Chapitre 6

Structures algébriques

6.1 Loi de composition interne

Définition 6.1.1 (Loi de composition interne)**.** *On appelle **loi de composition interne** (en abrégé lci) sur un ensemble E toute application $*$ de $E \times E$ dans E. Une lci est notée $* : E \times E \longrightarrow E$, $(x, y) \longmapsto x * y$, $x * y$ s'appelle composé de x et y.*

Une lci est notée $*$, ou encore $\top$, $\perp$, Δ, ∇, $\circ$, $\oplus$, $\otimes$,... et très souvent $+$ ou $\cdot$, si la lci est notée $+$ elle est dite additive, et si elle est notée $\cdot$, elle est dite multiplicative.

Exemple 6.1.1.
1. *L'addition est la multiplication sont des lci dans $\mathbb{N}$.*
2. *La soustraction n'est pas une lci dans $\mathbb{N}$.*
3. *Pour tout ensemble E, la réunion et l'intersection sont des lci dans $\mathcal{P}(E)$.*
4. *La loi $\oplus$ définie par : $\forall x \in \mathbb{R} : x \oplus y = x + y - 1$ est une lci dans $\mathbb{R}$.*
5. *La loi $\otimes$ définie par : $\forall x \in \mathbb{R} : x \otimes y = x + y - xy$ est une lci dans $\mathbb{R}$.*

Exercice 6.1.
1. *Montrer que l'addition des fonctions est une lci dans l'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ des fonctions réelles à variable réelle.*

   L'addition des fonctions est définie comme suit :

   Pour f et g deux éléments de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ la fonction $f + g$ est définie en donnant l'image de tout élément réel x par $f + g$, par

$$\forall x \in \mathbb{R}, (f + g)(x) = f(x) + g(x)$$

2. *Même question pour la composition des fonctions définie par :*

$$\forall x \in \mathbb{R}, (g \circ f)(x) = g[f(x)]$$

Définition 6.1.2 (compatibilité d'une relation d'équivalence avec une loi)**.** *On dit que la relation d'équivalence $\mathcal{R}$ est compatible avec la loi $*$ si :*

$$\forall x, y, z, t \in E, x\mathcal{R}y \text{ et } z\mathcal{R}t \implies x * z\mathcal{R}y * t$$

Si la relation $\mathcal{R}$ est compatible avec la loi $*$, l'application :

$$\begin{aligned}\hat{*} : (E/\mathcal{R}) \times (E/\mathcal{R}) &\longrightarrow (E/\mathcal{R}) \\ (\hat{x}, \hat{y}) &\longmapsto \hat{x}\hat{*}\hat{y} = \widehat{x * y}\end{aligned}$$

Définit une loi interne $\hat{*}$ sur $E/\mathcal{R}$, on l'appelle loi quotient de la loi $*$ par la relation $\mathcal{R}$.

Définition 6.1.3 (associativité)**.** *Une lci est dite* ***associative*** *si et seulement si*

$$\forall (x, y, z) \in E^3, (x * y) * z = x * (y * z)$$

Exemple 6.1.2. 1. *L'addition et la multiplication dans $\mathbb{N}$ sont associatives.*

2. *La lci*

$$\begin{aligned}* : \mathbb{Q}^2 &\longrightarrow \mathbb{Q} \\ (x, y) &\longmapsto \frac{x + y}{2}\end{aligned}$$

n'est pas associative. En effet, par exemple, pour $x = -1$, $y = 0$, $z = 1$, on a :

$$[(-1) * 0] * 1 = \frac{1}{4} \text{ et } (-1) * (0 * 1) = -\frac{1}{4}$$

3. *Pour tout ensemble E, la réunion et l'intersection dasn $\mathcal{P}(E)$ sont associatives.*
4. *La loi $\oplus$ définie par : $\forall x \in \mathbb{R} : x \oplus y = x + y - 1$dans $\mathbb{R}$ est associative. En effet, pour $x, y, z \in \mathbb{R}$, on a :*

$(x \oplus y) \oplus z = (x+y-1) \oplus z = (x+y-1)+z-1 = x+y+z-1-1 = x+y+z-2$

d'autre part :

$x \oplus (y \oplus z) = x \oplus (y+z-1) = x+(y+z-1)-1 = x+y+z-1-1 = x+y+z-2$

ainsi

$$(x \oplus y) \oplus z = x \oplus (y \oplus z)$$

la loi $\oplus$ est donc associative.

