Ces propriétés font de  $(R^*, \times)$  un groupe.

5. Enfin  $x \times y = y \times x$ , c'est la commutativité de la multiplication des réels.

❖  $(Q^*, \times), (C^*, \times)$  sont des groupes commutatifs.

❖  $(Z, +)$  est un groupe commutatif. Ici  $+$  est l'addition habituelle.

1. Si  $x, y \in Z$  alors  $x + y \in Z$ .

2. Pour tout  $x, y, z \in Z$  alors  $x + (y + z) = (x + y) + z$ .

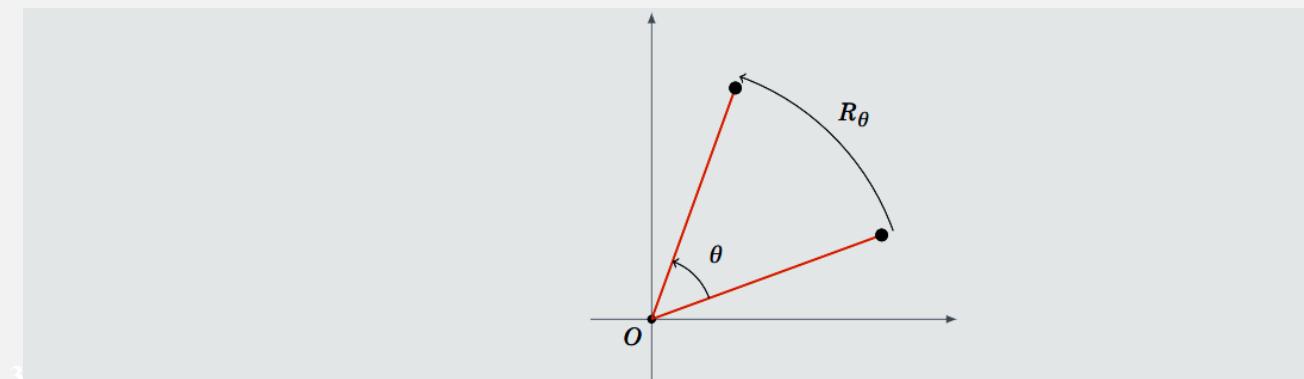
3. 0 est l'élément neutre pour l'addition, en effet  $0 + x = x$  et  $x + 0 = x$ , ceci quelque soit  $x \in Z$ .

4. L'inverse d'un élément  $x \in Z$  est  $x' = -x$  car  $x + (-x) = 0$  est bien l'élément neutre 0. Quand la loi de groupe

est + l'inverse s'appelle plus couramment l'**opposé**.

5. Enfin  $x+y = y+x$ , et donc  $(\mathbb{Z},+)$  est un groupe commutatif.

- ❖  $(\mathbb{Q},+), (\mathbb{R},+), (\mathbb{C},+)$  sont des groupes commutatifs.
- ❖ Soit  $\mathbf{R}$  l'ensemble des rotations du plan dont le centre est à l'origine O.

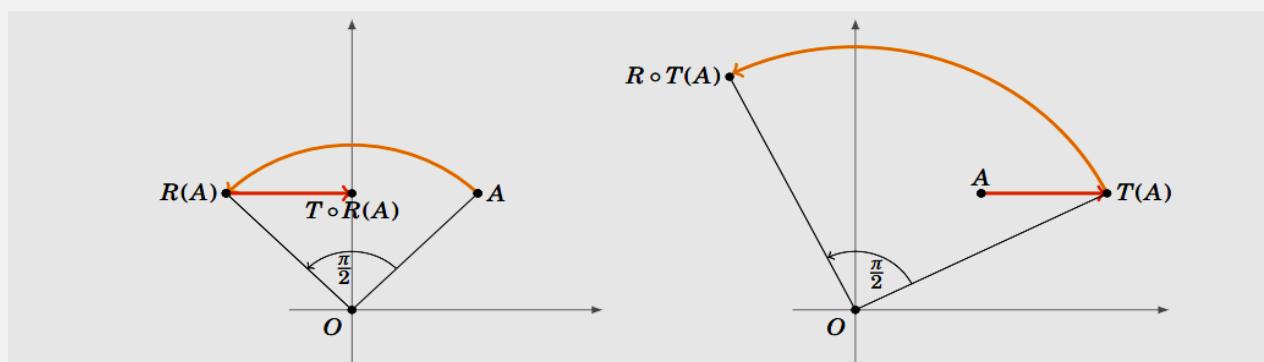


Alors pour deux rotations  $R_\theta$  et  $R_{\theta'}$  la composée  $R_\theta \circ R_{\theta'}$  est encore une rotation de centre l'origine et d'angle  $\theta + \theta'$ . Ici  $\circ$  est la composition. Ainsi  $(\mathcal{R}^\circ)$  forme un groupe (qui est même commutatif). Pour cette loi l'élément neutre est la rotation d'angle 0 : c'est l'identité du plan.

L'inverse d'une rotation d'angle  $\theta$  est la rotation d'angle  $-\theta$ .

- ❖ Si  $\mathcal{I}$  désigne l'ensemble des isométries du plan (ce sont les translations, rotations, réflexions et leurs composées) alors  $(\mathcal{I}, \circ)$  est un groupe. Ce groupe n'est pas un groupe commutatif. En effet, identifions le plan à  $\mathbb{R}^2$  et soit par exemple  $R$  la rotation de centre  $O = (0,0)$  et d'angle  $\frac{\pi}{2}$  et  $T$  la translation de vecteur  $(1,0)$ . Alors les isométries  $T \circ R$  et  $R \circ T$  sont des applications distinctes. Par exemple les images du point  $A = (1,1)$  par ces applications sont distinctes :

$$T \circ R(1,1) = T(-1,1) = (0,1) \text{ alors que } R \circ T(1,1) = R(2,1) = (-1,2).$$



Voici deux exemples qui **ne sont pas** des groupes :

- ❖  $(\mathbb{Z}^*, \times)$  n'est pas un groupe. Car si 2 avait un inverse (pour la multiplication  $\times$ ) ce serait  $\frac{1}{2}$  qui n'est pas un entier.
- ❖  $(\mathbb{N}, +)$  n'est pas un groupe. En effet l'inverse de 3 (pour l'addition  $+$ ) devrait être  $-3$  mais  $-3 \notin \mathbb{N}$ .

