Chapitre 4

Structures Algébriques

4.1 Loi de composition interne

Définition 4.1 *Soit E un ensemble.*
On appelle loi de composition interne (L.C.I) sur E, toute application de $E \times E$ dans E.
Exemple 4.1
- *Les lois de composition définies par l'addition et la multiplication sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des lois internes.*
- *Soit E un ensemble quelconque. Soient $X, Y \in P(E)$, la loi de composition $(X, Y) \to X \cup Y$ est une loi interne sur $P(E)$.*

4.1.1 Partie stable

Définition 4.2 *Soit $*$ une loi de composition interne dans un ensemble E.*
On dit que la loi $*$ est stable par rapport l'ensemble $F \subset E$ si

$$\forall x, y \in F, \quad x * y \in F.$$

4.1.2 Propriétés d'une loi de composition interne

Soient $*$ et Δ deux lois de composition interne dans un ensemble E.

1. *La loi $*$ est dite associative si et seulement si :*

$$\forall x, y, z \in E, \quad (x * y) * z = x * (y * z)$$

2. *La loi $*$ est dite commutative si et seulement si :*

$$\forall x, y \in E, \quad x * y = y * x$$

3. *La loi $*$ admet sur E un élément neutre (noté e), si et seulement si :*

$$\exists e \in E, \forall x \in E, \quad x * e = e * x = x$$

L'élément neutre, lorsqu'il existe, est unique. En effet, supposons que e' est un autre élément neutre pour la loi $*$, alors $e' = e' * e = e * e' = e$.

4. *L'élément $x \in E$ admet un élément symétrique, noté, x' si la loi $*$ admet un élément neutre e et si*

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

Le symétrique x' de $x \in E$ est unique pour la loi $*$. En effet, soit x'' un deuxième élément symétrique de x. En utilisant l'associativité de la loi $*$, on obtient

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

5. *$*$ est distributive par rapport à Δ, si et seulement si :*

$$\forall x, y, z \in E, \quad \begin{cases} x * (y \Delta z) = (x * y) \, \Delta \, (x * z) \\ \\ (y \Delta z) * x = (y * x) \, \Delta \, (z * x) \end{cases}$$

6. *On dit que l'élément a est régulier si*

$$\forall x, y \in E, \quad \begin{cases} x * a = y * a \Rightarrow x = y \\ \\ \text{et} \\ \\ a * x = a * y \Rightarrow x = y \end{cases}$$

Proposition 4.1
Soit $\bigstar$ une loi de composition interne dans un ensemble E, associative et admettant un élément neutre e, alors
– *si a et b sont deux éléments inversibles (symétrisables), alors $(a \bigstar b)$ est inversible et on a :*

$$(a \bigstar b)^{-1} = b^{-1} \bigstar a^{-1}$$

– *Tout élément symétrisable dans $(E, \bigstar)$ est régulier.*

Preuve
1. Soient $a, b \in E$ deux éléments inversibles, alors

$$(a \bigstar b) \bigstar (b^{-1} \bigstar a^{-1}) = a \bigstar (b \bigstar b^{-1}) \bigstar a^{-1}$$

$$= a \bigstar e \bigstar a^{-1}$$

$$= a \bigstar a^{-1}$$

$$= e$$

De la même manière on montre que

$$(b^{-1} \bigstar a^{-1}) \bigstar (a \bigstar b) = e$$

d'où on déduit que $(a \bigstar b)$ est inversible et que

$$(a \bigstar b)^{-1} = b^{-1} \bigstar a^{-1}$$

2. Soit $x \in E$ un élément symétrisable dans E, alors x^{-1} existe et pour tous a et b dans E, on a :

$$a\bigstar x = b\bigstar x \Rightarrow (a\bigstar x)\bigstar x^{-1} = (b\bigstar x)\bigstar x^{-1}$$

$$\Rightarrow a\bigstar (x\bigstar x^{-1}) = b\bigstar (x\bigstar x^{-1})$$

$$\Rightarrow a\bigstar e = b\bigstar e$$

$$\Rightarrow a = b$$

Ce qui montre que x est régulier à droite de $\bigstar$.
De la même manière on montre que x est régulier à gauche de $\bigstar$.

4.2 Groupes

Définition 4.3 *Soit G un ensemble muni d'une loi $*$. On dit que $(G, *)$ est un groupe si et seulement si*
– *$*$ est interne dans G.*
– *$*$ est associative.*
– *$*$ admet un élément neutre dans G.*
– *Tout élément de G admet un symétrique pour la loi $*$.*
Et si de plus $*$ est commutative, on dit que G est un groupe abélien (ou commutatif).
Exemple 4.2
Soit $E =]-1, 1[$. On définit sur E la loi $*$ par

$$\forall a, b \in E,\ a * b = \tfrac{a+b}{1+ab}$$

Montrer que $(E, *)$ est un groupe abélien.
1. Montrer que $*$ est interne, c'est à dire

$$\forall a, b \in E,\ a * b \in E.$$

Soient $a, b \in E$, on a :

$$a, b \in E \Rightarrow |ab| < 1$$

$$\Rightarrow 1 + ab > 0$$

Donc,

$$a * b \in E \Leftrightarrow -1 < \tfrac{a+b}{1+ab} < 1$$

$$\Leftrightarrow \left|\tfrac{a+b}{1+ab}\right| < 1$$

$$\Leftrightarrow |a + b| < |1 + ab| = 1 + ab$$

$$\Leftrightarrow |a + b| - 1 - ab < 0$$

Premier cas : si $a+b \leq 0$, alors

$$|a+b|-1-ab = -a-b-1-ab$$

$$= -a(1+b)-(1+b)$$

$$= -(1+a)(1+b) < 0$$

Deuxième cas : si $a+b \geq 0$, alors

$$|a+b|-1-ab = a+b-1-ab$$

$$= a(1-b)-(1-b)$$

$$= -(1-a)(1-b) < 0$$

Dans les deux cas, on déduit que la loi $*$ est interne dans E.
2. La loi $*$ est commutative, c'est à dire

$$\forall a, b \in E,\ a * b = b * a.$$

Soient $a, b \in E$, on a :

$$a * b = \tfrac{a+b}{1+ab} = \tfrac{b+a}{1+ba} = b * a$$

donc, $*$ est commutative.
3. La loi $*$ est associative, c'est à dire

$$\forall a, b, c \in E,\ a * (b * c) = (a * b) * c.$$

Soient $a, b, c \in E$, on a :

$$a * (b * c) = \ a * \tfrac{b+c}{1+bc}$$

$$= \frac{a+\frac{b+c}{1+bc}}{1+a\frac{b+c}{1+bc}}$$

$$= \left(\tfrac{a+abc+b+c}{1+bc}\right) \times \left(\tfrac{1+bc}{1+bc+ab+ac}\right)$$

$$= \tfrac{a+b+c+abc}{1+bc+ab+ac},$$

et

$$(a * b) * c = \tfrac{a+b}{1+ab} * c$$

$$= \frac{\frac{a+b}{1+ab}+c}{1+\frac{a+b}{1+ab}c}$$

$$= \left(\tfrac{a+b+c+abc}{1+ab}\right) \times \left(\tfrac{1+ab}{1+ab+ac+bc}\right)$$

