Loi de composition

Définition

Soit X un ensemble non vide. **Une loi de composition interne sur** X est une application

$$\begin{array}{rcl} \star : X \times X & \longrightarrow & X \\ (x, y) & \longmapsto & x \star y. \end{array}$$

L'élément $x \star y$ s'appelle la composée de x et y par $\star$.

Exemples

1. L'addition $+$ et la multiplication $\cdot$ sont des lois de composition sur les ensembles de nombres suivants $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.
2. La soustraction $-$ est une loi de composition sur les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, mais elle ne l'est pas sur $\mathbb{N}$.
3. La division est une loi de composition sur les ensembles de nombres suivants $\mathbb{Q}^*, \mathbb{R}^*$ et $\mathbb{C}^*$, mais elle ne l'est pas sur $\mathbb{N}^*$ ni sur $\mathbb{Z}^*$.
4. Soit $G = \mathbb{R} \setminus \{1\}$. Pour tout $(x, y) \in G \times G$ on pose

   $$x \star y = x + y - xy.$$

   $\star$ est une loi de composition interne sur G. Vérifier chez vous comme exercice.
5. Soit $G =]-1, 1[$. Pour tout $(x, y) \in G \times G$ on pose

   $$x \star y = \frac{x + y}{1 + xy}.$$

   $\star$ est une loi de composition interne sur G.

Exemples

1. Pour tout $(x, y) \in \mathbb{Z} \times \mathbb{N}^*$ et $(x', y') \in \mathbb{Z} \times \mathbb{N}^*$ on pose

   $$(x, y) \star (x', y') = (xy' + x'y, yy').$$

   $\star$ est une loi de composition interne sur $\mathbb{Z} \times \mathbb{N}^*$.
2. Pour tout $(x, y) \in \mathbb{R}^* \times \mathbb{R}$ et $(x', y') \in \mathbb{R}^* \times \mathbb{R}$ on pose

   $$(x, y) \star (x', y') = (xx', xy' + y).$$

   $\star$ est une loi de composition interne sur $\mathbb{R}^* \times \mathbb{R}$.
3. Pour tout $x = (x_1 \cdots, x_n) \in \mathbb{R}^n$ et $y = (y_1 \cdots, y_n) \in \mathbb{R}^n$ on pose

   $$x \star y = (x_1 + y_1, \cdots, x_n + y_n).$$

   $\star$ est une loi de composition interne sur $\mathbb{R}^n$.

Exemples

1. L'addition et la multiplication des matrices sont deux lois de composition sur l'ensemble $\mathrm{M}_n(\mathbb{K})$ des matrices $n \times n$ à coefficients dans $\mathbb{K} = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.
2. Soit E un ensemble et $X = \mathcal{P}(E)$ l'ensemble des parties de E. Alors l'application
$$(A, B) \mapsto A \cup B$$
est une loi de composition sur X. De même, l'application
$$(A, B) \mapsto A \cap B$$
est une loi de composition sur X.
3. Soit E un ensemble et $X = \mathcal{F}(E)$ l'ensemble des applications de E dans lui même. Alors l'application
$$(f, g) \mapsto f \circ g$$
est une loi de composition sur X.

Définition

Soit $\star$ une loi de composition sur un ensemble non vide X.

1. On dit que $\star$ est **associative** si
$$\forall (x, y, z) \in X^3 \ , \quad (x \star y) \star z = x \star (y \star z)$$
Dans ce cas, il n'est pas nécessaire de mettre les parenthèses et l'expression $x \star y \star z$ n'est pas ambigüe.
2. Soit $e \in X$. On dit que e est un **élément neutre pour** $\star$ si
$$\forall x \in X, \ , \quad x \star e = e \star x = x.$$
3. On dit que $\star$ est **commutative** si
$$\forall (x, y) \in X^2 \ , \quad x \star y = y \star x.$$

Proposition

Soit $\star$ une loi de composition sur un ensemble non vide X. Si $\star$ admet un élément neutre alors cet élément est unique.

Démonstration : Soient e et e' deux éléments neutres pour $\star$. Alors
$$e' = e \star e' = e.$$

Définition

Un **monoïde** est un ensemble X muni d'une loi de composition interne associative et possédant un élément neutre.