## Application :

Montrer que  $(\mathcal{M}_2(\mathbb{R}), +)$  est un groupe commutatif

## Correction

Soit  $A = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$  et  $B = \begin{pmatrix} x' & y' \\ z' & t' \end{pmatrix}$  et  $C =$

$\begin{pmatrix} x'' & y'' \\ z'' & t'' \end{pmatrix}$  des éléments de  $\mathcal{M}_2(\mathbb{R})$

On a  $A + B = \begin{pmatrix} x + x' & y + y' \\ z + z' & t + t' \end{pmatrix}$

$$= \begin{pmatrix} x' + x & y' + y \\ z' + z & t' + t \end{pmatrix} = B + A \quad \text{donc la}$$

loi  $+$  est commutative dans  $\mathcal{M}_2(\mathbb{R})$

$$(A + B) + C = \begin{pmatrix} x' + x & y' + y \\ z' + z & t' + t \end{pmatrix} + \begin{pmatrix} x'' & y'' \\ z'' & t'' \end{pmatrix}$$

$$= \begin{pmatrix} x + x' + x'' & y + y' + y'' \\ z + z' + z'' & t + t' + t'' \end{pmatrix}$$

$$= \begin{pmatrix} x & y \\ z & t \end{pmatrix} + \begin{pmatrix} x' + x'' & y' + y'' \\ z' + z'' & t' + t'' \end{pmatrix}$$

$$= A + (B + C)$$

Donc la loi  $+$  est associative dans  $\mathcal{M}_2(\mathbb{R})$

L'élément neutre dans  $(\mathcal{M}_2(\mathbb{R}), +)$  est la matrice

$$\text{nulle } 0_{\mathcal{M}_2(\mathbb{R})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\text{car } \forall X \in \mathcal{M}_2(\mathbb{R}) \quad X + 0_{\mathcal{M}_2(\mathbb{R})} = 0_{\mathcal{M}_2(\mathbb{R})} + X = X$$

pour tout  $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  de  $\mathcal{M}_2(\mathbb{R})$  un symétrique

$$X' = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \text{ dans } \mathcal{M}_2(\mathbb{R})$$

$$\text{car } \forall X \in \mathcal{M}_2(\mathbb{R}) \quad X + X' = 0_{\mathcal{M}_2(\mathbb{R})}$$

et par suite  $(\mathcal{M}_2(\mathbb{R}), +)$  est un groupe commutatif

## Exercice :

on pose  $A = \begin{pmatrix} -1 & 3 \\ 2 & -4 \end{pmatrix}$  et  $B = \begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix}$

1) Calculer  $A \times B$  et  $B \times A$  que peut-on déduire ?

2) Calculer  $A \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  et  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times A$  que peut-on déduire ?

3) Soit  $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  un élément de  $\mathcal{M}_2(\mathbb{R})$  tels que  $a, b, c, d \in \mathbb{R}$

Et soit  $Y = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$  le symétrique de  $X$  dans  $\mathcal{M}_2(\mathbb{R})$  tels que  $x, y, z, t \in \mathbb{R}$

Déterminer la matrice  $Y$  s'elle existe

Correction :

$$1) A \times B = \begin{pmatrix} -1 & 3 \\ 2 & -4 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix} = \\ \begin{pmatrix} -16 & 8 \\ -20 & -10 \end{pmatrix} \quad B \times A = \begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix} \times \\ \begin{pmatrix} -1 & 3 \\ 2 & -4 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 6 \end{pmatrix}$$

Comme  $A \times B \neq B \times A$  donc la

multiplication n'est pas commutative dans  
 $\mathcal{M}_2(\mathbb{R})$

$$2) A \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 2 & -4 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ = \begin{pmatrix} -1 & 3 \\ 2 & -4 \end{pmatrix} = A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times$$

A on déduit que la matrice  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  est  
l'élément neutre dans  $(\mathcal{M}_2(\mathbb{R}), \times)$

3) On sait que Y est le symétrique de X donc

$X \times Y = Y \times X = I$  alors  $X \times Y =$

$$\begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Donc } \begin{cases} ax + bz = 1 \\ cx + dz = 0 \end{cases} \text{ et } \begin{cases} ay + bt = 0 \\ cy + dt = 1 \end{cases}$$

On utilise la méthode de cramer on obtient

$$\begin{cases} x = \frac{\begin{vmatrix} 1 & b \\ 0 & d \end{vmatrix}}{\det A} = \frac{d}{\det A} \\ z = \frac{\begin{vmatrix} a & 1 \\ c & 0 \end{vmatrix}}{\det A} = \frac{-c}{\det A} \end{cases} \text{ et}$$

$$\begin{cases} y = \frac{\begin{vmatrix} 0 & b \\ 1 & d \end{vmatrix}}{\det A} = \frac{-b}{\det A} \\ t = \frac{\begin{vmatrix} a & 0 \\ c & 1 \end{vmatrix}}{\det A} = \frac{a}{\det A} \end{cases}$$

Et par suite  $Y = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$  est le  
symétrique de X si  $\det X \neq 0$

## 2) Propriétés :

### Propriété 1

Soit  $(G, *)$  groupe

- 1) L'élément neutre e est unique
- 2) Tout élément x de G admet un symétrique unique  $x'$
- 3) Si  $x'$  est le symétrique de x et  $y'$  est le symétrique de y alors  $(x * y)' = y' * x'$
- 4) Tout élément x de G est régulier c -à-d ( $\forall a \in G$ ) ( $\forall (x, y) \in G^2$ ),  $a * x = a * y \Rightarrow x = y$  et ),  
 $x * a = y * a \Rightarrow x = y$

### Propriété 2 :

Si  $(G, *)$  est un groupe d'élément neutre e et a et b deux éléments de G et  $a'$  le symétrique de a dans  $(G, *)$  alors :

Chacune des équations suivantes d'inconnue x ( $E_1$ ):  $a * x = b$  et ( $E_2$ ):  $x * a = b$  Admet une solution unique c'est  
 $x = a' * b$  pour l'équation  $E_1$  et  $x = b * a'$  pour l'équation  $E_2$

## 3) Sous-groupe

### Définition :

soit  $(G, *)$  un groupe et  $H \subset G$  on dit que  $(H, *)$  est un sous-groupe de  $(G, *)$  ssi

- $H$  Est une partie stable dans  $(G, *)$
- $(H, *)$  est un groupe

### Exemples :

- Soit  $(G, *)$  un groupe et  $e$  son l'élément neutre on a  $(G, *)$  et  $\{e\}$  sont de sous-groupe de  $(G, *)$
- $(\mathbb{Z}, +)$  Est un sous-groupe de  $(\mathbb{R}, +)$
- $(N, +)$  n'est pas un sous-groupe de  $(\mathbb{Z}, +)$
- $(\mathbb{U}, +)$  n'est pas un sous-groupe de  $(\mathbb{C}, +)$

### Propriété :

soit  $(G, *)$  un groupe et  $(H, *)$  un sous-groupe de  $(G, *)$

- 1)  $H \neq \emptyset$
- 2) Si  $e$  est l'élément neutre dans  $(G, *)$  alors  $e$  est l'élément neutre dans  $(H, *)$
- 3) Si  $x \in H$  .le symétrique de  $x$  dans  $(G, *)$  est le symétrique de  $x$  dans  $(H, *)$
- 4)  $\forall (x, y) \in H^2 \quad x * y \in H$
- 5)  $\forall (x, y) \in H^2 \quad x * y' \in H$