$$= \tfrac{a+b+c+abc}{1+ab+ac+bc}.$$

4. La loi $*$ est admet un élément neutre, c'est à dire

$$\exists e \in E, \forall a \in E,\ a * e = e * a = a.$$

Soit $a \in E$, on cherche un élément e dans E tel que $a * e = e * a = a$.
On a :

$$a * e = a \Leftrightarrow \tfrac{a+e}{1+ae} = a$$

$$\Leftrightarrow a + e = a + a^2 e$$

$$\Leftrightarrow e\,(1 - a^2) = 0$$

$$\Rightarrow e = 0, \qquad car\ \ |a| < 1.$$

Comme la loi $*$ est commutative, alors

$$0 * a = a * 0 = a,$$

donc, $*$ admet un élément neutre $e = 0$.
5. Chaque élément de E admet un symétrique dans E, c'est à dire

$$\forall a \in E,\ \exists a' \in E,\ a * a' = a' * a = e.$$

Soit $a \in E$, on cherche un élément a' dans E tel que $a * a' = a' * a = e$.
On a :

$$a * a' = e \Leftrightarrow \tfrac{a+a'}{1+aa'} = 0$$

$$\Leftrightarrow a + a' = 0,$$

$$\Leftrightarrow a' = -a \in E.$$

Comme la loi $*$ est commutative, alors

$$a' * a = a * a' = 0,$$

donc, chaque élément a de E admet un symétrique $a' = -a$ dans E.
Finalement, $(E, *)$ est un groupe abélien.

4.2.1 Sous-groupe

Définition 4.4
Soit $(E, *)$ un groupe, on appelle sous groupe de $(E, *)$ tout sous ensemble non vide F de E tel que la restriction de $*$ à F en fait un groupe.
Proposition 4.2 *Soient $(E, *)$ un groupe d'élément neutre e et F un sous ensemble de E. On dit que F est un sous groupe de E si et seulement si*
– (i)

$$e \in F$$

– (ii)

$$\forall x, y \in F, \quad x * y \in F$$

– (iii)

$$\forall x \in F, \quad x^{-1} \in F$$

Exemple 4.3

1. *Soit* $(E, *)$ *un groupe d'élément neutre* e*. Alors,* $F_1 = \{e\}$ *et* $F_2 = E$ *sont des sous groupes de* E*.*

2. *L'ensemble*

$$n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}, \quad avec \quad n \in \mathbb{N}$$

est un sous groupe de $(\mathbb{Z}, +)$

Proposition 4.3

Soient $(E, *)$ *un groupe et* F *un sous ensemble de* E*.*
On dit que F *est un sous groupe de* E *si et seulement si*

– (i)

$$F \neq \emptyset$$

– (ii)

$$\forall x, y \in F, \quad x * y^{-1} \in F$$

Preuve

(i) ($\Rightarrow$) Soit F un sous groupe de $(E, *)$, alors

– $*$ a un élémnt neutre dans F, donc $F \neq \emptyset$.

– Soient $x, y \in F$, comme F muni de la restriction de $*$ est un groupe alors y^{-1} existe dans F et comme F est stable par rapport à $*$ on déduit que $x * y^{-1} \in F$.

(ii) ($\Leftarrow$) Soit F un sous ensemble de E tel que

$$\begin{cases} F \neq \emptyset \\ \\ \forall x, y \in F, \quad x * y^{-1} \in F \end{cases}$$

Montrons que F muni de la restriction de $*$ est un groupe.

(1) Comme $F \neq \emptyset$ alors il existe $a \in F$ et d'après la deuxième hypothèse

$$e = a * a^{-1} \in F,$$

ce qui montre que la restriction de $*$ admet un élément neutre e dans F.

(2) Soit $x \in F$, c omme $e \in F$ alors d'après la deuxième hypothèse on aura

$$x^{-1} = e * x^{-1} \in F,$$

ce qui montre que tout élément x de F est inversible dans F par rapport à la restriction de $*$ à F.

(3) La restriction de $*$ à F est une loi de composition interne, car pour tous x et y dans F, d'après (2) on a

$$y^{-1} \in F$$

et en utilisant la deuxième hypothèse on déduit que

$$x * y = x * (y^{-1})^{-1} \in F$$

(4) La restriction de $*$ à F est associative, car $*$ est associative dans E.

Proposition 4.4

Soient $(E, *)$ un groupe d'élément neutre e et F_1, F_2 deux sous groupes de E. Alors $F_1 \cap F_2$ est un sous groupe de E.

Preuve

Notons $F = F_1 \cap F_2$. On a :

(i) $F \neq \emptyset$, car $e \in F_1, F_2$.

(ii) Soient $x, y \in F$

$$x, y \in F \Rightarrow x, y \in F_1 \cap F_2$$

$$\Rightarrow (x, y \in F_1) \text{ et } (x, y \in F_2)$$

$$\Rightarrow (x * y \in F_1) \text{ et } (x * y \in F_2)$$

$$\Rightarrow (x * y \in F_1 \cap F_2)$$

$$\Rightarrow x * y \in F$$

(iii) Soient $x \in F$

$$x \in F \Rightarrow x \in F_1 \cap F_2$$

$$\Rightarrow (x \in F_1) \text{ et } (x \in F_2)$$

$$\Rightarrow (x^{-1} \in F_1) \text{ et } (x^{-1} \in F_2)$$

$$\Rightarrow (x^{-1} \in F_1 \cap F_2)$$

$$\Rightarrow x^{-1} \in F$$

De (i), (ii) et (iii) on déduit que $F_1 \cap F_2$ *est un sous groupe de* E.

Remarque *En général, la réunion de sous groupes n'est pas un sous groupe.*

Exemple 4.4

On considère le groupe $(\mathbb{Z}, +)$. On a $(2\mathbb{Z}, +)$ et $(3\mathbb{Z}, +)$ sont deux sous groupes de $(\mathbb{Z}, +)$ mais $(2\mathbb{Z} \cup 3\mathbb{Z}, +)$ n'est pas un sous groupe de $(\mathbb{Z}, +)$, car

$$2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z} \text{ et } 2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$$

4.2.2 Groupe quotient

Soient $(E, *)$ un groupe et F un sous groupe de E. On définit une relation binaire $\Re$ sur E par :

$$\forall a, b \in E, \quad a \ \Re \ b \Leftrightarrow a * b^{-1} \in F.$$

$\Re$ est une relation d'équivalence sur E.

