I – Lois de composition internes

1 – Des ensembles particuliers

a – Ensembles des polynômes de degré inférieur ou égal à n : $\mathcal{P}_n$ ou $\mathbb{R}_n[X]$

Définition

Soit $n\epsilon\mathbb{N}$.

L'ensemble des polynômes à coefficients réels de degré inférieur ou égal à n est :

$$\mathcal{P}_n = \mathbb{R}_n[X] = \{P\epsilon\mathcal{F}(\mathbb{R},\mathbb{R}) / \ P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \text{ où } (a_n, a_{n-1}, \dots, a_1, a_0)\epsilon\mathbb{R}^{n+1}\}$$

On définit l'addition et la multiplication dans $\mathcal{P}_n$ par :

$$\forall(P,Q)\epsilon{\mathcal{P}_n}^2 : \begin{cases}(P+Q)(x) = P(x) + Q(x)\\(P\times Q)(x) = P(x)\times Q(x)\end{cases}$$

b – Ensembles des fonctions numériques définies sur un intervalle de $\mathbb{R}$: $\mathcal{F}(I,\mathbb{R})$

Définition

Soit I un intervalle de $\mathbb{R}$.

L'ensemble des fonctions numériques définies sur l'intervalle I est :

$$\mathcal{F}(\mathbb{I},\mathbb{R}) = \{f \ / \ f:\mathbb{I}\to\mathbb{R}, x\mapsto f(x)\}$$

On définit l'addition et la multiplication dans $\mathcal{F}(\mathbb{I},\mathbb{R})$ par :

$$\left(\forall(f,g)\epsilon\left(\mathcal{F}(\mathbb{I},\mathbb{R})\right)^2\right)(\forall x\epsilon\mathbb{I}) : \begin{cases}(f+g)(x) = f(x) + g(x)\\(f\times g)(x) = f(x)\times g(x)\end{cases}$$

c – Ensembles des classes d'équivalence modulo n : $\mathbb{Z}/_{n\mathbb{Z}}$

Définition

Soit $n\epsilon\mathbb{N}^*$.

L'ensemble des classes d'équivalence modulo n est :

$$\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

On définit l'addition et la multiplication dans $\mathbb{Z}/_{n\mathbb{Z}}$ par :

$$\left(\forall(\bar{x},\bar{y})\epsilon\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^2\right) : \begin{cases}\bar{x}+\bar{y} = \overline{x+y}\\\bar{x}\times\bar{y} = \overline{x\times y}\end{cases}$$

d – Ensembles des parties d'un ensemble E : $\mathcal{P}(E)$

Définition

Soit E un ensemble.

L'ensemble de toutes les parties de E est :

$$\mathcal{P}(E) = \{A \ / A\subset E\}$$

$$\forall(A,B)\epsilon\left(\mathcal{P}(E)\right)^2, on a : \begin{cases} x\epsilon A\cap B \Leftrightarrow x\epsilon A \ et \ x\epsilon B\\ x\epsilon A\cup B \Leftrightarrow x\epsilon A \ ou \ x\epsilon B\\ x\epsilon\bar{A} \Leftrightarrow x\notin A\\ x\in A-B \Leftrightarrow x\epsilon A \ et \ x\notin B\\ x\in A\Delta B \Leftrightarrow x\epsilon A-B \ ou \ x\epsilon B-a\end{cases}$$

e – Ensemble des matrices carrées d'ordre 2 : $\mathcal{M}_2(\mathbb{R})$

Définition

L'ensemble des matrices carrées d'ordre 2 est :

$$\mathcal{M}_2(\mathbb{R}) = \left\{\begin{pmatrix}a & c\\ b & d\end{pmatrix} / (a,b,c,d)\epsilon\mathbb{R}^4\right\}$$

On définit l'addition et la multiplication dans $\mathcal{M}_2(\mathbb{R})$ par :

$$\forall(a,b,c,d)\epsilon\mathbb{R}^4, \forall(x,y,z,t)\epsilon\mathbb{R}^4 : \begin{cases}\begin{pmatrix}a & c\\ b & d\end{pmatrix} + \begin{pmatrix}x & z\\ y & t\end{pmatrix} = \begin{pmatrix}a+x & c+z\\ b+y & d+t\end{pmatrix}\\ \begin{pmatrix}a & c\\ b & d\end{pmatrix} \times \begin{pmatrix}x & z\\ y & t\end{pmatrix} = \begin{pmatrix}ax+cy & az+ct\\ bx+dy & bz+dt\end{pmatrix}\end{cases}$$

f – Ensembles des matrices carrées d'rdre 3 : $\mathcal{M}_3(\mathbb{R})$

Définition

L'ensemble des matrices carrées d'ordre 3 est :

$$\mathcal{M}_3(\mathbb{R}) = \left\{\begin{pmatrix}a_1 & a_2 & a_3\\ b_1 & b_2 & b_3\\ c_1 & c_2 & c_3\end{pmatrix} / (a_1,a_2,a_3,b_1,b_2,b_3,c_1,c_2,c_3)\epsilon\mathbb{R}^9\right\}$$