### Démonstration :

- 1) Le sous-groupe  $(H, *)$  est non vide car il contient l'élément neutre  $e_H$
- 2) On démontre que  $e_H = e$  comme  $e$  est l'élément neutre dans  $(G, *)$  on a  $e_H * e = e_H$

Comme  $e_H$  est élément neutre dans  $(H, *)$  on a  $e_H * e_H = e_H$  et par suite  $e_H * e_H = e_H * e$  et on sait que tout élément dans un groupe est régulier on déduit que  $e_H = e$

- 3) Soit  $x$  un éléments de  $H$ . comme  $H \subset G$ .comme alors  $x \in G$  et soit  $x'$  le symétrique de  $x$  dans  $(G, *)$

Comme  $(H, *)$  est un groupe alors  $x$  admet un symétrique dans  $(H, *)$  on le désigne par  $x''$

## Cours

On a  $x * x' = e$  dans  $(G, *)$  et  $x * x'' = e$  dans  $(H, *)$ . Et par suite  $x * x'' = x * x'$  et d'après la régularité de  $x$  dans  $(G, *)$  on a  $x' = x''$ .

4) Comme  $(H, *)$  est un sous-groupe de  $(G, *)$  on a d'après la définition d'un sous-groupe :  $H$  est une partie stable dans  $(G, *)$  c à d  $[\forall (x, y) \in H^2] \quad x * y' \in H$

5) Soit  $x$  et  $y$  deux éléments de  $H$  d'après la propriété (3) :  $y' \in H$  et d'après (4) on a  $x * y' \in H$

⇒ on suppose que  $(H, *)$  est un sous-groupe de  $(G, *)$

D'après les propriétés d'un sous-groupe on a  $H \neq \emptyset$  et  $\forall (x, y) \in H^2 \quad x * y' \in H$  d'après la propriété précédente

⇐ Soit  $(G, *)$  un groupe et  $H$  une partie de  $G$  vérifié :  $H \neq \emptyset$  et  $[\forall (x, y) \in H^2] \quad x * y' \in H$  tel que  $y'$  est le symétrique de  $y$  dans  $(G, *)$ . On démontre que  $(H, *)$  est un groupe

Comme  $H \neq \emptyset$ , il existe au moins un élément  $a$  de  $H$  et comme  $H \subset G$  alors  $a \in G$

Soit  $a'$  le symétrique de  $a$  dans  $(G, *)$  donc  $a * a' = e$  tel que  $e$  est l'élément neutre dans  $(G, *)$  d'après la condition  $[\forall (x, y) \in H^2] \quad x * y' \in H$  si on prend  $x = a$  et  $y = a$  alors  $a * a' \in H$  c à d  $e \in H$

Soit  $x$  un élément de  $H$ . On a d'après la condition  $[\forall (x, y) \in H^2] \quad x * y' \in H$

On a  $e * x' \in H$  (tel que  $x'$  est le symétrique de  $x$  dans  $(G, *)$ ) et comme  $e * x' = x'$  alors  $x' \in H$

Soit  $x$  et  $y$  deux éléments de  $H$  on sait que  $x' \in H$  de ce qui précède et si on applique la condition

$[\forall (x, y) \in H^2] \quad x * y' \in H$  au  $x$  et  $y'$  on obtient  $x * (y')' \in H$  et on sait que  $(y')' = y$  dans  $(G, *)$

alors  $x * y \in H$

De ce qui précède on a  $H$  est une partie stable dans  $(G, *)$  et comme la loi  $*$  est associative dans  $(G, *)$  donc  $*$  est associative dans  $(H, *)$ .

### Propriété caractéristique d'un sous-groupe :

Soit  $(G, *)$  un groupe et  $H \subset G$

$(H, *)$  est un sous-groupe de  $(G, *)$  ssi

- 1)  $H \neq \emptyset$
- 2)  $[\forall (x, y) \in H^2] \quad x * y' \in H$  tel que  $y'$  est le symétrique de  $y$  dans  $(G, *)$

Propriété caractéristique	
Notation additive	1) $H \neq \emptyset$ 2) $[\forall(x,y) \in H^2] \quad x - y \in H$
Notation multiplicative	1) $H \neq \emptyset$ 2) $[\forall(x,y) \in H^2] \quad x \cdot y^{-1} \in H$

## Exemples :

1) soit  $I$  l'ensemble des entiers paires

On démontre que  $(I, +)$  est un sous-groupe de  $(\mathbb{Z}, +)$

- On a  $I \neq \emptyset$  car  $0 \in I$

Pour tout  $x$  et  $y$  de  $I$  on a  $x = 2q$  ( $q \in \mathbb{Z}$ ) et  $y = 2p$  ( $p \in \mathbb{Z}$ ) donc  $x - y = 2q - 2p = 2(q - p)$

Comme  $q - p \in \mathbb{Z}$  alors  $x - y \in \mathbb{Z}$  et par suite  $(I, +)$  est un sous-groupe de  $(\mathbb{Z}, +)$

2)  $(\mathbb{U}, \times)$  est un sous-groupe de  $(\mathbb{C}^*, \times)$

En effet on  $\mathbb{U} = \{z, z \in \mathbb{C} / |z| = 1\}$   $\mathbb{U}$  est non vide ( $\frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{U}$ ) car  $\left|\frac{1}{2} + i\frac{\sqrt{3}}{2}\right| = 1$

Soit  $u$  et  $v$  deux éléments de  $\mathbb{U}$  on  $|u| = 1$  et  $|v| = 1$

Le symétrique de  $v$  dans  $(\mathbb{C}^*, \times)$  est  $\frac{1}{v}$  on a  $\left|u \times \frac{1}{v}\right| = |u| \times \left|\frac{1}{v}\right| = 1$  et par suite  $u \times \frac{1}{v} \in \mathbb{U}$  donc

$\forall(u, v) \in \mathbb{U}^2 \quad u \times \frac{1}{v} \in \mathbb{U}$  donc d'après la propriété caractéristique alors  $(\mathbb{U}, \times)$  est un sous-groupe de  $(\mathbb{C}^*, \times)$

**Application :** démontrer que  $H = \{3^m 7^n / m \in \mathbb{Z} \text{ et } n \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{R}^*, \times)$

## 4) Morphisme de groupe

### Propriété :

Soit  $f$  un morphisme de groupe  $(G, *)$  dans  $(F, T)$

L'image de groupe  $(G, *)$  par le morphisme  $f$  est le groupe  $(f(G), T)$

**Démonstration :** on déjà montrer que : Si  $f$  est un morphisme de  $(G, *)$  dans  $(F, T)$  alors :

- $f(G)$  est une partie stable dans  $(F, T)$
- $*$  est associative dans  $(G, *)$  alors  $T$  est associative dans  $(f(G), T)$
- $e$  est l'élément neutre dans  $(G, *)$ . alors  $f(e)$  est l'élément neutre dans  $(f(G), T)$
- $x'$  est le symétrique de  $x$  dans  $(G, *)$  alors  $f(x')$  est le symétrique de  $f(x)$  dans  $(f(G), T)$

Et par suite  $(f(G), T)$  est un groupe .