En effet, pour $a, b, c \in E$ on a :
(i) $\Re$ est réflexive, car

$$a * a^{-1} = e \in F \ , \quad car \ F \ \ est \ un \ sous \ groupe \ de \ E,$$

donc, $a \ \Re \ a$.
(ii) $\Re$ est symétrique, car

$$a \ \Re \ b \Rightarrow a * b^{-1} \in F$$

$$\Rightarrow (a * b^{-1})^{-1} \in F$$

$$\Rightarrow b * a^{-1} \in F$$

$$\Rightarrow b \ \Re \ a$$

(iii) $\Re$ est transitive, car

$$(a \ \Re \ b) \ et \ (b \ \Re \ c) \ \Rightarrow (a * b^{-1} \in F) \ et \ (b * c^{-1} \in F)$$

$$\Rightarrow (a * b^{-1}) * (b * c^{-1}) \in F \ , \ \ car \ F \ \ est \ un \ sous \ groupe \ de \ E$$

$$\Rightarrow a * (b^{-1} * b) * c^{-1} \in F \ , \quad car \ \ * \ \ est \ associative,$$

$$\Rightarrow a * c^{-1} \in F$$

$$\Rightarrow a \ \Re \ c$$

On note E/F l'ensemble quotient $E/\Re$. On définit sur $E/F \times E/F$ l'opération $\oplus$ par :

$$\forall \left(\dot{a}, \dot{b}\right) \in E/F \times E/F, \ \dot{a} \oplus \dot{b} \ = \ \overline{\dot{a * b}}$$

Proposition 4.5
Si $(E, *)$ est un groupe abélien, alors $(E/F, \oplus)$ est un groupe abélien, appelé groupe quotient de E par F.
Preuve
(1) $\oplus$ est une loi de composition interne,
On montre que $*$ est une application de $E/F \times E/F$ dans E/F.
Soient $\dot{a}, \dot{b}, \dot{c}, \dot{d} \in E/F$, montrons que

$$\left(\dot{a}, \dot{b}\right) = \left(\dot{c}, \dot{d}\right) \Rightarrow \ \dot{a} \oplus \dot{b} \ = \ \dot{c} \oplus \dot{d}$$

Supposons que $\left(\dot{a},\dot{b}\right)=\left(\dot{c},\dot{d}\right)$, alors : $\forall x\in E$,

$$x\in\ \dot{a}\oplus\dot{b}\ \Leftrightarrow x\in\ \overline{\dot{a*b}}$$

$$\Leftrightarrow x\Re\left(a*b\right)$$

$$\Leftrightarrow x*\left(a*b\right)^{-1}\in F$$

$$\Leftrightarrow x*b^{-1}*a^{-1}\in F$$

$$\Rightarrow\left(x*b^{-1}*a^{-1}\right)*\left(a*c^{-1}\right)\in F,\ car\ F\ est\ un\ sous\ groupe$$

$$\Rightarrow\left(x*b^{-1}\right)*\left(a^{-1}*a\right)*c^{-1}\in F,\ car\ *\ est\ associative$$

$$\Rightarrow\left(x*b^{-1}\right)*c^{-1}\in F$$

$$\Rightarrow\left(\left(x*b^{-1}\right)*c^{-1}\right)*\left(b*d^{-1}\right)\in F,\ car\ F\ est\ un\ sous\ groupe$$

$$\Rightarrow x*\left(b^{-1}*b\right)*c^{-1}*d^{-1}\in F,\ car\ *\ est\ associative\ et\ commtative$$

$$\Rightarrow x*c^{-1}*d^{-1}\in F$$

$$\Rightarrow x*\left(d*c\right)^{-1}\in F$$

$$\Rightarrow x\Re\left(d*c\right)$$

$$\Rightarrow x\Re\left(c*d\right),\ car\ *\ est\ commtative$$

$$\Rightarrow x\in\ \overline{\dot{c*d}}$$

$$\Rightarrow x\in\ \dot{c}\oplus\dot{d}$$

donc

$$\dot{a}\oplus\dot{b}\ \subset\ \dot{c}\oplus\dot{d},$$

et de la même manière on montre que

$$\dot{c}\oplus\dot{d}\ \subset\ \dot{a}\oplus\dot{b},$$

par suite :

$$\dot{a}\oplus\dot{b}\ =\ \dot{c}\oplus\dot{d},$$

ce qui montre que la loi $\oplus$ est interne dans E/F.

(2) $\oplus$ est associative, car $\forall \dot{a}, \dot{b}, \dot{c} \in E/F$, on a

$$\begin{aligned}
\dot{a} \oplus \left(\dot{b} \oplus \dot{c}\right) &= \dot{a} \oplus \left(\overline{\dot{b} \dot{*} c}\right) \\
&= \overline{a \dot{*} (\dot{b} \dot{*} c)} \\
&= \overline{(a \dot{*} b) \dot{*} c} \quad , \textit{ car } * \textit{ est associative} \\
&= \left(\overline{\dot{a} \dot{*} b}\right) \oplus \dot{c} \\
&= \left(\dot{a} \oplus \dot{b}\right) \oplus \dot{c}
\end{aligned}$$

(3) $\oplus$ admet un élément neutre,
Si e est l'élément neutre de $*$, alors $\dot{e}$ est l'élément neutre de $\oplus$, car $\forall \dot{a} \in E/F$, on a

$$\dot{a} \oplus \dot{e} = \overline{a \dot{*} e} = \dot{a}$$

$$et$$

$$\dot{e} \oplus \dot{a} = \overline{e \dot{*} a} = \dot{a}$$

(4) Tout élément est inversible,
Soit $\dot{a} \in E/F$, alors $(\dot{a})^{-1} = \overline{\dot{a^{-1}}}$

$$\dot{a} \oplus (\dot{a})^{-1} = \overline{a \dot{*} a^{-1}} = \dot{e}$$

$$et$$

$$(\dot{a})^{-1} \oplus \dot{a} = \overline{a^{-1} \dot{*} a} = \dot{e}$$

(5) $\oplus$ est commutative, car $\forall \dot{a}, \dot{b} \in E/F$, on a

$$\begin{aligned}
\dot{a} \oplus \dot{b} &= \overline{\dot{a} \dot{*} b} \\
&= \overline{\dot{b} \dot{*} a}, \quad car \ * \ est \ commutative \\
&= \dot{b} \oplus \dot{a}
\end{aligned}$$

De (1), (2), (3), (4) et (5) on déduit que $(E/F, \oplus)$ est un groupe abélien.

Exemple 4.5

On sait que $n\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$ avec $n \in \mathbb{N}$. Donc $(\mathbb{Z}/_n\mathbb{Z}, \oplus)$ est un groupe quotient.

4.2.3 Groupe des permutations

Définition 4.5 *Soit E un ensemble non vide .*
On appelle permutation de E , toute bijection $\sigma : E \to E$.
Définition 4.6 *Lorsque l'ensemble $E = \{1, 2, 3, ...\}$, on note S_n le groupe des permutations de E.*
S_n est un groupe fini de cardinal $n!$ que l'on appellera le groupe symétrique d'ordre n.
Une permutation $\sigma \in S_n$ se note :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & . & . & . & n \\ \sigma(1) & \sigma(2) & \sigma(3) & . & . & . & \sigma(n) \end{pmatrix}$$

Exemple 4.6
Supposons que $E = \{1.2, 3, 4\}$, soient σ, μ deux permutation de S_4 telles que :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

et

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

On a :

$$\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2, \sigma(4) = 4,$$

$$\mu(1) = 4, \mu(2) = 1, \mu(3) = 3, \mu(4) = 2,$$

On peut calculer $\sigma \circ \mu$ comme suit :

$$\sigma \circ \mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \\ \sigma \circ \mu(1) & \sigma \circ \mu(1) & \sigma \circ \mu(3) & \sigma \circ \mu(4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \\ \sigma(\mu(1)) & \sigma(\mu(1)) & \sigma(\mu(3)) & \sigma(\mu(4)) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \\ \sigma(4) & \sigma(1) & \sigma(3) & \sigma(2) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Exemple 4.7 *Déterminer les permutations de l'ensemble $E = \{1.2, 3\}$.*

Dans ce cas, on a : $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ tel que :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 1 & 2 & 3 \end{pmatrix} = Id_3, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 1 & 3 & 2 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 2 & 1 \end{pmatrix}, \qquad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 2 & 3 & 1 \end{pmatrix}, \qquad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 1 & 2 \end{pmatrix}$$

$(S_3, \circ)$ est un groupe non commutatif.