Exemples

1. L'addition $+$ est une loi de composition associative et commutative sur les ensembles de nombres suivants $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$. L'élément neutre est 0.
2. La soustraction n'est pas associative : $5-(4-1)=5-3=2$ alors que $(5-4)-1=1-1=0$ et donc l'expression $5-4-1$ est ambigüe. La soustraction n'a pas d'élément neutre.
3. La multiplication des matrices sur l'ensemble $\mathrm{M}_n(\mathbb{K})$ est associative et son élément neutre est la matrice identité. Cette loi n'est pas commutative dès que $n \geq 2$.
4. Sur $\mathbb{N}$ on définit la loi de composition interne $\star$ par

   $$x \star y = 2(x+y)$$

   qui est visiblement commutative. Une telle loi n'est pas associative. En effet,

   $$(1 \star 2) \star 3 = 6 \star 3 = 18 \quad \text{alors que} \quad 1 \star (2 \star 3) = 1 \star 10 = 22.$$

Définition

Soit $\star$ une loi de composition sur un ensemble non vide X qui possède un élément neutre e. On dit qu'un élément x de X admet un **élément symétrique** s'il existe $y \in X$ tel que

$$x \star y = y \star x = e.$$

Proposition

*Soit $\star$ est une loi de composition **associative** sur un ensemble non vide X qui possède un élément neutre e. Si un élément x de X admet un élément symétrique y alors cet élément est unique. Autrement dit, dans un monoïde tout élément admet au plus un symétrique.*

Démonstration : Soit $x \in X$. Supposons que y et y' sont deux éléments symétriques de x. Alors, grâce à l'associativité de $\star$, on a

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

Corollaire

Soit $\star$ est une loi de composition associative sur un ensemble non vide X qui possède un élément neutre e. Si y est l'élément symétrique x alors y admet un élément symétrique et cet élément symétrique est x.

Exemples

1. L'addition $+$ est une loi de composition associative et commutative sur les ensembles de nombres suivants $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$. Son élément neutre est 0. Aucun élément de $\mathbb{N}^*$ n'a de symétrique dans $\mathbb{N}$. Tout élément x de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ admet un symétrique noté $-x$.
2. La multiplication est une loi de composition associative et commutative sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$. Son élément neutre est 1. Aucun élément de $\mathbb{N}, \mathbb{Z}$ n'a de symétrique dans $\mathbb{Z}$. Tout élément x non nul de $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ admet un symétrique noté x^{-1}.
3. La multiplication des matrices sur l'ensemble $\mathrm{M}_n(\mathbb{K})$ est associative et son élément neutre est la matrice identité. Un élément A de $\mathrm{M}_n(\mathbb{K})$ admet un symétrique si, et seulement si, A est une matrice inversible.

Exemple

Soit $G = \mathbb{R} \setminus \{1\}$. Pour tout $(x, y) \in G \times G$ on pose

$$x \star y = x + y - xy.$$

- $\star$ est une loi de composition interne sur G. En effet, pour tout $(x, y) \in G \times G$,

  $$1 - x \star y = 1 - x - y + xy = (1 - x)(1 - y).$$

  Si x et y sont des éléments de $G = \mathbb{R} \setminus \{1\}$ alors $1 - x \star y \neq 0$, et donc $x \star y \in G$.
- Il est clair que $\star$ est commutative.
- $\star$ est associative. En effet, soit x, y, z trois éléments de G. On a

  $$(x \star y) \star z = (1 - (1 - x)(1 - y)) \star z = 1 - (1 - x)(1 - y)(1 - z).$$

  De même, on a

  $$x \star (y \star z) = 1 - (1 - x)(1 - y)(1 - z) = (x \star y) \star z.$$

- Élément neutre. Si e est un élément neutre de $\star$ alors

  $$\forall x \in G, \quad x \star e = x + e - xe = x$$

  et donc

  $$\forall x \in G, \quad e(1 - x) = 0$$

  et finalement $e = 0$. Inversement, on vérifie que

  $$\forall x \in G, \quad x \star 0 = 0 \star x = x.$$

  Ainsi $e = 0$ est l'élément neutre de $\star$.
- Soit $x \in G$. Si x admet un élément symétrique y alors

  $$x \star y = x + y - xy = 0$$

  autrement dit, $y(x - 1) = x$; et comme $x \neq 1$, on déduit que

  $$y = \frac{x}{x - 1}.$$

  Inversement, on vérifie que cet élément appartient à G et c'est l'élément symétrique de x :

  $$\frac{x}{x - 1} \in G \quad \text{et} \quad x \star \frac{x}{x - 1} = \frac{x}{x - 1} \star x = 0.$$

Exercice

On considère l'ensemble $\mathcal{E}$ des matrices carrées à coefficients réels de la forme

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} , a \in \mathbb{R}^*, b \in \mathbb{R}.$$

1. *Vérifier que le produit des matrices est une loi de composition interne associative sur $\mathcal{E}$. Ce produit est-il commutatif ?*
2. *Trouver tous les éléments $E \in \mathcal{E}$ tels que*

$$\forall A \in \mathcal{E}, \quad AE = A.$$

De tels éléments E s'appellent des éléments neutres à droite de $(\mathcal{E}, \cdot)$.