### Remarque :

- Si le morphisme  $f$  est surjectif alors  $f(G) = F$  et dans ce cas si  $(G, *)$  est un groupe alors  $(F, T)$  est un groupe
- On dit que  $f$  transforme la structure de groupe de  $(G, *)$  à  $(f(G), T)$  ( ou à  $(F, T)$  si  $f$  est surjectif)
- Si  $f$  est un morphisme de  $(G, *)$  dans  $(F, T)$  alors si  $(G, *)$  est un groupe alors  $(f(G), T)$  est un groupe ( ou  $(F, T)$  c'est un groupe si  $f$  est surjectif)

### Exercice

soit  $(G, .)$  un groupe

On considère l'application  $f_a: \begin{array}{ccc} G & \xrightarrow{\quad} & G \\ a & \mapsto & a \cdot x \cdot a^{-1} \end{array}$

1) Démontrer que  $f_a$  est un morphisme bijectif (isomorphisme) de  $(G, .)$  Dans  $(G, .)$

2) On considère l'ensemble  $F = \{f_a / a \in G\}$

a) Démontrer que " $\circ$ " est une loi de composition interne dans  $F$

b) On considère l'application  $h: \begin{array}{ccc} G & \xrightarrow{\quad} & F \\ a & \mapsto & f_a \end{array}$

Démontrer que  $h$  est un morphisme surjectif de  $(G, .)$  Dans  $(F, \circ)$

Déduire que  $(F, \circ)$  c'est un groupe

Corrigé :

1) On démontre que  $f_a$  est un morphisme de  $(G, .)$

Dans  $(G, .)$

Soit  $x$  et  $y$  deux éléments de  $G$  on démontre que

$$f_a(x.y) = f_a(x).f_a(y) \text{ .On a}$$

$$f_a(x.y) = a.x.y.a^{-1} = a.x.e.y.a^{-1}$$

$$= a.x.a^{-1}.ay.a^{-1}$$

$$= (a.x.a^{-1}).(ay.a^{-1})$$

$$= f_a(x).f_a(y)$$

Donc  $f_a$  est un morphisme de  $(G, .)$  Dans  $(G, .)$

On démontre que  $f_a$  est bijectif

Soit  $y \in G$  on cherche un  $x$  de  $G$  tel que  $f_a(x) = y$

$$\text{On a } f_a(x) = y \Leftrightarrow a.x.a^{-1} = y$$

$$\Leftrightarrow a^{-1}.a.x.a^{-1} = a^{-1}.y$$

$$\Leftrightarrow e.x.a^{-1}.a = a^{-1}.y.a \Leftrightarrow x$$

$$= a^{-1}.y.a \in G \text{ donc tout élément de } y \text{ de } G \text{ admet}$$

un unique antécédent  $x = a^{-1}.y.a$  de  $G$  donc  $f_a$  est

bijectif

Et par suite  $f_a$  est un morphisme bijectif

(isomorphisme) de  $(G, .)$  Dans  $(G, .)$

2) a) on démontre que " $o$ " est une loi de composition

interne dans  $F$

soit  $f_a$  et  $f_b$  deux éléments de  $F$  on démontre que

$$f_a \circ f_b \in F$$

soit  $x \in G$  on calcul  $f_a \circ f_b(x)$

$$\text{on a } f_a \circ f_b(x) = f_a(f_b(x))$$

$$= f_a(b.x.b^{-1})$$

$$= a.b.x.b^{-1}.a^{-1}$$

$$= a.b.x.(b^{-1}.a^{-1})$$

$$= a.b.x.(a.b)^{-1} = f_{ab}(x) \text{ et}$$

$$\text{par suite } f_a \circ f_b(x) = f_{ab}(x)$$

Donc  $f_a \circ f_b = f_{ab}$  et on a  $\begin{cases} a \in G \\ b \in G \end{cases}$  donc  $a, b \in G$  et par

suite  $f_{a,b} \in F$

donc " $o$ " est une loi de composition interne dans  $F$

b) on démontre que  $h$  est un morphisme surjectif de  $(G, .)$  Dans  $(F, o)$

Soient  $a$  et  $b$  deux éléments de  $G$  on démontre que  $h(a.b) = h(a).h(b)$

$h(a.b) = f_{a,b} = f_a \circ f_b = h(a).h(b)$  donc  $h$  c'est un morphisme

et on a  $h$  est surjectif car pour tout élément  $f_a$  a au moins un antécédent  $a$  de  $G$

et par suite  $h$  est un morphisme surjectif de  $(G, .)$

Dans  $(F, o)$

❖ on démontre que  $(F, o)$  c'est un groupe

on a  $(G, .)$  C'est un groupe et  $h$  est un morphisme surjectif de  $(G, .)$  Dans  $(F, o)$  donc d'après la propriété des morphisme des groupe on a  $(F, o)$  c'est un groupe

**IV-Anneau****1) Distributivité d'une loi sur une autre****Définition :**

Soient  $\mathbf{E}$  un ensemble non vide et  $*$  et  $\mathbf{T}$  deux lois de composition internes sur  $\mathbf{E}$ .

$\mathbf{T}$  est distributive sur  $*$   $\Leftrightarrow \forall (x, y, z) \in \mathbf{E}^3, x \mathbf{T} (y * z) = (x \mathbf{T} y) * (x \mathbf{T} z)$  et  $(y * z) \mathbf{T} x = (y \mathbf{T} x) * (z \mathbf{T} x)$ .