4.2.4 Homomorphisme de groupes- isomorphisme de groupes

Soient $(E, *)$ et (G, Δ) deux groupes, avec e et h leurs éléments neutres respectifs.

Définition 4.7

Une application $f : E \to G$ est appelée homomorphisme de groupes de E dans G si :

$$\forall a, b \in E,\ f(a * b) = f(a)\, \Delta f(b)$$

- *Si f est bijective, on dit que f est un isomorphisme (de groupes) de E sur G. On dit alors que E est isomorphe à G, ou que E et G sont isomorphes.*
- *Si $E = G$, on dit que f est un endomorphisme de E, et si de plus f est bijective, on dit que f est un automorphisme (de groupe) de E.*

Exemple 4.8

Soient f et g deux applications telles que :

$$f : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$$

$$x \mapsto e^x$$

et

$$g : (\mathbb{R}^*, \times) \to (\mathbb{R}, +)$$

$$x \mapsto \ln |x|$$

Pour $x, y \in \mathbb{R}$ et $a, b \in \mathbb{R}^*$ on a

$$f(x + y) = e^{x+y}$$

$$= e^x \times e^y$$

$$= f(x) \times f(y)$$

et

$$g(a \times b) = \ln|a \times b|$$

$$= \ln|a| + \ln|b|$$

$$= g(a) + g(b)$$

Alors, f est un homomorphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$ et g est un homomorphisme de groupes de $(\mathbb{R}^*, \times)$ dans $(\mathbb{R}, +)$.

Définition 4.7

Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ).

– *On appelle **noyau** de f l'ensemble*

$$\ker f = f^{-1}(\{h\}) = \{x \in E \ / \ f(x) = h\}$$

– *On appelle **image** de f l'ensemble*

$$\text{Im } f = f(E) = \{f(x) \ / \ x \in E\}$$

Proposition 4.6

Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ). Alors

1.

$$f(e) = h$$

2. $\forall x \in E$,

$$(f(x))^{-1} = f(x^{-1})$$

Preuve

1. On a

$$f(e * e) = f(e) = h \ \Delta \ f(e)$$

et comme f est un homomorphisme on déduit que

$$f(e) \ \Delta \ f(e) = h \ \Delta \ f(e)$$

et comme tous les éléments du groupe (G, Δ) sont réguliers, on dé duit que

$$f(e) = h$$

2. Soit $x \in E$, on a

$$f(x) \ \Delta \ f(x^{-1}) = f(x * x^{-1})$$

$$= f(e)$$

$$= h$$

et

$$f(x^{-1}) \ \Delta \ f(x) \ = f(x^{-1} * x)$$

$$= f(e)$$

$$= h$$

On dé duit que

$$(f(x))^{-1} = f(x^{-1})$$

Proposition 4.7
Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ). Alors
1. L'image d'un sous groupe de E est un sous groupe de F.
2. L'image réciproque d'un sous groupe de F est un sous groupe de E.
Preuve
1. Soit E' un sous groupe de E .
(i) On a $e \in E'$, car E' est un sous groupe de E, donc

$$f(e) \in f(E'),$$

par suite

$$f(E') \neq \emptyset.$$

(ii) Soient $a, b \in f(E')$, alors il existe $x, y \in E'$ tels que $a = f(x)$ et $b = f(y)$, donc

$$a \ \Delta \ b^{-1} = f(x) \ \Delta \ (f(y))^{-1} = f(x) \ \Delta \ f(y^{-1}) = f(x * y^{-1})$$

et comme E' est un sous groupe de E alors $x * y^{-1} \in E'$, par suite

$$a \ \Delta \ b^{-1} = f(x * y^{-1}) \in f(E'),$$

de (i) e t (ii) on déduit que $f(E')$ est un sous groupe de F.
2. Soit F' un sous groupe de F, alors
(i) $f(e) = h$ et comme F' un sous groupe de F, alors

$$h \in F',$$

donc $e \in f^{-1}(F')$.
(ii) Soient $x, y \in f^{-1}(F')$, alors

$$f(x), f(y) \in F',$$

et comme F' estun sous groupe de F, alors

$$f(x)\Delta(f(y))^{-1} \in F' \Leftrightarrow f(x)\Delta f(y^{-1}) \in F'$$

$$\Leftrightarrow f(x * y^{-1}) \in F',$$

ce qui montre que

$$x * y^{-1} \in f^{-1}(F').$$

De (i) et (ii) on déduit que $f^{-1}(F')$ est un sous groupe de E.
Proposition 4.8
Soit $f : E \to F$ un homomorphisme de groupes de $(E, *)$ dans (G, Δ). Alors
1. f est injective si et seulement si $\ker f = \{e\}$.
2. f est surjective si et seulement si $\operatorname{Im} f = F$.
Preuve
Soit $f : E \to F$ un homomorphisme de groupes.

1. ($\Rightarrow$) Supposons que f est injectif.
On a

$$e \in \ker f.$$

Montrons que $\ker f \subset \{e\}$.
Soit $x \in \ker f$, alors $f(x) = h$

$$f(x) = h \Leftrightarrow f(x) = f(e)$$

$$\Rightarrow x = e \text{ , } car \ f \ est \ injectif$$

$$\Rightarrow x \in \{e\}$$

d'où $\ker f \subset \{e\}$.
($\Leftarrow$) Supposons que $\ker f = \{e\}$.
Soient $a, b \in E$,

$$f(a) = f(b) \Rightarrow f(a) \ \Delta \ (f(b))^{-1} = h$$

$$\Rightarrow f(a) \ \Delta \ f(b^{-1}) = h$$

$$\Rightarrow f(a * b^{-1}) \ = h$$

$$\Rightarrow a * b^{-1} \in \ker f$$

$$\Rightarrow a * b^{-1} = e \ \text{ , } car \ \ker f = \{e\}$$

$$\Rightarrow a = b,$$

ce qui montre que f est injectif.
2. La preuve est immédiate, sachant que

$$\operatorname{Im} f = f(E)$$

4.3 Anneaux

Définition 4.8
On appelle anneau, tout ensemble A muni de deux lois de composition internes $+$ et $\bullet$ telles que :

1. $(A, +)$ *est un groupe abélien (on notera 0_A l'élément neutre de $+$).*
2. $\bullet$ *est associative*
3. $\bullet$ *est distributive par rapport à $+$.*

Si de plus $\bullet$ est commutative, on dit que $(A, +, \bullet)$ est un anneau commutatif.
Si $\bullet$ admet un élément neutre, l'anneau est dit unitaire.
On note 0_A l'élément neutre de $+$ et *1_A l'élément neutre de $\bullet$.*

On note $-x$ le symétriqe de x par la loi $+$ (appelé opposé de x) et x^{-1} le symétriqe de x par la loi $\bullet$ (appelé inverse de x).