3. *Existe-t-il un élément $E \in \mathcal{E}$ tels que*

$$\forall A \in \mathcal{E}, \quad EA = A?$$

4. *Soit E un élément neutre à droite de $(\mathcal{E}, \cdot)$. Montrer que tout élément A de $\mathcal{E}$ admet un inverse à gauche pour cet élément neutre, i.e.*

$$\forall A \in \mathcal{E} \ , \ \exists B \in \mathcal{E} \quad BA = E.$$

Notations additive et multiplicative

1. *Parfois on utilise la notation additive $\star = +$, c-à-d*

$$x \star y = x + y$$

Dans ce cas, on dit que $x + y$ est la somme de x et y. Si $+$ possède un élément neutre il sera noté 0. Si un élément x possède élément symétrique alors cet élément symétrique sera noté $-x$ appelé l'opposé de x. Cette notation est exclusivement utilisée dans les cas commutatifs.

2. *La loi $\star$ peut être notée multiplicativement, c-à-d*

$$x \star y = x \cdot y \quad ou \quad x \star y = xy$$

et on dit que xy est le produit de x et y. Si $\cdot$ possède un élément neutre il sera noté 1. Si un élément x possède élément symétrique alors cet élément symétrique sera noté x^{-1} appelé l'inverse de x.

Itérés d'un élément

Supposons que $\star$ est une loi de composition associative sur un ensemble non vide X et $\star$ possède un élément neutre e. Dans toute la suite et sauf mention contraire, si un élément x de X admet un élément symétrique nous noterons x^{-1} son élément symétrique. Dans ce cas, x est l'élément symétrique de x^{-1} :

$$\forall x \in G \ , \quad (x^{-1})^{-1} = x.$$

De plus,

$$\forall (x, y) \in G^2 \ , \quad (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}.$$

On peut définir

$$x^0 := e \ , \ x^1 := x, \quad x^2 := x \star x, \quad \cdots , \quad x^{n+1} := x \star x^n = \underbrace{x \star x \star x \cdots \star x}_{\text{n+1 fois}} \ (\forall n \in \mathbb{N}).$$

Nous avons

$$\forall (m,n) \in \mathbb{N}^2, \quad x^{m+n} = x^m \star x^n \quad \text{et} \quad x^{mn} = (x^m)^n$$

Si x admet un élément symétrique alors, pour tout $n \in \mathbb{N}$, l'élément x^n admet un élément symétrique et

$$\forall n \in \mathbb{N}, \quad x^{-n} := (x^n)^{-1} = (x^{-1})^n$$

Ainsi, pour tout $m, n \in \mathbb{Z}$,

$$x^{m+n} = x^m \star x^n \text{ et } x^{mn} = (x^m)^n$$

Si $\star$ est additive, i.e. $\star = +$, alors il convient d'utiliser les notation suivantes :

- l'élément neutre se note 0 ;
- l'élément symétrique de x se note $-x$ et s'appelle l'opposé de x. Dans ce cas, $-(-x) = x$.
- Aussi $\underbrace{x + x + \cdots + x}_{n \text{ fois}}$ sera noté nx au lieu de x^n.

Définition

Soit X un ensemble non vide muni d'une loi de composition interne $\star$. Une partie H de X est dite **stable ou fermée pour** $\star$ si

$$\forall (x,y) \in H^2, \quad x \star y \in H.$$

Dans ce cas, la restriction de $\star$ à H est une loi de composition interne sur H appelée **loi induite par** $\star$ **sur** H que l'on notera $\star_H$ ou simplement $\star$ s'il n'y a pas de confusions.

Soit H une partie de X stable pour $\star$.

1. Si $\star$ est associative sur X alors $\star_H$ est associative sur H.
2. Si $\star$ est commutative sur X alors $\star_H$ sur H est aussi commutative sur H.
3. De même, si e est un élément neutre de $\star$ dans X et $e \in H$ alors e un élément neutre de $\star_H$ sur H.

Aucune des assertions précédentes n'a de réciproque vraie en général. Par exemple, $\star_H$ peut être commutative sans que $\star$ le soit.

Exemples

1. Supposons que $X = \mathbb{Z}, \star = +$ et $H = \mathbb{N}$. Il est clair que H est stable pour $+$. La même affirmation est vraie si on prend $\star = \cdot$.
2. Supposons que $X = \mathbb{C}, \star = \cdot$ et $\mathbb{U}$ l'ensemble des nombres complexes de module 1. Il est clair que $\mathbb{U}$ est stable pour $\cdot$. Attention $\mathbb{U}$ n'est pas stable pour $+$.
3. Posons $X = \mathcal{M}_2(\mathbb{R})$, $\star = \cdot$ la multiplication des matrices et

$$\begin{aligned} \mathcal{T}_2^-(\mathbb{R}) &= \left\{ \begin{pmatrix} a & 0 \\ c & b \end{pmatrix} \ / \ a,b,c \in \mathbb{R}. \right\}, \quad \mathcal{T}_2^+(\mathbb{R}) = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \ / \ a,b,c \in \mathbb{R} \right\} \\ \mathcal{D}_2(\mathbb{R}) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \ / \ a,b \in \mathbb{R} \right\} \quad \mathcal{R} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ / \ a \in \mathbb{R} \right\}. \end{aligned}$$