5. *La loi $\otimes$ définie par : $\forall x \in \mathbb{R} : x \otimes y = x + y - xy$ dans $\mathbb{R}$ est associative. En effet, pour $x, y, z \in \mathbb{R}$, on a :*

$(x \otimes y) \otimes z = (x+y-xy) \otimes z = (x+y-xy)+z-(x+y-xy)z = x+y+z-xy-xz-yz+xyz$

d'autre part :

$x \otimes (y \otimes z) = x \otimes (y+z-yz) = x+(y+z-yz)-x(y+z-yz) = x+y+z-xy-xz-yz+xyz$

ainsi :

$$(x \otimes y) \otimes z = x \otimes (y \otimes z)$$

la loi $\otimes$ est donc associative.

Exercice 6.2. *Montrer que la composition des applications est associative.*
Notation 6.1.1. *Soit E un ensemble, $*$, $\cdot$ ou $+$ une loi associative. On note :*

$$\overset{n}{\underset{i=1}{*}} x_i = x_1 * x_2 * ... * x_n$$

$$\prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdot ... \cdot x_n \text{ ou simplement } \prod_{i=1}^{n} x_i = x_1 x_2 ... x_n$$

$$\sum_{i=1}^{n} x_i = x_1 + x_2 + ... + x_n$$

$$x^n = x * x * ... * x \qquad n \text{ facteurs}$$

$$x^n = xx...x \qquad n \text{ facteurs}$$

$$nx = x + x + ... + x \qquad n \text{ termes}$$

Définition 6.1.4 (commutativité)**.** *Une lci dans un ensemble E est dite **commutative** si et seulement si :*

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

On dit que deux éléments x et y d'un ensemble E muni d'une lci $*$ commutent (ou sont permutables) si et seulement si $x * y = y * x$.
Exemple 6.1.3. *1. L'addition et la multiplication dans $\mathbb{R}$ sont commutatives.*

2. La soustraction dans $\mathbb{R}$ n'est pas commutative.

Exercice 6.3. *La loi $\oplus$ définie par dans $\mathbb{R}$: $\forall x \in \mathbb{R} : x \oplus y = x + y - 1$ est-elle commutative ?*

La loi $\otimes$ définie dans $\mathbb{R}$ par : $\forall x \in \mathbb{R} : x \otimes y = x + y - xy$ est-elle commutative ?

Solution Soient $x, y \in \mathbb{R}$:

$$x \oplus y = x + y - 1 = y + x - 1 = y \oplus x$$

ainsi $\oplus$ est commutative.

On a aussi :

$$x \otimes y = x + y - xy = y + x - xy = y + x - yx = y \otimes x$$

donc $\otimes$ est commutative.
Définition 6.1.5 (Eléments réguliers)**.** *Soit E un ensemble muni d'une lci $*$, $a \in E$*

1. On dit que a est régulier (ou simplifiable) à gauche pour $*$ si et seulement si :

$$\forall (x, y) \in E^2, (a * x = a * y \implies x = y)$$

2. *On dit que a est régulier (ou simplifiable) à droite pour $*$ si et seulement si :*

$$\forall (x,y) \in E^2, (x * a = y * a \implies x = y)$$

3. *On dit que a est **régulier** (ou **simplifiable**) si et seulement si a est régulier à gauche et régulier à droite pour $*$, c'est-à-dire :*

$$\forall (x,y) \in E^2, \begin{cases} a * x = a * y \implies x = y \\ x * a = y * a \implies x = y \end{cases}$$

Exemple 6.1.4. *1. Dans $\mathbb{R}$, tout élément est régulier pour l'addition.*

2. Les éléments de réguliers $\mathbb{R}$ pour la multiplication sont les réels différents de 0.

Proposition 6.1.1. *Soit E un ensemble muni d'une loi associative et commutative notée $+$, alors :*

1.