Exemple 4.9

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

4.3.1 Règles de calculs dans un anneau

Soit $(A, +, \bullet)$ un anneau, alors on a les règles de calculs suivantes :
Pour tous x, y et $z \in A$,

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

Preuve

1. Soit $x \in A$, alors

$$0_A \bullet x = (0_A + 0_A) \bullet x = (0_A \bullet x) + (0_A \bullet x)$$

car $\bullet$ est distributive par rapport à $+$
comme tous les éléments de A sont symétrisables, on déduit que

$$0_A \bullet x = 0_A.$$

De la même manière on montre que

$$x \bullet 0_A = 0_A.$$

2. Soient $x, y \in A$ et montrons que $x \bullet (-y)$ est le symétrique de $(x \bullet y)$. On a :

$$(x \bullet (-y)) + (x \bullet y) = x \bullet (-y + y) = x \bullet 0_A = 0_A$$

comme $+$ est commutative on déduit que

$$(x \bullet (-y)) = -(x \bullet y).$$

De la même manière on montre que

$$(-x) \bullet y = -(x \bullet y).$$

La preuve des propriétés **3** et **4** utilise essentiellement la distributivité de la loi $\bullet$ par rapport à $+$.

4.3.2 Anneaux intègres

Définition 4.9
Soit $(A, +, \bullet)$ un anneau commutatif.
– *On dit que $y \in A^* = A \setminus \{0_A\}$ divise $x \in A$, ou que y est un diviseur de x ou que x est divisible par y, si*

$$\exists z \in A^*,\ x = y \bullet z.$$

– *Si 0_A ne possède pas de diviseur dans A, on dit que $(A, +, \bullet)$ est un anneau intègre ou un anneau d'intégrité.*
– *$(A, +, \bullet)$ est un anneau intègre si*

$$\forall x, y \in A,\ (\ x \bullet y = 0_A \Rightarrow x = 0_A \text{ ou } y = 0_A)$$

– *Ou encore, par contraposition, si*

$$\forall x, y \in A,\ (\ x \neq 0_A \text{ et } y \neq 0_A \Rightarrow\ x \bullet y \neq 0_A)$$

4.3.3 Sous anneaux

Définition 4.10
On appelle sous anneau de $(A, +, \bullet)$, tout sous ensemble A' de A tel que muni des restrictions des lois $+$ et $\bullet$ est anneau.
Si A est un anneau unitaire et $1_A \in A'$, on dit que A' est sous anneau unitaire.
Proposition 4.9
Un sous ensemble A'de A est un sous anneau si et seulement si :
1. $A' \neq \emptyset$,
2. $\forall x, y \in A', (x - y) \in A'$
3. $\forall x, y \in A', (x \bullet y) \in A'$.

Exemple 4.10
$(\mathbb{Z}, +, \times)$ est un sous anneau de $(\mathbb{R}, +, \times)$.

4.3.4 Homomorphisme d'anneaux

Soient $(A, +, \bullet)$ et $(B, \oplus, \otimes)$ deux anneaux et $f : A- \rightarrow B$.
Définition 4.11 *On dit que f est un homomorphisme d'anneaux si :*

$$\forall x, y \in A,\ f(x + y) = f(x) \oplus f(y) \quad et \quad f(x \bullet y) = f(x) \otimes f(y)$$

– *Si $A = B$ on dit que f est un endomorphisme d'anneau de A.*
– *Si f est bijective, on dit que f est un isomorphisme d'anneaux*
– *Si f est bijective et $A = B$, on dit que f est un automorphisme d'anneaux.*

4.3.5 Idéaux

Soit $(A, +, \bullet)$ un anneau.

Définition 4.12 *On appelle idéal à droite (respectivement à gauche) de l'anneau A, tout ensemble $I \subset A$ tel que*

1. *I est un sous groupe de $(A, +)$,*
2. *$\forall x \in A$, $(\forall y \in I)$, $x \bullet y \in I$ (respectivement $y \bullet x \in I$).*

Si I est idéal à droite et à gauche de A, on dit que I est un idéal bilatère de A.
Si l'anneau A est commutatif, tout idéal de A est bilatère, et dans ce cas on parle seulement d'Idéal sans préciser s'il l'est à droite, à gauche ou bilatère.

Exemple 4.11
– *Soit $(A, +, \bullet)$ un anneau, alors $I = \{O_A\}$ est un idéal bilatère de A.*
– *Dans l'anneau commutatif $(Z, +, \times)$, $n\mathbb{Z}$ est un idéal.*

4.3.6 Anneaux quotients

Soient $(A, +, \bullet)$ un anneau commutatif et I un idéal de A. On considère le groupe quotient $(A/I, \oplus)$, et on définit l'application $\otimes$ de $A/I \times A/I$ dans A/I par

$$\forall \left(\dot{a}, \dot{b}\right) \in A/I \times A/I,\ \dot{a} \otimes \dot{b} \ = \ \dot{\overline{a \bullet b}}$$

$(A/I, \oplus, \otimes)$ est anneau commutatif. Si de plus A est un anneau unitaire, alors $(A/I, \oplus, \otimes)$ est un anneau unitaire et $\dot{\overline{1_A}}$ est son élément unité.

4.4 Corps

Définition 4.13
On dit qu'un anneau unitaire $(\mathbb{k}, +, \bullet)$ est un corps si tout élément non nul de $\mathbb{k}$ est inversible. Si de plus $\bullet$ est commutative, on dit que $\mathbb{k}$ est un corps commutatif.

Proposition 4.10
Tout corps est un anneau intègre.

Exemple 4.12
– *$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps commutatifs pour les lois usuelles $+, \times$.*
– *$(\mathbb{Z}, +, \times)$ n'est pas un corps car les éléments de $\mathbb{Z}$ n'ont pas d'inverses pour la loi $\times$.*

4.4.1 Sous corps

Définition 4.14
On appelle sous corps, d'un corps $(\mathbb{k}, +, \bullet)$, tout sous ensemble $\mathbb{k}'$ de $\mathbb{k}$ tel que, muni des restrictions des lois $+$ et $\bullet$ est un corps.

Proposition 4.11
$\mathbb{k}' \subset \mathbb{k}$ est un sous corps de $(\mathbb{k}, +, \bullet)$ si et seulement si

1. $\mathbb{k}' \neq \emptyset$

2. $\forall a, b \in \Bbbk'$, $a - b$ et $a \bullet b^{-1} \in \Bbbk'$.

Exemple 4.13
– $\mathbb{Q}$ est un sous corps de $\mathbb{R}$ pour les lois usuelles.
– $\mathbb{R}$ est un sous corps de $\mathbb{C}$ pour les lois usuelles.
Proposition 4.12
$\mathbb{Z}/_n\mathbb{Z}$ est un corps si n est premier

4.5 Exercices

Exercice 1
On munit $\mathbb{R}^2$ de la loi $\bigstar$ définie par :

$$\forall\,(x,y)\,,(x',y') \in \mathbb{R}^2, \quad (x,y) \bigstar (x',y') = \left(x + x', ye^{x'} + y'e^{-x}\right)$$

1. Montrer que $(\mathbb{R}^2, \bigstar)$ est un groupe.
2. $(\mathbb{R}^2, \bigstar)$ est-il abélien ?
Solution
1. Montrer que $(\mathbb{R}^2, \bigstar)$ est un groupe :
(1). Montrer que $\bigstar$ est interne, c'est à dire

$$\forall\,(x,y)\,,(x',y') \in \mathbb{R}^2, (x,y) \bigstar (x',y') \in \mathbb{R}^2.$$