   Les parties $\mathcal{D}_2(\mathbb{R}), \mathcal{T}_2^-(\mathbb{R}), \mathcal{T}_2^+(\mathbb{R})$ et $\mathcal{R}$ sont stables pour la multiplication des matrices . De plus, la multiplication des matrices est commutative sur $\mathcal{D}_2(\mathbb{R})$ et $\mathcal{R}$, mais elle ne l'est pas sur $X = \mathcal{M}_2(\mathbb{R})$ ni même sur $\mathcal{T}_2^-(\mathbb{R})$ et $\mathcal{T}_2^+(\mathbb{R})$. Par exemple,

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

Exemples

Posons $X = \mathcal{M}_2(\mathbb{R})$, $\star = \cdot$ la multiplication des matrices et

$$H' = \left\{ \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} \ / \ a \in \mathbb{R}. \right\}$$

H' n'est pas stable pour $\star$. En effet,

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

Notons aussi, qu'avec les notations de l'exemple précédent, la réunion $\mathcal{T}_2^-(\mathbb{R}) \cup \mathcal{T}_2^+(\mathbb{R})$ n'est pas stable pour la multiplication des matrices. Par exemple,

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

Groupes

Définition

On appelle **groupe** un ensemble non vide G muni d'une loi de composition interne $\star$ tels que :

1. $\star$ est associative : $\forall (x, y, z) \in G^3$, $(x \star y) \star z = x \star (y \star z)$
2. $\star$ possède un élément neutre, i.e. il existe un élément $e \in G$ tel que

$$\forall x \in G, \ , \quad x \star e = e \star x = x.$$

3. tout élément de G possède un élément symétrique, i.e.

$$\forall x \in G, \ \exists y \in G, \quad x \star y = y \star x = e$$

Un groupe $(G, \star)$ est dit **commutatif ou abélien** si la loi $\star$ est commutative, i.e. $\forall (x, y) \in G^2$, $x \star y = y \star x$.

Proposition

1. *L'élément neutre d'un groupe est unique.*
2. *Le symétrique d'un élément est unique.*
3. *Soit $(G, \star)$ un groupe.*
   (a) *Soit x un élément de G. Si y est l'élément symétrique de x alors x est l'élément symétrique y.*
   (b) *Soient x_1, x_2 deux éléments de G et y_1, y_2 leur élément symétrique respectifs. Alors l'élément symétrique de $x_1 \star x_2$ est $y_2 \star y_1$*

Preuve : Seul le troisième point n'est pas encore démontré. On a,

$$(y_2 \star y_1) \star (x_1 \star x_2) = y_2 \star (y_1 \star (x_1 \star x_2)) = y_2 \star ((y_1 \star x_1) \star x_2) = y_2 \star (e \star x_2) = y_2 \star x_2 = e.$$

De même,

$$(x_1 \star x_2) \star (y_2 \star y_1) = x_1 \star (x_2 \star (y_2 \star y_1)) = x_1 \star ((x_2 \star y_2) \star y_1)) = x_1 \star (e \star y_1)) = x_1 \star y_1 = e.$$

Ce qui finit la preuve.

Exemples

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes commutatifs.
2. $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ sont des groupes commutatifs.
3. L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles de taille $n \times n$ muni du produit des matrices est un groupe. Il est non commutatif si $n \geq 2$. Par exemple,
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$
4. L'ensemble $\mathcal{S}(X)$ des bijections d'un ensemble non vide X s'appelle l'ensemble des permutations de X. Le couple $(\mathcal{S}(X), \circ)$ est un groupe. On verra qu'il est non commutatif si X contient plus de trois éléments.

Exemple

L'ensemble
$$\mathcal{G} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ / \ a \in \mathbb{R} \right\}$$
est un groupe commutatif pour la multiplication des matrices. L'élément neutre étant la matrice unité
$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
De plus, l'élément inverse d'une matrice $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ est donné par
$$A^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}.$$

Exemple

L'ensemble

$$\mathcal{H} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ / \ (a,b,c) \in \mathbb{R}^3 \right\}$$

est un groupe pour la multiplication des matrices. Il s'appelle le **groupe de Heisenberg**. Son élément neutre est la matrice unité $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. De plus, l'élément inverse d'une matrice $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ est donné par

$$A^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Notons que ce groupe est non commutatif. En effet,

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

alors que

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

Remarque

Soit $(G, \star)$ un groupe et x, y, z des éléments de G. Nous avons

1. $x \star y = z \star y \Longrightarrow x = z$.
2. $y \star x = y \star z \Longrightarrow x = z$.