$\forall n \in \mathbb{N}, \forall (x_1, ..., x_n), (y_1, ..., y_n) \in E^n,$
$(x_1 + y_1) + (x_2 + y_2) + ... + (x_n + y_n) = (x_1 + x_2 + ... + x_n) + (y_1 + y_2 + ... + y_n)$

on note

$$\sum_{i=1}^{n} (x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$$

2. $\forall (n,p) \in (\mathbb{N}^*)^2$, $\begin{pmatrix} x_1 1 & x_1 2 & \cdots & x_1 p \\ x_2 1 & x_2 2 & \cdots & x_2 p \\ \vdots & \vdots & \vdots & \vdots \\ x_n 1 & x_n 2 & \cdots & x_n p \end{pmatrix} \in E$ *on a :*

$(x_1 1 + x_1 2 + ... + x_1 p) + (x_2 1 + x_2 2 + ... + x_2 p) + ... + (x_n 1 + x_n 2 + ... + x_n p) =$
$(x_1 1 + x_2 1 + ... + x_n 1) + (x_1 2 + x_2 2 + ... + x_n 2) + ... + (x_1 p + x_2 p + ... + x_n p)$

ce qui se note :

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{p} x_i j \right) = \sum_{j=1}^{p} \left(\sum_{i=1}^{n} x_i j \right)$$

3.

$$\forall n \in \mathbb{N}^*, \forall \sigma \in S_n, \forall (x_1, ..., x_n) \in E^n, \sum_{i=1}^{n} x_{\sigma(i)} = \sum_{i=1}^{n} x_i$$

c'est-à-dire que si on change l'ordre des éléments $x_1, ..., x_n$, la somme reste inchangée.

La preuve se fait très facilement par récurrence.

Définition 6.1.6 (Elément neutre). *Soit E un ensemble muni d'une lci $*$, $e \in E$: On dit que e est **neutre à gauche** pour $*$ si et seulement si :*

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

*On dit que e est **neutre à droite** pour $*$ si et seulement si :*

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

*On dit que e est **neutre** pour $*$ si et seulement si e est neutre à gauche et à droite pour $*$, c'est à dire :*

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

Exemple 6.1.5. 0 *est neutre pour $+$ dans $\mathbb{R}$.*

1 *est neutre pour $\cdot$ dans $\mathbb{R}$.*

Id_E est neutre pour la composition des applications de E dans E .
Exercice 6.4. *La loi $\oplus$ définie par dans $\mathbb{R}$: $\forall x \in \mathbb{R} : x \oplus y = x + y - 1$ admet-elle un élément neutre ?*

La loi $\otimes$ définie dans $\mathbb{R}$ par : $\forall x \in \mathbb{R} : x \otimes y = x + y - xy$ admet-elle un élément neutre ?

Solution Cherchons un élément neutre pour $\oplus$, un tel élément (qu'on note e), s'il existe, doit vérifier :

$$\forall x \in \mathbb{R}, x \oplus e = e \oplus x = x$$

Puisque $\oplus$ est commutative, il suffit de vérifier une des deux égalités précédentes, considérons l'équation :

$$x \oplus e = x$$

on a alors, pour $x \in \mathbb{R}$:

$$\begin{aligned} x \oplus e = x &\iff x + e - 1 = x \\ &\iff e - 1 = 0 \\ &\iff e = 1 \end{aligned}$$

Donc $\oplus$ admet un élément neutre qui est 1.

Voyons maintenant le cas de $\otimes$, comme $\otimes$ est aussi commutative, il suffit de traiter l'équation :

$$x \otimes f = x$$

On a alors, pour $x \in \mathbb{R}$:

$$\begin{aligned} x \otimes f = x &\iff x + f - xf = x \\ &\iff f - xf = 0 \\ &\iff f(1-x) = 0 \end{aligned}$$

si $x \neq 1$ on obtient $f = 0$, si $x = 1$ tout élément f de $\mathbb{R}$ vérifie l'équation, donc en particulier $f = 0$, ainsi, $\otimes$ admet un neutre, qui est 0.

Proposition 6.1.2 (unicité de l'élément neutre)**.** *Si e, e' sont deux éléments neutres dans E alors $e = e'$*

Preuve e est neutre, donc pour tout élément $x \in E$ on a :

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

En particulier pour $x = e'$, on a :

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

De même, e' est neutre donc :

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

En particulier pour $x = e$, on a :

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

Donc $e = e'$

Définition 6.1.7 (Eléments symétrisable)**.** *Soit E un ensemble muni d'une lci $*$ admettant un élément neutre e.*

Un élément x de E est dit symétrisable pour $*$ si et seulement s'il existe un élément y de E tel que :

$$x * y = y * x * e$$

Un tel élément y est appelé un symétrique de x pour $*$.