Soient $(x,y)\,,(x',y') \in \mathbb{R}^2$, on a :

$$x + x' \in \mathbb{R}$$

$$et$$

$$ye^{x'} + y'e^{-x} \in \mathbb{R}$$

Donc,

$$\left(x + x', ye^{x'} + y'e^{-x}\right) \in \mathbb{R}^2$$

On déduit que la loi $\bigstar$ est interne dans $\mathbb{R}^2$.
(2). La loi $\bigstar$ est associative, c'est à dire

$$\forall\,(x,y)\,,(x',y')\,,\left(x'',y''\right) \in \mathbb{R}^2, \;\; (x,y) \bigstar \left((x',y') \bigstar \left(x'',y''\right)\right) = ((x,y) \bigstar (x',y')) \bigstar \left(x'',y''\right).$$

Soient $(x,y)\,,(x',y')\,,\left(x'',y''\right) \in \mathbb{R}^2$, on a :

$$(x,y) \bigstar \left((x',y') \bigstar \left(x'',y''\right)\right) = (x,y) \bigstar \left(x' + x'', y'e^{x''} + y''e^{-x'}\right)$$

$$= \left(x + x' + x'', ye^{x'+x''} + \left(y'e^{x''} + y''e^{-x'}\right)e^{-x}\right)$$

$$= \left(x + x' + x'', ye^{x'+x''} + y'e^{-x+x''} + y''e^{-x-x'}\right),$$

et

$$\begin{aligned}((x,y)\bigstar(x',y'))\bigstar\left(x'',y''\right) &= \left(x+x',ye^{x'}+y'e^{-x}\right)\bigstar\left(x'',y''\right)\\ &= \left(x+x'+x'',\left(ye^{x'}+y'e^{-x}\right)e^{x''}+y''e^{-x-x'}\right)\\ &= \left(x+x'+x'',ye^{x'+x''}+y'e^{-x+x''}+y''e^{-x-x'}\right),\end{aligned}$$

et donc on a

$$(x,y)\bigstar\left((x',y')\bigstar\left(x'',y''\right)\right)=((x,y)\bigstar(x',y'))\bigstar\left(x'',y''\right).$$

(3). La loi $\bigstar$ est admet un élément neutre, c'est à dire

$$\exists\,(e_1,e_2)\in\mathbb{R}^2,\forall\,(x,y)\in\mathbb{R}^2,\ \ (x,y)\bigstar(e_1,e_2)=(e_1,e_2)\bigstar(x,y)=(x,y).$$

Soit $(x,y)\in\mathbb{R}^2$, on a

$$\begin{aligned}(x,y)\bigstar(e_1,e_2)=(x,y)&\Leftrightarrow(x+e_1,ye^{e_1}+e_2e^{-x})\\ &\Leftrightarrow\begin{cases}x+e_1=x\\ ye^{e_1}+e_2e^{-x}=y\end{cases}\\ &\Leftrightarrow\begin{cases}e_1=0\\ y+e_2e^{-x}=y\end{cases}\\ &\Rightarrow\begin{cases}e_1=0\\ e_2=0\end{cases}\end{aligned}$$

et

$$\begin{aligned}(e_1,e_2)\bigstar(x,y)=(x,y)&\Leftrightarrow(e_1+x,e_2e^{x}+ye^{-e_1})=(x,y)\\ &\Leftrightarrow\begin{cases}e_1+x=x\\ e_2e^{x}+ye^{-e_1}=y\end{cases}\\ &\Leftrightarrow\begin{cases}e_1=0\\ e_2e^{x}+y=y\end{cases}\\ &\Rightarrow\begin{cases}e_1=0\\ e_2=0\end{cases},\end{aligned}$$

donc, $\bigstar$ admet un élément neutre $(0,0)$.

(4). Chaque élément de $\mathbb{R}^2$ admet un symétrique dans $\mathbb{R}^2$, c'est à dire

$$\forall\,(x,y)\in\mathbb{R}^2,\ \exists\,(a,b)\in\mathbb{R}^2,\ \ (x,y)\bigstar(a,b)=(a,b)\bigstar(x,y)=(0,0)\,.$$

Soit $(x,y)\in\mathbb{R}^2$, on cherche un élément (a,b) dans $\mathbb{R}^2$ tel que $(x,y)\bigstar(a,b)=(a,b)\bigstar(x,y)=(0,0)$.
On a :

$$(x,y)\bigstar(a,b)=(0,0)\Leftrightarrow(x+a,ye^{a}+be^{-x})=(0,0)$$

$$\Leftrightarrow\begin{cases}x+a=0\\ \\ ye^{a}+be^{-x}=0\end{cases},$$

$$\Leftrightarrow\begin{cases}a=-x\\ \\ ye^{-x}+be^{-x}=0\end{cases}.$$

$$\Leftrightarrow\begin{cases}a=-x\\ \\ b=-y\end{cases}$$

et

$$(a,b)\bigstar(x,y)=(0,0)\Leftrightarrow(a+x,be^{x}+ye^{-a})=(0,0)$$

$$\Leftrightarrow\begin{cases}a+x=0\\ \\ be^{x}+ye^{-a}=0\end{cases},$$

$$\Leftrightarrow\begin{cases}a=-x\\ \\ be^{x}+ye^{x}=0\end{cases}.$$

$$\Leftrightarrow\begin{cases}a=-x\\ \\ b=-y\end{cases},$$

donc, chaque élément $(x,y)\in\mathbb{R}^2$ admet un symétrique $(-x,-y)$ dans $\mathbb{R}^2$.
Finalement, $(\mathbb{R}^2,\bigstar)$ est un groupe.
2. $(\mathbb{R}^2,\bigstar)$ est-il abélien ?
C'est à dire la loi $\bigstar$ est-elle commutative ?

$$\forall\,(x,y),(x',y')\in\mathbb{R}^2,\ \ (x,y)\bigstar(x',y')=(x',y')\bigstar(x,y)\,.$$

On a

$$(x,y)\bigstar(x',y')=\left(x+x',ye^{x'}+y'e^{-x}\right)$$

et

$$(x',y')\bigstar(x,y)=\left(x'+x,y'e^{x}+ye^{-x'}\right)$$

Pour $(x, y) = (1, 0)$ et $(x', y') = (0, 1)$ on a :

$$(1, 0) \bigstar (0, 1) = (1, e^{-1})$$

$$(0, 1) \bigstar (1, 0) = (1, e)$$

D'où $(\mathbb{R}^2, \bigstar)$ n'est pas un groupe abélien.

Exercice 2

On considère les permutations suivantes

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

1. Calculer $\sigma_1 \circ \sigma_2$, $\sigma_1 \circ \sigma_3$, $\sigma_2 \circ \sigma_3$, $\sigma_3 \circ \sigma_2$, $\sigma_4 \circ \sigma_4$.