On définit l'addition et la multiplication dans $\mathcal{M}_3(\mathbb{R})$ par :

- $\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} + \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} = \begin{pmatrix} a_1+x_1 & a_2+x_2 & a_3+x_3 \\ b_1+y_1 & b_2+y_2 & b_3+y_3 \\ c_1+z_1 & c_2+z_2 & c_3+z_3 \end{pmatrix}$
- $\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \times \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} = \begin{pmatrix} a_1x_1+a_2y_1+a_3z_1 & a_1x_2+a_2y_2+a_3z_2 & a_1x_3+a_2y_3+a_3z_3 \\ b_1x_1+b_2y_1+b_3z_1 & b_1x_2+b_2y_2+b_3z_2 & b_1x_3+b_2y_3+b_3z_3 \\ c_1x_1+c_2y_1+c_3z_1 & c_1x_2+c_2y_2+c_3z_2 & c_1x_3+c_2y_3+c_3z_3 \end{pmatrix}$

g – Ensemble des transformations du plan : $\mathcal{T}$

Définition

- On appelle transformation du plan $\mathcal{P}$ toute application bijective de $\mathcal{P}$ dans $\mathcal{P}$.
- Les ensembles des translations, des homothéties, des rotations sont des parties de l'ensemble de transformations $\mathcal{T}$.
- $(\forall (f,g)\epsilon \mathcal{T}^2)(\forall M \epsilon \mathcal{P})$: $(f \circ g)(M) = f(g(M))$.

2 - Définition - exemples - notations

Définition

Soit E un ensemble non vide.
On appelle loi de composition interne sur E, toute application $f: E \times E \to E$.
Toutefois, en général, au lieu de noter l'image d'un couple (x,y) d'éléments de E par $f(x,y)$ on utilise plus souvent une notation du type : $x * y$ ou $x \perp y$ ou $x \top y$ ou $x + y$ ou $x \times y$.
On note $(E,*)$ un ensemble E muni d'une loi de composition interne $*$.

Exemples

Lois de composition internes particulières :

- L'addition $(+)$ est une loi de composition interne dans $\mathbb{N}, \mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathcal{P}_n, \mathcal{F}(\mathbb{I},\mathbb{R}), \mathbb{Z}/_{n\mathbb{Z}}, \mathcal{M}_2(\mathbb{R}), \mathcal{M}_3(\mathbb{R})$.
- La multiplication $(\times)$ est une loi de composition interne dans $\mathbb{N}, \mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathcal{P}_n, \mathcal{F}(\mathbb{I},\mathbb{R}), \mathbb{Z}/_{n\mathbb{Z}}, \mathcal{M}_2(\mathbb{R}), \mathcal{M}_3(\mathbb{R})$
- L'intersection $(\cap)$, la réunion $(\cup)$, la différence symétrique (Δ) sont des lois de composition internes dans $\mathcal{P}(E)$.

Exercices

1) Soit $E = [0,1]$. Soit $(x,y)\epsilon E$ on pose : $x * y = x + y - xy$.
Montrer que $*$ est une loi de composition interne sur E.
2) Soit $E = \{(x,y)\epsilon \mathbb{R}^2 / x^2 - y^2 = 1\}$.
Soient $(x,y)\epsilon\mathbb{R}^2$ et $(x',y')\epsilon\mathbb{R}^2$, on pose $(x,y) \top (x',y') = (xx'+yy', xy'+yx')$.
Montrer que $\top$ est une loi de composition interne dans E
3) Soit $E =]-1,1[$.
Soient $(x,y)\epsilon E^2$, on pose : $x \perp y = \frac{x+y}{1+xy}$.
Montrer que $\perp$ est une loi de composition interne dans E

3 – Stabilité des parties pour une loi de composition interne

Définition

Soit $(E,*)$ un ensemble muni d'une loi de composition interne $*$, et soit F une partie de E.
On dit que F est stable par $*$ si et seulement si pour tout x et y de F on a : $x * y \in$ F.
On dit que $*$ définie une loi de composition interne dans F appelée loi induite par $*$ sur F

Exemples

1) Montrer que $A = \left\{\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} / a \in \mathbb{R}\right\}$ est une partie stable de $(\mathcal{M}_2(\mathbb{R}),\times)$
2) Montrer que $F = \{z\epsilon\mathbb{C} / R_e(z) \geq 0\}$ est une partie stable de $(\mathbb{C},+)$ mais n'est pas une partie stable de $(\mathbb{C},\times)$
3) Montrer que $G = \left\{\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} / (a,b,c) \in \mathbb{R}^3\right\}$ est une partie stable de $(\mathcal{M}_3(\mathbb{R}),\times)$

III – Propriétés des lois de composition internes

1 – Commutativité

Définition

Soit $(E,*)$ un ensemble muni d'une loi de composition interne $*$.
On dit que la loi $*$ est commutative dans $(E,*)$ si et seulement si pour tout $(x,y)\epsilon E^2$ on a: $x * y = y * x$

Remarque

La loi $*$ n'est pas commutative dans $(E,*)$ $\Leftrightarrow$ $(\exists(a,b)\epsilon E^2 :\ a*b \neq b*a$

Exemples

1) L'addition est commutative dans $\mathbb{N},\mathbb{Z},\mathbb{D},\mathbb{Q},\mathbb{R},\mathbb{C},\mathcal{P}_n,\mathcal{F}(\mathbb{I},\mathbb{R}),{}^{\mathbb{Z}}/_{n\mathbb{Z}},\mathcal{M}_2(\mathbb{R}),\mathcal{M}_3(\mathbb{R})$.