On dit que tous les éléments d'un groupe sont réguliers.

En effet, supposons que $x \star y = z \star y$. L'élément y possède un élément symétrique que nous noterons y'. On a

$$(x \star y) \star y' = (z \star y) \star y'.$$

Comme $\star$ est associative, on a

$$x \star (y \star y') = z \star (y \star y').$$

Ainsi

$$x \star e = z \star e$$

et donc $x = z$. Le second point se montre de la même façon.

Remarque

Soit $(G, \star)$ un groupe et a, b deux éléments de G. Notons a' l'élément symétrique de a. Alors l'équation

$$x \star a = b$$

admet une unique solution donnée par $x = b \star a'$. En effet, on a

$$(b \star a') \star a = b \star (a' \star a) = b \star e = b$$

et donc $b \star a'$ est bien une solution de l'équation $x \star a = b$. De plus, si x est solution de $x \star a = b$ alors

$$b \star a' = (x \star a) \star a' = x \star (a \star a') = x \star e = x.$$

De même l'équation

$$a \star x = b$$

admet une unique solution donnée par $x = a' \star b$.

Par exemple dans le groupe de Heisenberg $\mathcal{H} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ / \ (a,b,c) \in \mathbb{R}^3 \right\}$ l'équation

$$X \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

admet une unique solution

$$\begin{aligned} X = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Remarque

Attention les équations de type $AX = B$ peuvent s'avérer complexes quand on ne travaille pas dans un groupe. Par exemple, considérons dans $\mathcal{M}_2(\mathbb{R})$ les deux équations :

$$\underbrace{\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}}_{A} X = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad AX = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

D'une part, la première équation admet une infinité de solutions distinctes données par :

$$X = \begin{pmatrix} a & b \\ -a & -b \end{pmatrix}, \quad a, b \in \mathbb{R}.$$

D'une autre part, la seconde équation n'admet aucune solution. Ces deux phénomènes ne peuvent se produire dans un groupe car les éléments d'un groupe sont réguliers. D'ailleurs, la matrice A ci-dessus n'admet pas d'élément symétrique pour la multiplication (inverse).

Notations additives

Un groupe $(G, \star)$ est dit additif si son opération est notée $\star = +$. Dans ce cas, $+$ est toujours supposée commutative et

- l'élément neutre se note 0 ;
- l'élément symétrique de x se note $-x$ et s'appelle l'opposé de x.

On peut définir les multiples d'un élément donné x de G par

$$0x := 0,\ 1x = x,\ \ 2x = x + x,\ \ \cdots,\quad (n+1)x := x + nx = \underbrace{x + x + \cdots + x}_{(n+1) \text{ fois}}\ \ (\forall n \in \mathbb{N})$$

On peut aussi définir,

$$\forall n \in \mathbb{N},\ \ (-n)x = n(-x).$$

On a ainsi définit nx pour $n \in \mathbb{Z}$. Nous avons ainsi :

$$(n+m)x = nx + mx \quad \text{et} \quad n(x+y) = nx + ny.$$

Le dernière égalité suit de la commutativité de $+$.

Notations multiplicatives

Si le groupe est multiplicatif, c-à-d $\star = \cdot$ alors

- l'élément neutre se note 1
- l'élément symétrique de x se note x^{-1} et s'appelle l'inverse de x. Dans ce cas, x est l'inverse de x^{-1} :

  $$\forall x \in G\ ,\quad (x^{-1})^{-1} = x.$$

  De plus,

  $$\forall (x, y) \in G^2\ ,\quad (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}.$$

On peut définir les puissances d'un élément donné x de G par

$$x^0 := 1\ ,\ x^1 := x,\ \ x^2 := x \cdot x,\ \ \cdots,\ \ x^{n+1} := x \cdot x^n = \underbrace{x \cdot x \cdots x}_{(n+1) \text{ fois}}\ \ (\forall n \in \mathbb{N}).$$

De même,

$$\forall n \in \mathbb{N},\quad x^{-n} := (x^{-1})^n$$

Ainsi, pour tout $m, n \in \mathbb{Z}$,

$$x^{m+n} = x^m \cdot x^n \text{ et } x^{mn} = (x^m)^n$$

De plus,

$$\forall (x, y) \in G^2\ ,\ \ x \cdot y = y \cdot x \Longrightarrow (x \cdot y)^n = x^n \cdot y^n$$

Cas général

Soit $(G, \star)$ un groupe. Dans toute la suite et sauf mention contraire, nous noterons x^{-1} l'élément symétrique d'un élément x de G. De plus, les puissances d'un élément donné x de G sont données par

$$x^0 := e \ , \ x^1 := x, \quad x^2 := x \star x, \quad \cdots , \quad x^{n+1} := x \star x^n = \underbrace{x \star x \star \cdots \star x}_{(n+1) \text{ fois}} \quad (\forall n \in \mathbb{N}).$$