**Remarque :** Si on sait que  $\mathbf{T}$  est commutative, une et une seule des deux égalités ci-dessus suffit.

**Exemples**

- Dans  $\mathbf{C}$ , la multiplication est distributive sur l'addition mais l'addition n'est pas distributive sur la multiplication.
- Dans  $\mathbf{P}(\mathbf{E})$ , l'intersection est distributive sur la réunion et la réunion est distributive sur l'intersection.
- Dans  $\mathbf{R}^{\mathbf{R}}$ ,  $\circ$  est distributive à droite sur  $+$ , mais pas à gauche,  $(g + h) \circ f = g \circ f + h \circ f$  mais en général  $f \circ (g + h) \neq f \circ g + f \circ h$
- Dans  $\mathcal{F}(I, \mathbb{R})$  la multiplication est distributive sur l'addition
- Dans  $\mathcal{M}_2(\mathbb{R})$  et  $\mathcal{M}_3(\mathbb{R})$  la multiplication est distributive sur l'addition
- Dans  $\mathcal{P}(E)$  la loi  $\cap$  est distributive sur la loi  $\cup$  et la réciproque est vraie
- Dans  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  l'addition n'est pas distributive sur la multiplication car  $1 + (5 \times 3) \neq (1 + 5) \times (1 + 3)$

On vérifié dans  $\mathcal{M}_2(\mathbb{R})$  que la multiplication est distributive sur l'addition

Soient  $(a, b, c, d)$  et  $(t, x, y, z)$  et  $(\alpha, \beta, \gamma, \sigma)$  de  $\mathbb{R}^4$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  et  $B = \begin{pmatrix} x & y \\ t & z \end{pmatrix}$  et  $C = \begin{pmatrix} \alpha & \beta \\ \gamma & \sigma \end{pmatrix}$  des éléments de  $\mathcal{M}_2(\mathbb{R})$

$$\begin{aligned} A \times (B + C) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x + \alpha & y + \beta \\ t + \gamma & z + \sigma \end{pmatrix} = \begin{pmatrix} ax + bt + a\alpha + b\gamma & ay + bz + a\beta + b\sigma \\ cx + dt + c\alpha + d\gamma & cy + dz + c\beta + d\sigma \end{pmatrix} \\ &= \begin{pmatrix} ax + bt & ay + bz \\ cx + dt & cy + dz \end{pmatrix} + \begin{pmatrix} a\alpha + b\gamma & a\beta + b\sigma \\ c\alpha + d\gamma & c\beta + d\sigma \end{pmatrix} = (A \times B) + (A \times C) \quad (1) \end{aligned}$$

De même on démontre que  $(B + C) \times A = (B \times A) + (C \times A)$  (2)

De (1) et (2) on déduit que dans  $\mathcal{M}_2(\mathbb{R})$  que la multiplication est distributive sur l'addition

## 2) Définition d'un anneau

### Définition

Soit A un ensemble muni de deux lois de composition internes  $*$  et  $T$  on dit que  $(A, *, T)$  c'est un anneau ssi

- 1)  $(A, *)$  est un groupe commutatif
- 2)  $T$  est distributive sur  $*$
- 3)  $T$  est associative

### Remarque

- Si la loi  $T$  admet un élément neutre on dit que  $(A, *, T)$  c'est un anneau unitaire
- Si la loi  $T$  est commutative on dit que  $(A, *, T)$  c'est un anneau commutatif
- Les lois  $T$  et  $*$  sont généralement notées  $+$  et  $\times$ .
- Leurs neutres sont quant à eux notés  $0_A$  et  $1_A$ .

### Exemples

$(\mathbb{Z}, +, \times)$ ,  $(\mathbb{Q}, +, \times)$ ,  $(\mathbb{R}, +, \times)$  et  $(\mathbb{C}, +, \times)$  sont des anneaux commutatifs unitaires

- $(\mathbb{R}^2, +, \times)$  est un anneau commutatif.

Dans celui-ci rappelons les opérations :  $(x, y) + (x', y') = (x + x', y + y')$  et  $(x, y) \times (x', y') = (xx', yy')$

- $(\mathbb{Z}^n, +, \times)$ ,  $(\mathbb{R}^n, +, \times)$  et  $(\mathbb{C}^n, +, \times)$  sont des anneaux commutatifs.
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau commutatif unitaire

## 3) Règles du calcul dans un anneau

### Propriété

- 1) Soit  $(A, *, T)$  un anneau d'élément neutre  $e$  alors on a  $(\forall a \in A) : aTe = eTa = e$
- 2) Soit  $(A, *, T)$  un anneau d'élément neutre  $e$  et  $a'$  le symétrique de  $a$  dans  $(A, *)$  et  $b'$  le symétrique de  $b$  dans  $(A, *)$  donc  $\begin{cases} \forall (a, b) \in A^2; (aTb)' = a'Tb = aTb' \\ \forall (a, b) \in A^2; aTb = a'Tb' \end{cases}$

## Démonstration :

- On a  $aT(e * e) = aTe$  c à d  $(aTe) * (aTe) = aTe$  donc  $(aTe) * (aTe) = (aTe) * e$  et comme  $(A, *)$  est un groupe alors tout ses éléments sont réguliers donc  $aTe = e$   
De même on démontre que  $eTa = e$
- $\begin{cases} (a'Tb) * (aTb) = (a' * a)Tb = eTb = e \\ (aTb') * (aTb) = aT(b' * b) = aTe = e \\ aTb = [(aTb)']' = (a'Tb)' = a'Tb' \end{cases}$

**Remarque** on applique les propriétés de propriété précédente dans l'anneau  $(A, +, \times)$  on obtient

Soit  $a, b, c, d$  des éléments quelconques de  $A$ . On a :

- $a \times 0_A = 0_A \times a = 0_A$  (on dit que  $0_A$  est absorbant)

En effet  $a \times 0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A$

D'où, par régularité des éléments dans le groupe  $(A, +)$   $a \times 0_A = 0_A$

De même de l'autre côté.

- $a \times (-b) = -(a \times b) = (-a) \times b$  En effet :  $ab + a(-b) = a(b + (-b)) = a \times 0_A = 0_A$

D'où  $a(-b) = -(ab)$ . De même pour l'autre égalité.

- Développement des produits de sommes :

$$(a + b)(c + d) = ac + ad + bc + bd \text{ (Attention à l'ordre dans les produits)}$$

Immédiat en appliquant deux fois la distributivité.

- Pour  $n \in \mathbb{N}$ , on définit  $a^n$  par  $a^0 = 1_A$  et  $\forall n \in \mathbb{N} a^{n+1} = a^n a$ .

Alors  $\forall (n, p) \in \mathbb{N}^2 a^{n+p} = a^n a^p$  (immédiat par associativité de  $\times$ ).