2) La multiplication est commutative dans $\mathbb{N},\mathbb{Z},\mathbb{D},\mathbb{Q},\mathbb{R},\mathbb{C},\mathcal{P}_n,\mathcal{F}(\mathbb{I},\mathbb{R}),{}^{\mathbb{Z}}/_{n\mathbb{Z}},$ mais elle n'est pas commutative dans $\mathcal{M}_2(\mathbb{R}), et\ \mathcal{M}_3(\mathbb{R})$.

2 – Associativité

Définition

Soit $(E,*)$ un ensemble muni d'une loi de composition interne $*$.
On dit que la loi $*$ est associative dans $(E,*)$ si et seulement si pour tout $(x,y,z)\epsilon E^3$ on a: $(x*y)*z = x*(y*z)$

Remarques

- La loi $*$ n'est pas associative dans $(E,*)$ $\Leftrightarrow$ $(\exists(a,b,c)\epsilon E^3 :\ (a*b)*c \neq a*(b*c)$
- Si la loi $*$ est associative dans $(E,*)$, alors on peut écrire : $(a*b)*c = a*(b*c) = a*b*c$

Exemples

1) L'addition est associative dans $\mathbb{N},\mathbb{Z},\mathbb{D},\mathbb{Q},\mathbb{R},\mathbb{C},\mathcal{P}_n,\mathcal{F}(\mathbb{I},\mathbb{R}),{}^{\mathbb{Z}}/_{n\mathbb{Z}},\mathcal{M}_2(\mathbb{R}),\mathcal{M}_3(\mathbb{R})$.

2) La multiplication est associative dans $\mathbb{N},\mathbb{Z},\mathbb{D},\mathbb{Q},\mathbb{R},\mathbb{C},\mathcal{P}_n,\mathcal{F}(\mathbb{I},\mathbb{R}),{}^{\mathbb{Z}}/_{n\mathbb{Z}},\mathcal{M}_2(\mathbb{R}),\mathcal{M}_3(\mathbb{R})$.

3) La réunion $(\cup)$ et l'intersection $(\cap)$ sont associatives respectivement dans $(\mathcal{P}(E),\cup)$ et $(\mathcal{P}(E),\cap)$.

3 – Elément neutre

Définition

Soit $(E,*)$ un ensemble muni d'une loi de composition interne $*$. Soit $e\ \epsilon\ E$.
On dit que e est un élément neutre de $(E,*)$ si et seulement si : $(\forall x\ \epsilon\ E):\ x*e = e*x = x$

Exemples

1) 0 est l'élément neutre de $(\mathbb{N},+);\ (\mathbb{Z},+);\ (\mathbb{Q},+);\ (\mathbb{R},+);\ (\mathbb{C},+)$

2) 1 est l'élément neutre de $(\mathbb{N}^*,\times);\ (\mathbb{Z},^*\times);\ (\mathbb{Q}^*,\times);\ (\mathbb{R}^*,\times);\ (\mathbb{C}^*,\times)$

3) La matrice $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ est l'élément neutre de $(\mathcal{M}_2(\mathbb{R}),\times)$ La matrice nulle $O = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$ est l'élément de $(\mathcal{M}_2(\mathbb{R}),+)$

4) $\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$ est l'élément neutre de $(\mathcal{M}_3(\mathbb{R}),+)$ et $\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$ est l'élément neutre de $(\mathcal{M}_3(\mathbb{R}),\times)$.

Proposition

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

Remarques

- Si la loi de composition interne $*$ est commutative, alors pour montrer que e est l'élément neutre de $(E,*)$ il suffit de montrer seulement l'une des égalités : $(\forall x\ \epsilon\ E):\ x*e = x$ ou $(\forall x\ \epsilon\ E):\ e*x = x$.
- Si A est une partie stable de $(E,*)$ et si e est l'élément neutre de $(E,*)$ alors n'est pas nécessairement l'élément neutre de $(A,*)$

Exemples

1) On munit $\mathbb{Z}$ de la relation $*$ définie par : $(\forall(x,y)\epsilon\mathbb{Z}^2 :\ x*y = x+y+2)$.

a) Montrer que $*$ est une loi de composition interne dans $\mathbb{Z}$.

b) Montrer que $*$ est associative et commutative

c) Montrer que $*$ admet un élément neutre que l'on déterminera

2) Soit $E = \left\{M(a,b) = \begin{pmatrix}a & b\\ -4b & a+2b\end{pmatrix} / (a,b)\epsilon\mathbb{R}^2\right\}$.

a) Montrer que + est une loi de composition interne dans E

b) Montrer que + est associative et commutative

c) la loi + admet-elle un élément neutre dans E ?