De même,

$$\forall n \in \mathbb{N}, \quad x^{-n} := (x^{-1})^n$$

Ainsi, pour tout $m, n \in \mathbb{Z}$,

$$x^{m+n} = x^m \star x^n \text{ et } x^{mn} = (x^m)^n$$

De plus,

$$\forall (x, y) \in G^2 \ , \quad x \star y = y \star x \Longrightarrow (x \star y)^n = x^n \star y^n$$

Remarque

Soit G un ensemble non vide muni d'une loi de composition associative notée $\star$. On peut montrer que $(G, \star)$ est un groupe si, et seulement si, il existe un élément $e \in G$ tel que

$$(1) \quad \forall g \in G \quad g \star e = g$$
$$(2) \quad \forall g \in G \quad \exists g' \in G, g \star g' = e.$$

En effet, les conditions (1) et (2) sont clairement nécessaires. Pour montrer qu'elles sont suffisantes il nous suffit de montrer que e est un élément neutre de $\star$ et que tout élément g de G admet un symétrique. Pour cela soit $g \in G$. D'après la condition (2) il existe $g' \in G$ tel que $g \star g' = e$. En composant avec g' à gauche on obtient

$$g' \star (g \star g') = g' \star e$$

et comme $\star$ est associative et par la condition (1) on obtient

$$(g' \star g) \star g' = g'.$$

Maintenant, d'après la condition (2) appliquée à g', il existe $g'' \in G$ tel que $g' \star g'' = e$. En composant avec g'' à droite on obtient

$$(g' \star g) \star (g' \star g'') = g' \star g'' = e$$

et donc

$$g' \star g = e.$$

Finalement,

$$g' \star g = g \star g' = e \quad (\#)$$

On en déduit que $e \star g = g$, car

$$e \star g = (g \star g') \star g = g \star (g' \star g) = g \star e = g.$$

Donc e est l'élément neutre de $(G, \star)$. Finalement, la relation $(\#)$ montre que $g' = g^{-1}$.

Sous groupes

Définition

Soit $(G, \star)$ un groupe et H une partie *non vide* de G. On dit que H est un **sous groupe de** G si

1. H est stable par $\star$, c-à-d
$$\forall (x, y) \in H^2 \ , \quad x \star y \in H;$$
2. le symétrique de tout élément x de H appartient à H :
$$\forall x \in H, \quad x^{-1} \in H.$$

En particulier, tout sous groupe H de G contient l'élément neutre de G. En effet, comme H est non vide, il existe $x \in H$ et donc x^{-1} appartient aussi à H. Ainsi, comme H est stable pour $\star$, il vient que $e = x \star x^{-1} \in H$.

Exercice :

Soit H une partie non vide de G. Montrer que les assertions suivantes sont équivalentes :

1. *H est un sous groupe de $(G, \star)$*
2. *H est stable pour $\star$ et $(H, \star_H)$ est un groupe*
3. $\forall (x, y) \in H^2 \ , \quad x \star y^{-1} \in H;$

Solution : 1)$\Longrightarrow$2) : Supposons que H est un sous groupe de $(G, \star)$. Alors H est stable pour $\star$ et contient e. Ainsi, la restriction de $\star$ notée par $\star_H$ est une loi de composition interne sur H qui est associative, et e est son élément neutre. De plus, tout élément x de H voit son symétrique x^{-1} dans H et donc
$$x \star_H x^{-1} = x \star x^{-1} = e = x^{-1} \star x = x^{-1} \star_H x \ ;$$
autrement dit, x^{-1} est le symétrique de x dans $(H, \star_F)$. D'où $(H, \star_F)$ est un groupe.

2)$\Longrightarrow$1) : Supposons que H est stable pour $\star$ et $(H, \star_H)$ est un groupe. Notons e_H l'élément neutre de $(H, \star_H)$. Donc
$$e_H \star e_H = e_H \star_H e_H = e_H.$$
Notons e_H^{-1} l'inverse de e_H dans G. Nous avons donc dans G :
$$e_H = e \star e_H = (e_H^{-1} \star e_H) \star e_H = e_H^{-1} \star (e_H \star e_H) = e_H^{-1} \star e_H = e.$$
Donc e est l'élément neutre de $(H, \star_H)$. Il reste à montrer que, pour tout $x \in H$, $x^{-1} \in H$.

Soit $x \in H$. Comme $(H, \star_H)$ est un groupe il existe un élément $y \in H$ tel que
$$x \star_H y = y \star_H x = e$$
et donc
$$x \star y = y \star x = e$$
Or ceci signifie que y est le symétrique de x dans G aussi. Finalement, $x^{-1} = y \in H$.