Proposition 6.1.3 (unicité du symétrique d'un élément)**.** *Soit E un ensemble muni d'une lci associative et admettant un élément neutre, et soit $x \in E$. Si x est symétrisable pour $*$ alors x admet un et un seul symétrique pour $*$.*

Preuve On suppose que x admet deux symétriques x' et x''.

x' est un symétrique de x implique que

$$x' * x = e$$

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

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

x'' est un symétrique de x implique que :

$$x'' * x = e$$

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

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

On a donc $x' = x''$

Notation 6.1.2. *Soient E un ensemble muni d'une lci $*$ associative et admettant un élément neutre, x un élément de E symétrisable pour $*$. Le symétrique de x est noté x', $sym(x)$ ou x^{-1}, il est aussi appelé inverse de x. Lorsque la loi est notée $+$, le symétrique de x (s'il existe) est noté $-x$ et appelé opposé de x.*

Proposition 6.1.4 (le symétrique du composé)**.** *Soient E un ensemble muni d'une lci associative et admettant un élément neutre, $x, y \in E$. Si x et y sont symétrisables pour $*$ alors $x * y$ est symétrisable pour $*$ et*

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

Preuve

Définition 6.1.8 (Distributivité)**.** *Soient E un ensemble, $\top$, $*$ deux lci dans E.*

On dit que $\top$ est distributive à gauche (resp. à droite) sur (ou : pour ou par rapport à) $*$ si et seulement si :

$$\forall (x, y, z) \in E^3, x \top (y * z) = (x \top y) * (x \top z)$$

resp.

$$\forall (x, y, z) \in E^3, (y * z) \top x = (y \top x) * (z \top x)$$

On dit que $\top$ est distributive sur $*$ si et seulement si $\top$ est distributive à gauche et distributive à droite sur $*$.

Exemple 6.1.6. *La multiplication est distributive sur l'addition.*

L'intersection est distributive sur la réunion.

Exercice 6.5. *Soient les lci $\oplus$ et $\otimes$ définies sur $\mathbb{R}$ par :*

$$\forall x \in \mathbb{R} : x \oplus y = x + y - 1$$

$$\forall x \in \mathbb{R} : x \otimes y = x + y - xy$$

Montrer que $\otimes$ est distributive par rapport à $\oplus$.

Solution Soient $x, y, z \in \mathbb{R}$, $\otimes$ étant commutative, il suffit de vérifier qu'elle distributive à gauche (ou à droite) :

$$x\otimes(y\oplus z) = x\otimes(y+z-1) = x+(y+z-1)-x(y+z-1) = x+y+z-1-xy-xz+x = 2x+y+z-xy-xz-1$$

d'autre part :

$$(x\otimes y)\oplus(x\otimes z) = (x+y-xy)\oplus(x+z-xz) = (x+y-xy)+(x+z-xz)-1 = 2x+y+z-xy-xz-1$$

ainsi

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$$

Donc $\otimes$ est distributive par rapport à $\oplus$.

Exercice 6.6. *1. Montrer que la loi de composition des applications est distributive par rapport à l'addition des applications.*

2. Montrer que la multiplication des applications est distributive par rapport à l'addition des applications.

6.2 Groupes, Anneaux, Corps

Définition 6.2.1 (Groupe)**.** *On dit qu'un ensemble G muni d'une lci $*$ est un groupe si et seulement si :*

1. *$*$ est associative.*
2. *G admet un neutre pour $*$.*
3. *Tout élément de G admet un symétrique pour $*$.*

Si de plus $*$ est commutative, on dit que G est un groupe abélien (ou groupe commutatif)

Exemple 6.2.1. $\mathbb{R}^2 = \{(x, y)/x \in \mathbb{R}, y \in \mathbb{R}\}$*, si (x, y), (x', y') sont deux éléments de $\mathbb{R}^2$*

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

$\mathbb{R}^2$ muni de l'addition des couples est un groupe commutatif.