4 – Eléments symétrisables

Définition

Soit $(E,*)$ un ensemble muni d'une loi de composition interne $*$, soit e l'élément neutre de $(E,*)$ et soit $x\epsilon E$.
On dit que x est symétrisable ou inversible pour la loi $*$ si et seulement s'il existe $x'\epsilon E$ tel que : $x*x' = x'*x = e$

L'élément x' de E s'appelle le symétrique ou l'inverse de x pour $\ast$.

Remarques

- Si x' est le symétrique de x pour la loi $\ast$, alors x est le symétrique de x' pour la loi $\ast$.
- Si x' est le symétrique de x pour la loi $\ast$, on dit que $x \; et \; x'$ sont symétriques dans $(E,\ast)$
- Si la loi $\ast$ est commutative, pour montrer que $x \; et \; x'$ sont symétriques dans $(E,\ast)$ on peut se contenter à montrer que $x \ast x' = e$ ou $x' \ast x = e$.

Exemples

1) Dans $(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{R},+)$; $(\mathbb{C},+)$, Chaque élément x admet un symétrique x' qui est son opposé : $x' = -x$.

2) Dans $(\mathbb{Q}^*,\times)$; $(\mathbb{R}^*,\times)$; $(\mathbb{C}^*,\times)$, Chaque élément x admet un symétrique x' qui est son inverse : $x' = x^{-1}$.

3) Dans $(\mathcal{M}_2(\mathbb{R}),\times)$ la matrice $\begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix}$ est le symétrique de la matrice $\begin{pmatrix} 7 & -3 \\ -2 & 1 \end{pmatrix}$, par contre la matrice $\begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}$ n'a pas de symétrique.

Proposition 1 (unicité du symétrique)
Soit $(E,\ast)$ un ensemble muni d'une loi de composition interne associative $\ast$ qui admet un élément neutre e.
Si x est symétrisable dans $(E,\ast)$, alors le symétrique de x est unique.

Preuve

Soit $x \epsilon E$. Supposons que x admet deux symétriques $x' \; et \; x"$ donc on a : $x \ast x' = x' \ast x = e$ et $x \ast x" = x" \ast x = e$.
Comme $\ast$ est associative, alors : $x" = x" \ast e = x" \ast (x \ast x') = (x" \ast x) \ast x' = e \ast x' = x'$. d'où $x" = x'$.

Proposition 2
Soit $(E,\ast)$ un ensemble muni d'une loi de composition interne associative $\ast$ qui admet un élément neutre e.
Soient $x \; et \; y$ deux éléments symétrisables dans $(E,\ast)$ de symétriques respectifs $x' et \; y'$, alors $x \ast y$ est symétrisable dans $(E,\ast)$ et son symétrique est $(x \ast y)' = y' \ast x'$.

Preuve

On a : $(x \ast y) \ast (y' \ast x') = x \ast (y \ast y') \ast x' = x \ast e \ast x' = x \ast x' = e$
et $(y' \ast x') \ast (x \ast y) = y' \ast (x' \ast x) \ast y = y' \ast e \ast y = y' \ast y = e$ D'où $(x \ast y)' = y' \ast x'$

Exemples

- Soient $f \; et \; g$ deux applications bijectives d'un ensemble dans lui-même, alors $f \circ g$ est une application bijective de E dans E et sa bijection réciproque est : $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
- Soient M et N deux matrices inversibles dans $(\mathcal{M}_3(\mathbb{R}),\times)$, alors M×N est inversible et sa matrice inverse est : $(M \times N)^{-1} = N^{-1} \times M^{-1}$.

5 – Elément absorbant

Définition
Soit $(E,\ast)$ un ensemble muni d'une loi de composition interne $\ast$, et $a \in E$.
On dit que a est un élément absorbant pour $\ast$ si et seulement si pour tout $x \in E$, on a : $a \ast x = x \ast a = a$.

Exemples

- Dans $\mathbb{N}, \mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R} \; et \; \mathbb{C}$, le nombre 0 est un élément absorbant pour la multiplication.
- Dans $\mathcal{P}(E)$, l'ensemble E est l'élément absorbant pour l'intersection
- Dans $\mathcal{M}_2(\mathbb{R})$, la matrice nulle $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est l'élément absorbant pour la multiplication.

6 – Eléments réguliers

Définition
Soit $(E,\ast)$ un ensemble muni d'une loi de composition interne $\ast$, et $a \in E$.
On dit que a est un élément régulier pour $\ast$ si et seulement si pour tout $(x,y) \in E^2$, on a :

$$\begin{cases} a \ast x = a \ast y & \Rightarrow x = y \\ x \ast a = y \ast a & \Rightarrow x = y \end{cases}$$

Remarque

- Si la loi $\ast$ est commutative dans E , pour montrer que a est un élément régulier pour $\ast$, il suffit de montrer seulement l'une des deux implications : $a \ast x = a \ast y \Rightarrow x = y$ ou $x \ast a = y \ast a \Rightarrow x = y$.
- Pour dire aussi qu'un élément a est régulier, on dit aussi simplifiable.