1)$\Longrightarrow$3) : Supposons que H est un sous groupe de $(G, \star)$. Soit $(x, y) \in H^2$. Alors $y^{-1} \in H$ et $x \star y^{-1} \in H$.

3)$\Longrightarrow$1) : supposons que la dernière assertion est vraie. Comme H non vide, on prend un $x \in H$ et donc $e = x \star x^{-1} \in H$. De plus, pour tout élément $y \in H$
$$y^{-1} = e \star y^{-1} \in H.$$

Ainsi, pour tout $(x, y) \in H^2$ on a $x \star y = x \star (y^{-1})^{-1} \in H$. Ici nous avons utilisé le fait que $(y^{-1})^{-1} = y$.

Exemples

1. $\{e\}$ et G sont deux sous groupes de G.
2. $\mathbb{R}_+^*$ est un sous groupe de $(\mathbb{R}^*, \cdot)$. Notons que $\mathbb{R}_-^*$ n'est pas un sous groupe de $(\mathbb{R}^*, \cdot)$.
3. L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est un sous groupe de $(\mathbb{C}^*, \cdot)$.
4. Soit a un élément de $\mathbb{Z}$. Alors l'ensemble des multiples de a noté $H = a\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$.

Proposition

les sous groupes de $(\mathbb{Z}, +)$ sont les parties de la forme $a\mathbb{Z}$.

Preuve : (i) Selon l'exemple précédent, si $H = a\mathbb{Z}$ alors H est un sous groupe de $(\mathbb{Z}, +)$

(ii) Soit H un sous groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Sinon, notons a le plus petit élément positif non nul de H. Comme H stable pour l'addition, on déduit que $a\mathbb{Z} \subset H$. Pour montrer l'autre inclusion, soit $b \in H$. La division euclidienne de b par a montre qu'il existe $q, r \in \mathbb{Z}$ tel que

$$b = aq + r \quad \text{et} \quad 0 \leq r < a.$$

Ainsi

$$r = b - aq \in H.$$

Donc $0 \leq r < a, r \in H$ et comme a est le plus petit élément non nul positif de H, on déduit que $r = 0$. Finalement, $b = aq$ et donc $H \subset a\mathbb{Z}$.

Corollaire : Théorème de Bezout

Soient a, b deux éléments de $\mathbb{Z}$ et d leur P.G.C.D. Alors il existe deux éléments u et v de $\mathbb{Z}$ tels que

$$au + bv = d.$$

En particulier, a et b sont premiers entre eux si, et seulement si, il existe deux éléments u et v de $\mathbb{Z}$ tels que $au + bv = 1$.

Preuve : Posons

$$H = \{au + bv \ / \ (u, v) \in \mathbb{Z}\}$$

Il est clair que H est un sous groupe de $\mathbb{Z}$. Donc il existe $n \in \mathbb{Z}$ tel que $H = n\mathbb{Z}$. Comme a et b appartiennent à H alors n divise a et b; et donc n divise d. De plus, si un entier divise a et b alors il divise tout élément de H. Comme $n \in H$, et d divise a et b, on déduit que d divise n. Finalement, $d = \pm n \in H$ ce qui est l'assertion recherchée.

Exemples

1. L'ensemble
$$\mathcal{G}_1 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ / \ a \in \mathbb{R} \right\}$$
est un sous groupe de $\mathrm{GL}_2(\mathbb{R})$. En particulier, muni de la multiplication des matrices $\mathcal{G}_1$ est un groupe. Le lecteur pourra vérifier que ce groupe est commutatif.
2. L'ensemble
$$\mathcal{G}_2 = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \ / \ a \in \mathbb{R}^*, \ b \in \mathbb{R} \right\}$$
est un sous groupe de $\mathrm{GL}_2(\mathbb{R})$. En particulier, muni de la multiplication des matrices $\mathcal{G}_2$ est un groupe. Le lecteur pourra vérifier que ce groupe n'est pas commutatif.
3. L'ensemble
$$\mathcal{H} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ / \ (a,b,c) \in \mathbb{R}^3 \right\}$$
est un sous groupe $\mathrm{GL}_3(\mathbb{R})$. En particulier, muni de la multiplication des matrices $\mathcal{G}$ est un groupe. Le lecteur pourra vérifier que ce groupe n'est pas commutatif.