2. $(S_3, \circ)$ *est - il groupe commutatif ?*

Solution

1. $\sigma_1 \circ \sigma_2$

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ \sigma_1 \circ \sigma_2(1) & \sigma_1 \circ \sigma_2(1) & \sigma_1 \circ \sigma_2(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ \sigma_1(\sigma_2(1)) & \sigma_1(\sigma_2(1)) & \sigma_1(\sigma_2(3)) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ \sigma_1(2) & \sigma_1(1) & \sigma_1(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$= \sigma_4$$

De la même manière, on trouve

$$\sigma_1 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_2 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \sigma_1$$

$$\sigma_3 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_4 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_3$$

2. $(S_3, \circ)$ n'est pas un groupe commutatif, car

$$\sigma_2 \circ \sigma_3 \neq \sigma_3 \circ \sigma_2$$

Exercice 3
Soient $(G, *)$ un groupe et H, K deux sous-groupes de G.
Démontrer que :
$H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.
Solution
($\Rightarrow$) En utilisant le raisonnement par l'absurde.
Supposons que $H \cup K$ est un sous-groupe de G et que ni $H \subset K$, ni $K \subset H$.
Soient $x \in H \setminus K$ et $y \in K \setminus H$.
Puisque $H \cup K$ est un groupe et que $x, y \in H \cup K$, on a $x * y \in H \cup K$.
Mais si $x * y \in H$, alors

$$x^{-1} * (x * y) = y \in H, \ \textit{car } H \textit{ est un sous groupe,}$$

ce qui est une contradiction.
On obtient de même une contradiction dans l'autre cas possible $x * y \in K$.

$$(x * y) * y^{-1} = x \in K, \ \textit{car } K \textit{ est un sous groupe.}$$

L'hypothèse de départ est donc fausse, alors d'après l'absurde on déduit que $H \subset K$ ou $K \subset H$.
($\Leftarrow$)Si $H \subset K$, alors $H \cup K = K$ qui est un sous-groupe de G.
De même, si $K \subset H$, $H \cup K = H$ qui est un sous-groupe de G.
Exercice 4
Soit

$$A = \left\{ \tfrac{m}{n}, \ m \in \mathbb{Z}, \ n \textit{ entier naturel impair} \right\}$$

Démontrer que $(A, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?
Solution
1. Démontrons que A est un sous-anneau de $(\mathbb{Q}, +, \times)$.
Soient $x = \frac{m}{n}, y = \frac{p}{q} \in A$, on a :

$$x + (-y) = \tfrac{m}{n} - \tfrac{p}{q} = \tfrac{mq - pn}{nq}$$

et

$$xy = \tfrac{mp}{nq}$$

Comme nq, produit de deux nombres impairs, est impair, et que $A \neq \emptyset$ ($\text{car} 1_{\mathbb{Q}} = 1 \in A$), on déduit que A est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2. Déterminons les inversibles de A.
Soit $x = \frac{m}{n} \in A$ inversible, et soit $y = \frac{p}{q} \in A$ tel que $xy = 1$.

$$xy = 1 \Leftrightarrow \tfrac{m}{n} = \tfrac{p}{q} \Leftrightarrow mq = np$$

En particulier, m est nécessairement impair.
Réciproquement, si $x = \frac{m}{n}$ avec m impair, alors $y = \frac{n}{m} \in A$ (si $m < 0$, il suffit d'écrire $y = \frac{-n}{-m}$) et $xy = 1$.
Donc, les inversibles de A sont les éléments $\frac{m}{n}$ avec $m \in \mathbb{Z}, n \in \mathbb{N}^*$ et m, n impairs.

Exercice 5

Soient $+$ et $\bullet$ deux lois de composition internes dans $\mathbb{R}^2$ définies par :

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b)+(c,d) = (a+c, b+d)$$

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b)\bullet(c,d) = (ac-bd, ad+cb)$$

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

Solution

1. $(\mathbb{R}^2, +)$ est un groupe abélien

(a). $+$ est commutative

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b)+(c,d) = (c,d)+(a,b)$$

Soient $(a,b),(c,d) \in \mathbb{R}^2$, on a

$$\begin{aligned}(a,b)+(c,d) &= (a+c, b+d)\\ &= (c+a, d+b)\\ &= (c,d)+(a,b)\end{aligned}$$

(b). $+$ est associaive,

$$\forall (a,b),(c,d),(e,f) \in \mathbb{R}^2, \quad (a,b)+((c,d)+(e,f)) = ((a,b)+(c,d))+(e,f)$$

Soient $(a,b),(c,d),(e,f) \in \mathbb{R}^2$, on a

$$\begin{aligned}(a,b)+((c,d)+(e,f)) &= (a,b)+(c+e, d+f)\\ &= (a+c+e, b+d+f)\\ &= (a+c, b+d)+(e,f)\\ &= ((a,b)+(c,d))+(e,f)\end{aligned}$$

(c). Elément neutre

$$\exists (e_1,e_2) \in \mathbb{R}^2, \forall (a,b) \in \mathbb{R}^2, \quad (a,b)+(e_1,e_2) = (e_1,e_2)+(a,b) = (a,b)$$

Soit $(a,b) \in \mathbb{R}^2$, on a

$$(a,b)+(e_1,e_2)=(a,b)\Leftrightarrow(a+e_1,b+e_2)=(a,b)$$

$$\Leftrightarrow\begin{cases}a+e_1=a\\ \\ b+e_2=b\end{cases}$$

$$\Leftrightarrow\begin{cases}e_1=0\\ \\ e_2=0\end{cases},$$

comme la loi + est commtative, alors

$$(e_1,e_2)+(a,b)=(a,b)+(e_1,e_2)=(a,b),$$

d'où + possède un élément neutre $0_{\mathbb{R}^2}=(0,0)$.
(d). Elément symétrique

$$\forall(a,b)\in\mathbb{R}^2,\exists(a',b')\in\mathbb{R}^2,\quad(a,b)+(a',b')=(a',b')+(a,b)=(e_1,e_2)$$

Soit $(a,b)\in\mathbb{R}^2$,

$$(a,b)+(a',b')=(0,0)\Leftrightarrow(a+a',b+b')=(0,0)$$

$$\Leftrightarrow\begin{cases}a+a'=0\\ \\ b+b'=0\end{cases}$$

$$\Leftrightarrow\begin{cases}a'=-a\\ \\ b'=-b\end{cases}$$

comme la loi + est commtative, alors

$$(a',b')+(a,b)=(a,b)+(a',b')=(0,0),$$

D'où tout élément $(a,b)\in\mathbb{R}^2$ est symétrisable et son symétrique est $(a',b')=(-a,-b)$.
2. • est associative,

$$\forall(a,b),(c,d),(e,f)\in\mathbb{R}^2,\quad(a,b)\bullet((c,d)\bullet(e,f))=((a,b)\bullet(c,d))\bullet(e,f)$$