Et  $\forall (n, p) \in \mathbb{N}^2 (a^n)^p = a^{np}$

(mais attention :  $(ab)^n = ab \times ab \times ab \times \dots \times ab$ ,  $\times$  n'est pas nécessairement commutative)

- Dans le groupe  $(A, +)$ , on a toujours la définition et les propriétés pour  $n.a$  ( $A, +$ ), et de plus :

$$(n.a) \times b = n(a.b) = a \times (nb) \text{ (qu'on peu noter } nab \text{ )}$$

En effet, pour  $n \in \mathbb{N}$ , on le montre aisément par récurrence, en utilisant la distributivité de  $\times$  sur  $+$ , puis pour

$$n = -p \text{ avec } p \in \mathbb{N}, \text{ on a : } (p(-a)) \times b = (p(-a) \times b) = p(-ab) = p(a(-b)) = a \times (p(-b))$$

d'après les règles précédentes.

$$\text{D'où } (n.a) \times b = n(ab) = a \times (nb) \text{ selon la règle. } (-p)x = p(-x)$$

## 4) les diviseurs de zéro dans un anneau

### Définition :

Soit  $(A, +, \times)$  un anneau et  $x \in A$

On dit que  $x$  c'est un diviseur de 0 dans  $A$  ssi  $\begin{cases} x \neq 0_A \\ \exists y \in A - \{0_A\} \quad x \times y = y \times x = 0_A \end{cases}$

### Exemples

- Dans  $(\mathbb{C}, +, \times), (\mathbb{R}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{Z}, +, \times)$  il n'existent pas des diviseurs de zéro
- Dans  $(\mathcal{M}_2(\mathbb{R}), +, \times)$  les deux matrices  $M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$  et  $N = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$  sont des diviseurs de zéro
- Dans  $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ ,  $\bar{2} \times \bar{3} = \bar{0}$  alors que  $\bar{2} \neq \bar{0}$  et  $\bar{3} \neq \bar{0}$  donc  $\bar{2}$  et  $\bar{3}$  sont des diviseurs de zéro
- Dans  $(\mathbb{R}^2, +, \times)$  ( les diviseurs de zéros sont les  $(x,0);(x,0)$  et  $(0,x);(0,x)$  avec  $x \neq 0$ .

## 5) anneau intègre

### Définition :

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

On dit que  $(A, +, \times)$  c'est un anneau intègre ssi n'admet pas des diviseurs de zéro c à d

$$\forall (a, b) \in A^2 \quad a \times b = 0_A \Leftrightarrow a = 0_A \text{ ou } b = 0_A$$

### Exemples

- $(\mathbb{C}, +, \times), (\mathbb{R}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{Z}, +, \times)$  sont des anneaux intègres
- $(\mathcal{M}_2(\mathbb{R}), +, \times)$  et  $(\mathcal{M}_3(\mathbb{R}), +, \times)$  deux anneaux non intègres

### Théorème :

Soit  $(A, *, T)$  un anneau unitaire et  $x \in A$

Si  $x$  admet un symétrique dans  $(A, T)$  alors  $x$  n'est pas un diviseur de 0 dans  $(A, *, T)$

### Démonstration :

Soit  $e$  l'élément neutre dans  $(A, *)$

# Cours

Soit  $a$  et  $b$  deux élément de  $A$  et  $a'$  le symétrique de  $a$  dans  $(A, T)$  et  $e'$  l'élément neutre dans  $(A, T)$

On  $aTb = e \Rightarrow a'TaTb = a'Te$

$\Rightarrow (a'Ta)Tb = e \Rightarrow e'Tb = e$

$\Rightarrow b = e$

## V- Le corps

### Définition :

Soit  $K$  un ensemble muni de deux lois de compositions internes  $*$  et  $T$  on dit que

$(K, *, T)$  c'est un corps ssi

- 1)  $(K, *, T)$  c'est un anneau unitaire
- 2) Tout élément de  $K$  différent neutre admet un symétrique pour la loi  $T$

### Remarque :

- Si la loi  $T$  est commutative on dit que  $(K, *, T)$  c'est un corps commutatif
- Tout élément de  $K - \{e\}$  admet un symétrique pour la loi  $T$  donc tout élément de  $K - \{e\}$  est régulier pour la loi  $T$

### Exemples :

- $(\mathbb{C}, +, \times), (\mathbb{R}, +, \times), (\mathbb{Q}, +, \times)$  sont des corps commutatifs
- $(\mathbb{Z}, +, \times)$  n'est pas un corps car  $2$  n'admet pas d'inverse
- $(M_2(\mathbb{R}), +, \times)$  n'est pas un corps car la matrice  $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$  n'a pas d'inverse car  $\det A = 0$
- $(\mathbb{Z}/6\mathbb{Z}, +, \times)$  n'est pas un corps car  $\bar{3}$  n'a pas d'inverse
- $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  avec  $p$  est un nombre premier positif c'est un corps commutatif
- On considère l'ensemble  $H = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} / (a, b) \in \mathbb{R}^2 \right\}$   
 $(H, +, \times)$  c'est un corps . Vérifier le ?

## Notation additive et notation multiplicative

On générale on désigne à la loi  $*$  par  $+$  :  $(x, y) \rightarrow x + y$  et la loi  $T$  par  $\times$  :  $(x, y) \rightarrow x \cdot y$

Et on désigne à l'élément neutre pour la loi  $*$  par  $0$  ( on l'appelle zéro du corps) et l'élément neutre pour la loi  $T$  par  $1$  ( on l'appelle unité du corps )

Donc  $(K, +, \times)$  c'est un corps si les lois  $+$  et  $\times$  vérifient les conditions suivantes :

$\forall(x, y, z) \in K^3$	$(x + y) + z = x + (y + z)$
$(\exists \mathbf{0} \in K)(\forall x \in K$	$x + \mathbf{0} = x \text{ et } \mathbf{0} + x = x$
$(\exists \mathbf{0} \in K)(\forall x \in K)$	$x + \mathbf{0} = x \text{ et } \mathbf{0} + x = x$
$(\forall x \in K)(\exists -x \in K)$	$x + (-x) = \mathbf{0} \text{ et } -x + x = \mathbf{0}$
$\forall(x, y) \in K^2$	$(xy)z = x(yz)$
$(\exists \mathbf{1} \in K)(\forall x \in K)$	$\mathbf{1}x = x \text{ et } x\mathbf{1} = x$
$(\forall x \in K - \{\mathbf{0}\})(\exists x^{-1} \in K - \{\mathbf{0}\})$	$xx^{-1} = \mathbf{1} \text{ et } x^{-1}x = \mathbf{1}$
$\forall(x, y, z) \in K^3$	$(y + z)x = xy + xz \text{ et } x(y + z) = xy + xz$

### Propriété :

Soit  $K$  un ensemble muni par deux loi de compositions internes  $*$  et  $T$ .

$(K, *, T)$  c'est un corps ssi

- 1)  $(K, *)$  c'est un groupe commutatif ( d'élément neutre  $e$  )
- 2)  $(K - \{e\}, T)$  c'est un groupe
- 3)  $T$  Distributive sur  $*$

### Application :

- 1) Soit  $(\mathbb{R}^2, +, \times)$  tel que :  $(a, b) + (a', b') = (a + a', b + b')$  et  $(a, b) \times (a', b') = (aa' - bb'; ab' + ba')$

Montrer que  $(\mathbb{R}^2, +, \times)$  c'est un corps commutatif

## Exercice 1

Soit  $E = [0,1]$ . On définit une loi  $*$  sur  $E$  par  $\forall x, y \in E, x * y = x + y - xy$

- Montrer que  $*$  est une loi de composition interne commutative et associative.
- Montrer que  $*$  possède un neutre.
- Quels sont les éléments symétrisables ? réguliers ?