IV – Morphismes

1 – Définition et exemples

Définition

Soient $(E,*)$ *et* $(F,\top)$ deux ensembles munis de deux lois de composition internes $*$ *et* $\top$, et soit f une application de E vers F.

- On dit que f est un morphisme de $(E,*)$ dans $(F,\top)$ si et seulement si
$$(\forall(x,y)\epsilon E^2: f(x*y) = f(x)\top f(y))$$
- Un morphisme est appelé aussi un homomorphisme
- un endomorphisme de $(E,*)$ est un homomorphisme de $(E,*)$ dans lui-même
- Un isomorphisme de $(E,*)$ dans $(F,\top)$ est un homomorphisme bijectif de $(E,*)$ dans $(F,\top)$
- Un automorphisme de $(E,*)$ est un endomorphisme bijectif de $(E,*)$

Exemples

1) L'application $f: x \mapsto e^x$ est un homomorphisme de $(\mathbb{R},+)$ dans $(\mathbb{R}_+^*,\times)$

2) L'application $g: x \longmapsto \ln(x)$ est un homomorphisme de $(\mathbb{R}_+^*,\times)$ dans $(\mathbb{R},+)$

2 – Propriétés des morphismes

Proposition

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

- ★ $f(E)$ est une partie stable de $(F,\top)$.
- ★ Si la loi $*$ est associative dans E, alors la loi $\top$ est associative dans $f(E)$.
- ★ Si la loi $*$ est commutative dans E, alors la loi $\top$ est commutative dans $f(E)$.
- ★ Si e est l'élément neutre de la loi $*$ dans E, alors $f(e)$ est l'élément neutre de la loi $\top$ dans $f(E)$.
- ★ Si x' est le symétrique de x dans $(E,*)$, alors $f(x')$ est le symétrique de $f(x)$ dans $(f(E),\top)$.
- ★ Si f est bijectif de E dans F, alors : $f(E) = F$.

Corollaire

Si f un isomorphisme de $(E,*)$ dans $(F,\top)$, alors f transfère toutes les propriétés de la loi $*$ dans $(E,*)$ vers la loi $\top$ dans $(F,\top)$. On dit que $(E,*)$ et $(F,\top)$ ont la même structure .

Exemples

1) Soit f un homomorphisme de $(E,*)$ dans $(F,\top)$.

a) Soit B une partie stable de $(F,\top)$. Montrer que $f^{-1}(B)$ est une partie stable de $(E,*)$.

b) Soit A une partie stable de $(E,*)$. Montrer que $f(A)$ est une partie stable de $(F,\top)$.

2) Soit $F = \left\{\begin{pmatrix}2 & a\\1 & 0\end{pmatrix} / a \epsilon \mathbb{R}\right\}$ et $\begin{cases} f: \mathbb{R} \longrightarrow F \\ \quad x \longmapsto \begin{pmatrix}2 & x\\1 & 0\end{pmatrix}\end{cases}$.

a) Montrer que f est un isomorphisme de $(\mathbb{R},+)$ dans $(F,+)$.

b) Sachant que 0 est l'élément neutre de $(\mathbb{R},+)$, Déterminer l'élément neutre de $(F,+)$.

c) Montrer que + est associative et commutative dans F

d) Déterminer le symétrique de la matrice $A = \begin{pmatrix}2 & 7\\1 & 0\end{pmatrix}$.

V – Groupes

1 – Définition et exemples

Définition

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

- On dit que $(G,*)$ est un groupe si et seulement si $\begin{cases}\text{La loi } * \text{ est associative}\\ \text{La loi } * \text{ admet un élément neutre dans G}\\ \text{Tout élément de G admet un symétrique dans G}\end{cases}$
- Si en plus la loi $*$ est commutative, le groupe $(G,*)$ est dit commutatif ou abélien

Exemples

1) $(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{R},+)$; $(\mathbb{C},+)$ sont des groupes commutatifs.

2) $(\mathbb{Q}^*,\times)$; $(\mathbb{R}^*,\times)$; $(\mathbb{C}^*,\times)$ sont des groupes commutatifs.

3) $(\mathcal{M}_2(\mathbb{R}),+)$ et $(\mathcal{M}_3(\mathbb{R}),+)$ sont des groupes commutatifs.