Remarque

1. L'intersection de deux sous groupes d'un groupe G est un sous groupe de G.
2. La réunion de deux sous groupes de G n'est pas toujours un sous groupe de G. Par exemple, $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous groupe de $\mathbb{Z}$.
3. Soit H un sous groupe de G et $x \in G$. Si H contient x alors il contient toutes les puissances x^k de x avec $k \in \mathbb{Z}$. Autrement dit,
$$\langle x \rangle := \{x^k \ / \ k \in \mathbb{Z}\} \subset H.$$
De plus, $\langle x \rangle$ est un sous groupe de G appelé le sous groupe engendré par x. Il s'agit du plus petit sous groupe de G contenant x et son cardinal s'appelle l'ordre de x.
4. Soit A une partie de G. Parmi les sous groupes de G contenant A, il existe un qui est plus petit que tous les autres. Il s'agit de l'intersection de tous les sous groupes de G contenant A appelé le sous groupe de G engendré par A.

Morphismes de groupes

Définition

Soit $(G_1, \star)$ et $(G_2, \cdot)$ deux groupes. et $\psi : G_1 \longrightarrow G_2$ une application.

1. On dit que ψ est un homomorphisme si ψ vérifie les propriétés suivantes :
$$\forall (x,y) \in G_1^2 \ , \quad \psi(x \star y) = \psi(x) \cdot \psi(y)$$
2. On dit que ψ est un isomorphisme si ψ est un homomorphisme de groupe qui est bijectif. Dans ce cas, on dit que les deux groupes $(G_1, \star)$ et $(G_2, \cdot)$ sont isomorphes.
3. Un automorphisme de groupe est un isomorphisme d'un groupe sur lui même.

En particulier, si e_1, e_2 désignent les éléments neutres de G_1 et G_2 respectivement alors

$$\boxed{\psi(e_1) = e_2}.$$

En effet,

$$\psi(e_1) = \psi(e_1 \star e_1) = \psi(e_1)\psi(e_1).$$

En composant avec l'inverse de $\psi(e_1)$ on obtient :

$$e_2 = (\psi(e_1))^{-1}\, \psi(e_1) = \psi(e_1).$$

De plus, pour tout $x \in G_1$ on a

$$e_2 = \psi(e_1) = \psi(x \star x^{-1})) = \psi(x) \cdot \psi(x^{-1}).$$

Ainsi, pour tout $x \in G_1$ on a

$$\boxed{\psi(x^{-1}) = (\psi(x))^{-1}}$$

Remarque

Soit $(G_1, \cdot), (G_2, \cdot)$ et $(G_3, \cdot)$ trois groupes. Si $\psi : G_1 \longrightarrow G_2$ et $\varphi : G_2 \longrightarrow G_3$ sont des morphismes de groupe alors $\varphi \circ \psi$ est un morphisme de groupe. De même, si ψ est un isomorphisme de groupe alors ψ^{-1} est un isomorphisme de groupe. Le lecteur a la charge de démontrer ces deux assertions.

Exemple

On rappelle que $(\mathbb{R}_+^*, \cdot)$ est un groupe commutatif. L'application

$$\begin{array}{rcl} \exp : (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}_+^*, \cdot) \\ x & \longmapsto & \exp(x) = e^x \end{array}$$

est un isomorphisme de groupe. Sa réciproque est

$$\begin{array}{rcl} \ln : (\mathbb{R}_+^*, \cdot) & \longrightarrow & (\mathbb{R}, +) \\ x & \longmapsto & \ln(x). \end{array}$$

Exemple

On rappelle que $\mathcal{G} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ / \ a \in \mathbb{R} \right\}$ est un groupe pour la multiplication des matrices. L'application

$$\begin{array}{rcl} \psi : (\mathbb{R}, +) & \longrightarrow & (\mathcal{G}, \cdot) \\ a & \longmapsto & \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \end{array}$$

est un isomorphisme de groupe.

Exercice

1. Montrer que l'ensemble
$$\mathcal{R} = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \ / \ \theta \in \mathbb{R} \right\}$$
est un groupe pour la multiplication des matrices. Est-il commutatif ? Montrer que l'application
$$\begin{array}{rcl} \psi : (\mathbb{R}, +) & \longrightarrow & (\mathcal{G}, \cdot) \\ \theta & \longmapsto & \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{array}$$
est un morphisme de groupe.
2. De même, montrer que l'application
$$\begin{array}{rcl} f : (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \cdot) \\ t & \longmapsto & e^{it} \end{array}$$
est un morphisme de groupe.

Exemple

1. Soit $(G, \star)$ un groupe et $g \in G$. L'application
$$\begin{array}{rcl} \psi_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$
est un morphisme de groupe.
2. Soit $(G, \star)$ un groupe **commutatif** et $n \in \mathbb{Z}$. L'application
$$\begin{array}{rcl} \psi_n : G & \longrightarrow & G \\ g & \longmapsto & g^n \end{array}$$
qui est un morphisme de groupe.

Exercice

Soit $(G, \star)$ un groupe tel que l'application
$$\begin{array}{rcl} \psi_2 : G & \longrightarrow & G \\ g & \longmapsto & g^2 \end{array}$$
qui est un morphisme de groupe. Montrer que G est commutatif.