## Corrigés

a)  $1 - (x + y - xy) = (1 - x)(1 - y)$

donc si  $x \leq 1$  et  $y \leq 1$  alors  $x * y \leq 1$ .

Par suite  $*$  est bien une loi de composition interne  
sur  $E$

$*$  est clairement commutative et associative.

b) 0 est élément neutre de  $E$ .

c) Si  $x \in ]0, 1]$  alors pour tout  $y \in [0, 1]$ ,

$$x * y = x(1 - y) + y > 0$$

et donc  $x$  n'est pas inversible (dans  $[0, 1]$ ).

Ainsi, seul 0 est inversible.

Pour tout  $x, y, z \in [0, 1]$ ,

$$x * y = x * z \Leftrightarrow y(1 - x) = z(1 - x)$$

Par suite, tout  $x \in [0, 1[$  est régulier tandis que 1 ne  
l'est visiblement pas.

## Exercice 2

Soit  $*$  une loi de composition interne associative sur  $E$ .

On suppose qu'il existe  $a \in E$  tel que l'application  $f: E \rightarrow E$  définie par  $f(x) = a * x * a$  soit surjective et on note  $b$  un antécédent de  $a$  par  $f$ .

- Montrer que  $e = a * b$  et  $e' = b * a$  sont neutres resp. à gauche et à droite puis que  $e = e'$ .
- Montrer que  $a$  est symétrisable et  $f$  bijective.

## Corrigé

Par la surjectivité de  $f$ , il existe  $b \in E$  tel que

$$a * b * a = a$$

a)  $a * b * a = a$

Pour tout  $x \in E$ , il existe  $a \in E$  tel qu'on peut écrire  
 $x = a * a * a$ .

Pour  $e = a * b$ ,  $e * x = a * b * a * a * a$   
 $= a * a * a = x$ .

Pour  $e' = b * a$ ,  $x * e' = x * b * a = a * a * a * b * a$   
 $= a * a * a$ .

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

b) Puisque  $a * b = b * a = e$ ,  $a$  est symétrisable et  
 $\text{sym}(a) = b$ .

De plus  $g: x \rightarrow b * x * b$  est clairement  
application réciproque de  $f$ .

### Exercice 3

Soit  $G = \mathbb{R}^* \times \mathbb{R}$  et  $*$  la loi dans  $G$  définie par  $(x, y) * (x', y') = (xx', xy' + y)$

1. Montrer que  $G$  est un groupe non commutatif

2. Montrer que  $[0; +\infty[ \times \mathbb{R}; *)$  est un sous-groupe de  $(G; *)$

### Corrigé

1. Si  $x \neq 0$  et  $x' \neq 0$  alors  $xx' \neq 0$  donc

$(x, y) * (x', y') = (xx', xy' + y) \in \mathbb{R}^* \times \mathbb{R}$  donc la loi

\* est interne

Soit  $(x, y)$  et  $(x', y')$  et  $(x'', y'')$  des éléments de  $G$

$$\begin{aligned} & \text{Et } ((x, y) * (x', y')) * (x'', y'') \\ &= (xx', xy' + y) * (x'', y'') = (xx'x, x(x'y + y') + y) \\ &= (xx'x'', xx'y'' + xy' + y) \end{aligned}$$

Donc la loi \* est associative

Soit  $(a, b)$  tel que pour tout  $(x, y) \in G$  :

$$(a, b) * (x, y) = (x, y) = (x, y) * (a, b)$$

Ces égalités équivalent à :

$$\begin{aligned} (ax, ay + b) &= (x, y) = (xa, xb + y) \\ \Leftrightarrow \begin{cases} ax = x = xa \\ ay + b = y = xb + y \end{cases} & \\ \Leftrightarrow \begin{cases} a = 1 \\ b = 0 \end{cases} & \end{aligned}$$

Donc  $(1, 0)$  est l'élément neutre.

Soit  $(x, y) \in G$ , on cherche  $(x', y')$  tel que

$$(x, y) * (x', y') = (1, 0) = (x', y') * (x, y)$$

Ces égalités équivaut à :

$$(xx', xy' + y) = (1, 0) = (xx', x'y + y')$$

$$\begin{aligned} & \text{On a } (x, y) * ((x', y') * (x'', y'')) \\ &= (x, y) * (x'x, x'y'' + y') = (xx'x, x(x'y + y') + y) \\ &= (xx'x'', xx'y'' + xy' + y) \end{aligned}$$

$$\Leftrightarrow \begin{cases} xx' = 1 = x'x \\ xy' + y = 0 = x'y + y' \end{cases}$$

$$\Leftrightarrow \begin{cases} x' = \frac{1}{x} \\ xy' + y = 0 = \frac{1}{x}y + y' \end{cases} \Leftrightarrow \begin{cases} x' = \frac{1}{x} \neq 0 \\ y' = -\frac{y}{x} \end{cases}$$

Donc le symétrique de  $(x, y)$  est  $\left(\frac{1}{x}, -\frac{y}{x}\right)$

donc  $(G, *)$  est un groupe.

Comme  $(1, 2) * (2, 0) = (2, 2)$  et  $(2, 0) * (1, 2) =$

$(2, 4)$  il est clair que ce groupe n'est pas commutatif

L'élément neutre de  $(G, *)$  est  $(1, 0) \in [0; +\infty[ \times \mathbb{R}$

Soit  $(x, y) \in [0; +\infty[ \times \mathbb{R}$  et  $(x', y') \in [0; +\infty[ \times \mathbb{R}$

$$\text{alors } (x, y) * \left(\frac{1}{x'}, -\frac{y'}{x'}\right) = \left(\frac{x}{x'}, x\left(-\frac{y'}{x'}\right) + y\right)$$

$$= \left(\frac{x}{x'}, \frac{-xy' + x'y}{x'}\right)$$

Comme  $\frac{x}{x'} > 0$  alors  $\frac{-xy' + x'y}{x'} \in \mathbb{R}$

donc  $[0; +\infty[ \times \mathbb{R}; *)$  est un sous-groupe de  $(G; *)$

## Exercice 4

On munit  $A = \mathbb{R} \times \mathbb{R}$  de deux lois définies par  $(x, y) + (x', y') = (x + x', y + y')$   
et  $(x, y) * (x', y') = (xx', xy' + x'y)$

1) Montrer  $(A, +)$  est un groupe commutatif

2) .