4) $\left(\mathbb{Z}/_{n\mathbb{Z}},+\right)$ est un groupe commutatif

2 – Propriétés des groupes

Proposition 1

Soit $(G,*)$ un groupe. Alors :

- ★ G est non vide. G contient au moins son élément neutre
- ★ Son élément neutre e est unique.
- ★ Chaque élément x de G admet un unique symétrique x'
- ★ Si x' est le symétrique de x et y' est le symétrique de y, alors le symétrique de $x*y$ est :
  $(x*y)'=y'*x'$
- ★ Chaque élément de G est régulier

Proposition 2

Soit $(G,*)$ un groupe d'élément neutre e et soit $(a,b)\in G^2$ et a' le symétrique de a dans $(G,*)$. alors:

- ★ L'équation $a*x=b$, d'inconnue x, admet une unique solution dans G : $x=a'*b$
  Autrement dit : $a*x=b \iff x=a'*b$
- ★ L'équation $x*a=b$, d'inconnue x, admet une unique solution dans G : $x=b*a'$
  Autrement dit : $x*a=b \iff x=b*a'$

Exercice

On définit la relation $\perp$ dans $\mathbb{R}$ par : $\left(\forall(a,b)\in\mathbb{R}^2,\ a\perp b=\ln(e^a+e^b)\right)$.

1) Montrer que $(\mathbb{R},\perp)$ est un groupe commutatif.
2) Montrer que tout réel est régulier dans $(\mathbb{R},\perp)$.
3) Résoudre l'équation : $x\perp 3=-1$

3 – Sous-groupes

Définition

Soit $(G,*)$ un groupe et soit H une partie non vide de G.

On dit que $(H,*)$ est un sous-groupe de $(G,*)$ si et seulement si : $\begin{cases} H \text{ est stable pour la loi } * \\ (H,*) \text{ est un groupe}\end{cases}$

Exemples

1) $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{R},+)$.
2) $(\mathbb{N},+)$ n'est pas un sous-groupe de $(\mathbb{Z},+)$ car 1 n'a pas de symétrique dans $(\mathbb{N},+)$.
3) Soit $(G,*)$ un groupe d'élément neutre e, alors $\{e\}$ est un sous-groupe de $(G,*)$.

Proposition

Soit $(G,*)$ un groupe et $(H,*)$ un sous-groupe de $(G,*)$. Alors :

- ★ $H\neq\emptyset$
- ★ Si e est l'élément neutre dans $(G,*)$, alors e est aussi l'élément neutre dans $(H,*)$.
- ★ Si $x\in H$, le symétrique de x dans $(G,*)$ est le symétrique de x dans $(H,*)$.
- ★ $(\forall(x,y)\in H^2)$: $x*y\in H$.
- ★ $(\forall(x,y)\in H^2)$: $x*y'\in H$ où y' est le symétrique de y dans $(G,*)$.

Propriété caractéristique d'un sous-groupe

Soit $(G,*)$ un groupe et soit H une partie de G.

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

Remarque

Dorénavant, on peut noter les lois de composition internes par + ou par x.

Pour montrer que $(H,*)$ est un sous-groupe de $(G,*)$ on peut utiliser les natations additive et multiplicative :

- ♦ Avec la notation additive : $\begin{cases} H\neq\emptyset \\ (\forall(x,y)\in H^2):\ x-y\in H\end{cases}$
- ♦ Avec la notation multiplicative : $\begin{cases} H\neq\emptyset \\ (\forall(x,y)\in H^2):\ x\times y^{-1}\in H\end{cases}$

4 – Morphismes de groupes

Proposition

Soit f un morphisme de $(G,*)$ dans $(F,\perp)$.

- ★ Si $(G,*)$ est un groupe, alors $(f(G),\perp)$ est un groupe.
- ★ Si f est un isomorphisme et $(G,*)$ est un groupe, alors $(F,\perp)$ est aussi un groupe.

Remarque

Tout morphisme d'un groupe $(G,*)$ dans un groupe $(F,\perp)$, est appelé un morphisme de groupes

Exercice

On définit sur $\mathbb{R}$, la loi de composition $*$ par : $\left(\forall (x,y)\in\mathbb{R}^2\right),\ x*y = x+y-3xy$

1) a) Vérifier que : $\left(\forall (x,y)\in\mathbb{R}^2\right),\ (1-3x)(1-3y)=1-3(x*y)$

b) Montrer que $\left(\mathbb{R}-\left\{\frac{1}{3}\right\},*\right)$ est un groupe commutatif.

2) On considère l'application $\begin{array}{l}\varphi:\mathbb{R}-\left\{\frac{1}{3}\right\}\to\mathbb{R}^*\\ \quad x\ \mapsto 1-3x\end{array}$.

Montrer que φ est un isomorphisme de $\left(\mathbb{R}-\left\{\frac{1}{3}\right\},*\right)$ dans $(\mathbb{R}^*,\times)$

VI – Anneaux

1 – Distributivité d'une loi par rapport à une autre loi

Définition

Soit E un ensemble non vide muni de deux lois de composition internes $*$ et $\top$.