Soient $(a,b),(c,d),(e,f)\in\mathbb{R}^2$, on a :

$$(a,b)\bullet((c,d)\bullet(e,f))=(a,b)\bullet(ce-df,cf+ed)$$

$$=(a(ce-df)-b(cf+ed),a(cf+ed)+(ce-df)b)$$

$$=(ace-adf-bcf-bed,acf+aed+ceb-dfb)$$

et

$$((a,b)\bullet(c,d))\bullet(e,f)=(ac-bd,ad+cb)\bullet(e,f)$$

$$=((ac-bd)\,e-(ad+cb)\,f,(ac-bd)\,f+e\,(ad+cb))$$

$$=(ace-bde-adf-cbf,acf-bdf+ade+cbe),$$

et donc on a

$$(a,b)\bullet((c,d)\bullet(e,f))=((a,b)\bullet(c,d))\bullet(e,f)$$

3. $\bullet$ est commtative,

$$\forall\,(a,b),(c,d)\in\mathbb{R}^2,\quad (a,b)\bullet(c,d)=(c,d)\bullet(a,b)$$

$$(a,b)\bullet(c,d)=(ac-bd,ad+cb)$$

$$=(ca-db,cb+ad)$$

$$=(c,d)\bullet(a,b)$$

4. $\bullet$ est distributive par rapport à $+$, $\forall\,(a,b),(c,d),(e,f)\in\mathbb{R}^2$,

$$(a,b)\bullet((c,d)+(e,f))=((a,b)\bullet(c,d))+((a,b)\bullet(e,f))$$

et

$$((c,d)+(e,f))\bullet(a,b)=((c,d)\bullet(a,b))+((e,f)\bullet(a,b))$$

Soient $(a,b),(c,d),(e,f)\in\mathbb{R}^2$, on a

$$(a,b)\bullet((c,d)+(e,f))=(a,b)\bullet(c+e,d+f)$$

$$=(a\,(c+e)-b\,(d+f),a\,(d+f)+(c+e)\,b)$$

$$=(ac+ae-bd-bf,ad+af+cb+eb),$$

et

$$((a,b)\bullet(c,d))+((a,b)\bullet(e,f))=(ac-bd,ad+cb)+(ae-bf,af+eb)$$

$$=(ac-bd+ae-bf,ad+cb+af+eb),$$

donc

$$(a,b)\bullet((c,d)+(e,f))=((a,b)\bullet(c,d))+((a,b)\bullet(e,f))$$

Comme la loi $\bullet$ est commtative, alors

$$((c,d)+(e,f))\bullet(a,b)=(a,b)\bullet((c,d)+(e,f))$$

$$=((a,b)\bullet(c,d))+((a,b)\bullet(e,f))$$

$$=((c,d)\bullet(a,b))+((e,f)\bullet(a,b))$$

d'où $\bullet$ est distributive par rapport à $+$.

5. Elément neutre par rapport à $\bullet$

$$\exists\,(a_1,a_2)\in\mathbb{R}^2, \forall\,(a,b)\in\mathbb{R}^2,\quad (a,b)\bullet(a_1,a_2)=(a_1,a_2)\bullet(a,b)=(a,b)$$

Soit $(a,b)\in\mathbb{R}^2$

$$(a,b)\bullet(a_1,a_2)=(a,b)\Leftrightarrow(aa_1-ba_2,aa_2+a_1b)=(a,b)$$

$$\Leftrightarrow\begin{cases} aa_1-ba_2=a \\ \\ aa_2+a_1b=b \end{cases}$$

$$\Leftrightarrow\begin{cases} a_1=1 \\ \\ a_2=0 \end{cases},$$

comme la loi $\bullet$ est commtative, alors

$$(a_1,a_2)+(a,b)=(a,b)+(a_1,a_2)=(a,b)\,,$$

d'où $\bullet$ possède un élément neutre $1_{\mathbb{R}^2}=(1,0)$

6. Elément symétrique par rapport à $\bullet$

$$\forall\,(a,b)\in\mathbb{R}^2-\{(0,0)\}\,,\exists\,(a',b')\in\mathbb{R}^2-\{(0,0)\}\,,\quad (a,b)\bullet(a',b')=(a',b')\bullet(a,b)=(1,0)$$

Soit $(a,b)\in\mathbb{R}^2-\{(0,0)\}$, on cherche un élément (a',b') dans $\mathbb{R}^2-\{(0,0)\}$ tel que

$$(a,b)\bullet(a',b')=(a',b')\bullet(a,b)=(1,0)$$

On a :

$$(a,b)\bullet(a',b')=(1,0)\Leftrightarrow(aa'-bb',ab'+a'b)=(1,0)$$

$$\Leftrightarrow\begin{cases} aa'-bb'=1 \\ \\ ab'+a'b=0 \end{cases}$$

$$\Leftrightarrow\begin{cases} a'=\frac{a}{a^2+b^2}\in\mathbb{R}^* \\ \\ b'=\frac{-b}{a^2+b^2}\in\mathbb{R}^* \end{cases},$$

comme la loi $\bullet$ est commtative, alors

$$(a',b')+(a,b)=(a,b)+(a',b')=(1,0)\,,$$

donc, chaque élément $(a,b)\in\mathbb{R}^2-\{(0,0)\}$ admet un inverse $\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$ dans $\mathbb{R}^2-\{(0,0)\}$.

Exercice 6

1. *Est-ce que* $\dot{\overline{23}}$ *est inversible dans* $\mathbb{Z}/_{121}\mathbb{Z}$ *? Si oui, quel est son inverse ?*
2. *Est-ce que* $\dot{\overline{25}}$ *est inversible dans* $\mathbb{Z}/_{90}\mathbb{Z}$ *? Si oui, quel est son inverse ?*

Solution
1. 23 et 121 sont premiers entre eux, et donc $\dot{\overline{23}}$ est inversible dans $\mathbb{Z}/_{121}\mathbb{Z}$.
Pour trouver son inverse, il faut résoudre l'équation de Bezout

$$23u + 121v = 1$$

Avec l'algorithme d'Euclide, on trouve que

$$121 = 23 \times 5 + 6$$

$$23 = 6 \times 3 + 5$$

$$6 = 5 \times 1 + 1$$

$$6 = 5 \times 1 + 1 \Leftrightarrow 6 - 5 \times 1 = 1$$

$$\Leftrightarrow 6 - (23 - 6 \times 3) = 1$$

$$\Leftrightarrow 6 \times (4) + 23 \times (-1) = 1$$

$$\Leftrightarrow (121 - 23 \times 5) \times (4) + 23 \times (-1) = 1$$

$$\Leftrightarrow 121 \times (4) + 23 \times (-21) = 1$$

Ainsi, l'inverse de $\dot{\overline{23}}$ dans $\mathbb{Z}/_{121}\mathbb{Z}$ est $\dot{\overline{-21}} = \dot{\overline{100}}$.
2. 5 divise à la fois 25 et 90. Ainsi, $\dot{\overline{25}}$ n'est pas inversible dans $\mathbb{Z}/_{90}\mathbb{Z}$.
Exercice 7

1. *Montrer que* $\mathbb{Z}/_{6}\mathbb{Z}$ *admet des diviseurs de zéro.* $\mathbb{Z}/_{6}\mathbb{Z}$ *est -il un corps ?*
2. *Montrer que* $\mathbb{Z}/_{5}\mathbb{Z}$ *est un corps.*

Solution
1. On sait que

$$\mathbb{Z}/_{6}\mathbb{Z} = \left\{\dot{\overline{0}}, \dot{\overline{1}}, \dot{\overline{2}}, \dot{\overline{3}}, \dot{\overline{4}}, \dot{\overline{5}}\right\}$$

On a :

$$\dot{\overline{2}} \times \dot{\overline{3}} = \dot{\overline{0}}$$

et

$$\dot{\overline{4}} \times \dot{\overline{3}} = \dot{\overline{0}}$$

Donc, $\mathbb{Z}/_{6}\mathbb{Z}$ admet des diviseurs de zéro.
Ce qui montre que $\mathbb{Z}/_{6}\mathbb{Z}$ n'est pas un corps.
2. $\mathbb{Z}/_{5}\mathbb{Z}$ est un corps, car 5 est premier.