- a) Montrer que la loi  $*$  est commutative.
- b) Montrer que la loi  $*$  est associative
- c) Déterminer l'élément neutre de  $A$  pour la loi  $*$ .
- d) Montrer que  $(A, +, *)$  est un anneau .

## Corrigé

1) On a  $(x, y) + (x', y') = (x + x', y + y') \in A$

donc la loi est interne

$$\begin{aligned}(x, y) + [(x', y') + (x'', y'')] &= (x, y) + (x' + x'', y' + y'') \\ &= (x + (x' + x''), y + (y' + y'')) \\ &= ((x + x') + x'', (y + y') + y'') \\ &= [(x, y) + (x', y')] + (x'', y'')\end{aligned}$$

Soit  $(x', y')$  tel que  $(x, y) + (x', y') = (0, 0)$  cela  
équivaut à  $(x + x', y + y') = (0, 0) \Leftrightarrow \begin{cases} x + x' = 0 \\ y + y' = 0 \end{cases}$

$$\Leftrightarrow \begin{cases} x' = -x \\ y' = -y \end{cases} \text{ donc le symétrique de } (x, y) \text{ est } (-x, -y)$$

Et par suite  $(A, +)$  est un groupe commutatif.

2) .

a)  $(x, y) * (x', y') = (xx', xy' + x'y) = (x'x, x'y + xy') = (x', y') * (x, y)$  donc la loi  $*$  est commutative

$$\begin{aligned}\text{b)} \quad (x, y) * [(x', y') * (x'', y'')] &= (x, y) * (x'x'', x'y'' + x''y') \\ &= (xx'x'', x(x'y'' + x''y')) \\ &= (xx'x'', xx'y'' + xx''y' + x'x''y) \\ &[(x, y) * (x', y')] * (x'', y'') = (xx', xy' + x'y) * (x'', y'') \\ &= (xx'x'', xx'y'' + x''(xy' + x'y)) \\ &= (xx'x'', xx'y' + x'x''y)\end{aligned}$$

Donc la loi  $*$  est associative

Donc la loi  $+$  est associative .

$$(x, y) + (x', y') = (x + x', y + y') = (x' + x, y' + y) = (x', y') + (x, y)$$

Donc la loi  $+$  est commutative

Soit  $(a, b)$  tel que  $(x, y) + (a, b) = (x, y)$  il est clair que  $(a, b) = (0, 0)$  est l'unique élément neutre

c) Soit  $(e, f)$  tel que pour tout  $(x, y) \in A$ ,

$$(x, y) * (e, f) = (x, y)$$

et  $f$  vérifiant  $\begin{cases} xe = x \\ xf + ye = y \end{cases} \Leftrightarrow \begin{cases} e = 1 \\ xf + y = y \end{cases} \Leftrightarrow \begin{cases} e = 1 \\ f = 0 \end{cases}$  donc  $(1, 0) \in A$  est l'élément neutre de  $A$

pour la loi  $*$ .

d) Toutes les propriétés pour qu'un ensemble muni de deux lois soit un anneau sont dans les questions précédentes sauf la distributivité de  $*$  par rapport à l'addition (à gauche ou à droite puisque la loi  $*$  est commutative), c'est d'ailleurs cette commutativité qui rend l'anneau commutatif).

$$\begin{aligned}(x, y) * [(x', y') + (x'', y'')] &= (x, y) * (x' + x'', y' + y'') \\ &= (x(x' + x''), y(y' + y'')) + (x' + x'')y \\ &= (xx' + xx'', xy' + xy'' + x'y + x''y) \\ &= (xx' + xx'', xy' + x'y + xy'' + x''y) \\ &= (xx', xy' + x'y) + (xx'', xy'' + x''y) \\ &= (x, y) * (x', y') + (x, y) * (x'', y'')\end{aligned}$$

Et voilà  $(A, +, *)$  est un anneau commutatif.

## Exercice 5

Soit  $\mathbf{K}$  l'ensemble des nombres complexes de la forme  $z = r + is$  où  $r \in \mathbb{Q}$  et  $s \in \mathbb{Q}$

- 1) Montrer que  $(\mathbf{K}, +)$  est un groupe commutatif
- 2) Montrer que  $(\mathbf{K}^*, \cdot)$  est un groupe commutatif.
- 3) En déduire que  $(\mathbf{K}, +, \cdot)$  est un corps commutatif.

### Correction

1)  $0 = 0 + i \cdot 0 \in K$  car  $0 \in \mathbb{Q}$  et  $0 \in \mathbb{Q}$

Soient  $z_1 = r_1 + is_1 \in K$  et  $z_2 = r_2 + is_2 \in K$

On a  $z_1 - z_2 = r_1 + is_1 - (r_2 + is_2)$

$$= r_1 - r_2 + i(s_1 - s_2) \in K$$

car  $r_1 - r_2 \in \mathbb{Q}$  et  $s_1 - s_2 \in \mathbb{Q}$

L'addition étant commutative dans  $\mathcal{C}$ , et par suite  
 $(K, +)$  est un sous-groupe commutatif de  $(\mathcal{C}, +)$ ,

Donc c'est un groupe commutatif.

2)  $1 = 1 + i \cdot 0 \in K$  car  $1 \in \mathbb{Q}$  et  $0 \in \mathbb{Q}$

$z_1 = r_1 + is_1 \in K$  et  $z_2 = r_2 + is_2 \in K$

$$\begin{aligned} z_1 z_2^{-1} &= \frac{r_1 + is_1}{r_2 + is_2} = \frac{(r_1 + is_1)(r_2 - is_2)}{r_2^2 + s_2^2} \\ &= \frac{r_1 r_2 + s_1 s_2 + i(r_2 s_1 - r_1 s_2)}{r_2^2 + s_2^2} \end{aligned}$$

$$= \frac{r_1 r_2 + s_1 s_2}{r_2^2 + s_2^2} + i \frac{(r_2 s_1 - r_1 s_2)}{r_2^2 + s_2^2}$$

Donc  $z_1 z_2^{-1} \in K$  car  $\frac{r_1 r_2 + s_1 s_2}{r_2^2 + s_2^2} \in \mathbb{Q}$  et  $\frac{(r_2 s_1 - r_1 s_2)}{r_2^2 + s_2^2} \in \mathbb{Q}$

Comme la multiplication étant commutative

dans  $\mathcal{C}$ , donc  $(\mathbf{K}^*, \cdot)$  est un sous-groupe  
 commutatif de  $(\mathcal{C}^*, \cdot)$

Et par suite  $(\mathbf{K}^*, \cdot)$  est un groupe commutatif.

3) il ne reste qu'à rappeler que la multiplication  
 est distributive par rapport à l'addition dans  
 $\mathcal{C}$ , pour conclure que  $(\mathbf{K}, +, \cdot)$  est un corps  
 commutatif, car la multiplication est  
 commutatif.