On dit que la loi $\top$ est distributive par rapport à la loi $*$ si et seulement si :

$$\left(\forall (x,y,z)\in E^3\right):\begin{cases} x\top(y*z)=(x\top y)*(x\top z)\\ (y*z)\top x=(y\top x)*(z\top x)\end{cases}$$

Exemples

1) Sur les ensembles $\mathbb{N}$; $\mathbb{Z}$; $\mathbb{Q}$; $\mathbb{R}$ et $\mathbb{C}$ la multiplication $\times$ est distributive par rapport à l'addition +

2) Sur $\mathcal{M}_2(\mathbb{R})$ *et* $\mathcal{M}_3(\mathbb{R})$ la multiplication $\times$ est distributive par rapport à l'addition +

2) Sur $\mathcal{P}(E)$ la réunion ∪ est distributive par rapport à l'intersection ∩

2 – Structure d'anneaux

Définition

Soit A un ensemble non vide muni de deux lois de composition internes $*$ et $\top$.

- On dit que $(A,*,\top)$ est un anneau si et seulement si :
  $\begin{cases}(A,*) \text{ est un groupe commutatif}\\ \text{La loi } \top \text{ est associative et distributive par rapport à la loi } *\end{cases}$
- On dit que $(A,*,\top)$ est un anneau commutatif si et seulement si $\begin{cases}(A,*,\top) \text{ est un anneau}\\ \text{La loi } \top \text{ est commutative}\end{cases}$
- On dit que $(A,*,\top)$ est un anneau unitaire si et seulement si $\begin{cases}(A,*) \text{ est un anneau}\\ \text{La loi } \top \text{ afmet un élément neutre}\end{cases}$

Exemples

1) $(\mathbb{Z},+,\times)$; $(\mathbb{Q},+,\times)$; $(\mathbb{R},+,\times)$ *et* $(\mathbb{C},+,\times)$ Sont des anneaux commutatifs unitaires.

2) $(\mathcal{M}_2(\mathbb{R}),+,\times)$ *et* $(\mathcal{M}_3(\mathbb{R}),+,\times)$ sont deux anneaux unitaires non commutatifs

3) $(\mathbb{Z}/_{n\mathbb{Z}},+,\times)$ est un anneau commutatif unitaire $(n\geq 2)$

3 – Règles de calculs dans un anneau

Proposition 1

Soit $(A,*,\top)$ un anneau unitaire d'éléments neutres 0_A et 1_A respectivement dans $(A,*)$ *et* $(A,\top)$. Alors :

- ★ Pour tout $x \in A$: $0_A \top x = x \top 0_A = 0_A$
- ★ Pour tout $(x, y) \in A^2$: $x' \top y = x \top y' = (x * y)'$ où x' et y' sont les symétriques respectifs de x et y dans $(A, *)$
- ★ Pour tout $(x, y) \in A^2$: $x' \top y' = x \top y$ où x' et y' sont les symétriques respectifs de x et y dans $(A, *)$

Notation additive et notation multiplicative dans un anneau

- Dans un anneau la première loi est notée, habituellement, $+$; l'élément neutre de + est noté 0 et le symétrique de x est noté $(-x)$.
- Dans un anneau la deuxième loi est notée, habituellement, $\times$; l'élément neutre de $\times$ est noté 1 et le symétrique de x est noté x^{-1}.

Proposition 2

Soit $(A, +\ \times)$ un anneau unitaire. Alors :

- ★ Pour tout $x \in A$: $0 \times x = x \times 0 = 0$ (0 est l'élément absorbant de la loi $\times$)
- ★ Pour tout $x \in A$: $(-1) \times x = x \times (-1) = -x$
- ★ Pour tout $(x, y) \in A^2$: $(-x) \times y = x \times (-y) = -(x + y)$
- ★ Pour tout $(x, y) \in A^2$: $(-x) \times (-y) = x \times y$

4 – Diviseurs de zéro dans un anneau - Anneau intègre

Définition 1

Soit $(A, +\ \times)$ un anneau et soit $a \in A - \{0_A\}$.

On dit que a est un diviseur de zéro dans l'anneau $(A, +\ \times)$ si et seulement s'il existe $b \in A - \{0_A\}$ tel que :

$$a \times b = 0_A \quad ou \quad b \times a = 0_A$$

Exemples

1) Dans l'anneau $(\mathbb{Z}/_{10\mathbb{Z}}, +, \times)$ on a $\overline{2} \neq \overline{0}$ et $\overline{5} \neq \overline{0}$ et $\overline{2} \times \overline{5} = \overline{0}$. Donc $\overline{2}$ et $\overline{5}$ sont des diviseurs de zéro dans $(\mathbb{Z}/_{10\mathbb{Z}}, +, \times)$

2) Dans l'anneau $(\mathcal{M}_2(\mathbb{R}), +, \times)$, la matrice $\begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix}$ est un diviseur de zéro car $\begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et on a :

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Définition 2

On dit qu'un anneau $(A, +\ \times)$ est intègre si et seulement si : $\begin{cases} A \neq \{0_A\} \\ n'admet aucun\ diviseur\ de\ zéro \end{cases}$

Autrement dit : $(A, +\ \times)$ est intègre $\Leftrightarrow$ $[(\forall (a, b) \in A^2);\ a \times b = 0_A \implies (a = 0_A\ ou\ b = 0_A)]$

Exemples

1) $(\mathbb{Z}, +, \times)$; $(\mathbb{Q}, +, \times)$; $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux intègres

2) Les anneaux $(\mathcal{M}_2(\mathbb{R}), +, \times)$, $(\mathcal{M}_3(\mathbb{R}), +, \times)$ et $(\mathbb{Z}/_{10\mathbb{Z}}, +, \times)$ ne sont pas intègres

Proposition

Soit $(A, +\ \times)$ un anneau unitaire et soit $a \in A - \{0_A\}$.

Si a est inversible dans $(A, \times)$, alors a n'est pas un diviseur de zéro dans l'anneau $(A, +\ \times)$.

Remarque

Si tout élément de $A - \{0_A\}$ est inversible dans $(A, \times)$, alors l'anneau $(A, +\ \times)$ est intègre

Proposition 2

Soit $M = \begin{pmatrix} a & d \\ b & c \end{pmatrix}$ une matrice de $(\mathcal{M}_2(\mathbb{R}), +, \times)$.

- ★ Le déterminant de la matrice $M = \begin{pmatrix} a & d \\ b & c \end{pmatrix}$ est le nombre réel : $\det M = \begin{vmatrix} a & d \\ b & c \end{vmatrix} = ac - bd$
- ★ La matrice $M = \begin{pmatrix} a & d \\ b & c \end{pmatrix}$ est inversible dans $(\mathcal{M}_2(\mathbb{R}), +, \times)$ si et seulement si $detM \neq 0$
- ★ Si la matrice $M = \begin{pmatrix} a & d \\ b & c \end{pmatrix}$ est inversible alors sa matrice inverse est donnée par : $M^{-1} = \frac{1}{detM} \begin{pmatrix} c & -b \\ -d & a \end{pmatrix}$

Exemple

Soit $A=\begin{pmatrix}2 & 1\\5 & 3\end{pmatrix}$. Montrer que A est inversible et calculer sa matrice inverse A^{-1}.

En effet, A est inversible car $detA = 2\times 3 - 5\times 1 = 6-5 = 1 \neq 0$.

Et on a $A^{-1} = \frac{1}{detA}\begin{pmatrix}3 & -5\\-1 & 2\end{pmatrix} = \begin{pmatrix}3 & -5\\-1 & 2\end{pmatrix}$.

VII – Corps

Définition

- On dit que $(K,+,\times)$ est un corps si et seulement si : $\begin{cases} K \neq \{0_K\} \\ (K,+,\times) \text{ est un anneau unitaire} \\ (\forall x \in K-\{0_K\}) : x \text{ est inversible dans } (K,\times) \end{cases}$
- Si en plus la loi $\times$ est commutative, on dit que $(K,+,\times)$ est un corps commutatif.

Exemples

1) $(\mathbb{Q},+,\times)$; $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps commutatifs.

2) $(\mathbb{Z},+,\times)$, $(\mathcal{M}_2(\mathbb{R}),+,\times)$ et $(\mathcal{M}_3(\mathbb{R}),+,\times)$ ne sont pas des corps mais seulement des anneaux unitaires commutatifs.

Proposition

Soit $(K,+,\times)$ un ensemble non vide et muni de deux lois de composition internes $+$ et $\times$.

- ★ $(K,+,\times)$ est un corps $\Leftrightarrow \begin{cases} (K,+) \text{ est un groupe commutatif} \\ (K-\{0_K\},\times) \text{ est un groupe} \\ \text{La loi } \times \text{ est distributive par rapport à la loi } + \end{cases}$
- ★ $(K,+,\times)$ est un corps commutatif $\Leftrightarrow \begin{cases} (K,+,\times) \text{ est un corps} \\ \text{La loi } \times \text{ est commutative dans K} \end{cases}$

Remarque

La loi $\times$ est distributive par rapport à la loi $+$ si et seulement si :

$$(\forall (a,b,c)\in K^3, a\times(b+c) = a\times b + a\times c \ et\ (b+c)\times a = b\times a + c\times a$$

Proposition 2

Soit $(K,+,\times)$ un corps. Alors :

- ★ Tout élément de $K-\{0_K\}$ est régulier pour la loi $\times$

  Autrement dit : $(\forall a\epsilon K-\{0_K\})(\forall (x,y)\epsilon K^2), [a\times x = a\times y \implies x = y]\ et\ [x\times a = y\times a \implies x=y]$
- ★ $(K,+,\times)$ est un anneau unitaire et intègre Mais la réciproque est fausse
- ★ $(\forall a \in K-\{0_K\})(\forall x\in K) : [a\times x = b \Leftrightarrow x = a^{-1}\times b]\ et\ [x\times a = b \Leftrightarrow x = b\times a^{-1}]$

Exercice

On définit dans $\mathbb{R}^2$ deux lois de composition internes $+$ et $\times$ par :

$(\forall(a,b)\epsilon\mathbb{R}^2)\big((\forall(a',b')\epsilon\mathbb{R}^2) : (a,b)+(a'+b') = (a+a',b+b')\big)$ et $(a,b)\text{ɽ}(a',b') = (aa'-bb', ab'+a'b)$

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