Exemple 6.2.2. *L'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ noté $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est un groupe commutatif pour l'addition des applications. Soient f et g deux éléments de $\mathcal{F}(\mathbb{R}, \mathbb{R})$, l'application $f + g$ est définie en donnant l'image de tout nombre réel x par $f + g$, par :*

$$\forall x \in \mathbb{R}, (f + g)(x) = f(x) + g(x)$$

Exercice 6.7. *Soient les lci $\oplus$ et $\otimes$ définies sur $\mathbb{R}$ par :*

$$\forall x \in \mathbb{R} : x \oplus y = x + y - 1$$

$$\forall x \in \mathbb{R} : x \otimes y = x + y - xy$$

Montrer que $\oplus$ confère à $\mathbb{R}$ une structure de groupe commutatif.

Qu'en est-il de $\otimes$?

Solution On a montré précédemment que $\oplus$ est associative, commutative et qu'elle admet un élément neutre qui est 1, pour montrer qu'elle confère à $\mathbb{R}$ une structure de groupe, il reste à montrer que tout élément est symétrisable.

Soit $x \in \mathbb{R}$, existe-t-il un élément $x' \in \mathbb{R}$ tel que $x \oplus x' = x' \oplus x = 1$? $\oplus$ étant commutative, il suffit de vérifier l'égalité $x \oplus x' = 1$

$$\begin{aligned} x \oplus x' = 1 &\iff x + x' - 1 = 1 \\ &\iff x + x' = 2 \\ &\iff x' = 2 - x \end{aligned}$$

ainsi, tout élément $x \in \mathbb{R}$ admet un symétrique qui est $x' = 2 - x$. Donc, d'après ce qui précède, $(\mathbb{R}, \oplus)$ est un groupe.

On a aussi montré dans ce qui précède que $\otimes$ est commutative, associative, et qu'elle admet un neutre qui est 0, étudions maintenant l'existence des éléments symétriques de chaque élément $x \in \mathbb{R}$, $\otimes$ étant commutative, il suffit d'étudier l'existence des symétriques à droite ou à gauche. soit $x \in \mathbb{R}$ existe-t-il $x^- \in \mathbb{R}$ tel que $x \otimes x^- = 0$?

$$\begin{aligned} x \otimes x^- = 0 &\iff x + x^- - xx^- = 0 \\ &\iff x + x^-(1 - x) = 0 \\ &\iff x^-(1 - x) = -x \end{aligned}$$

Si $x \neq 1$ on obtient

$$x^- = \frac{-x}{1 - x}$$

si $x = 1$ l'équation précédente deviens $0 = -1$, ce qui est impossible. Ainsi, les éléments symétrisables pour $\otimes$ sont les réels différents de 1, donc $(\mathbb{R}, \otimes)$ n'est pas un groupe.

Définition 6.2.2 (Sous-groupe)**.** *Soit $(G, *)$ un groupe. Une partie H non vide de G est appelée un sous-groupe de G si la restriction de $*$ à H lui confère une structure de groupe.*

Remarque 6.2.1. *Comme dans G, tout élément est simplifiable, alors l'élément neutre de tout sous-groupe H de G coïncide avec celui de G*

Proposition 6.2.1. *Soit $(G, *)$ un groupe et H un sous-ensemble non vide de G, alors H est un sous-groupe de G si et seulement si :*

$$\forall x, y \in H, x * y \in H$$

$$\forall x \in H, x^{-1} \in H$$

Ce qui est aussi équivalent à :

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

Preuve : Exercice

Exemple 6.2.3. *Pour tout groupe G d'élément neutre e, le singleton $\{e\}$ est un sous-groupe de G.*

Proposition 6.2.2. *Soient G un groupe, $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Preuve

Notons $H = \bigcap_{i\in I} H_i$.

1. pour tout $(x, y) \in G^2$

$$\begin{aligned}(x,y) \in H^2 &\implies (\forall i \in I, x \in H_i \text{ et } y \in H_i)\\ &\implies (\forall i \in I, x * y \in H_i)\\ &\implies x * y \in H\end{aligned}$$

2. $(\forall i \in I, e \in H_i)$ donc $e \in H$
3. Pour tout x de G :

$$\begin{aligned}x \in H &\implies (\forall i \in I, x \in H_i)\\ &\implies (\forall i \in I, x^{-1} \in H_i)\\ &\implies (x^{-1} \in H)\end{aligned}$$

Définition 6.2.3 (Sous-groupe engendré)**.** *Soient $(G, *)$ un groupe et $A \in \mathcal{P}(G)$. L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G, appelé **sous-groupe engendré** par A, et noté $\langle A\rangle$.*

Proposition 6.2.3. *Soient $(G, *)$ un groupe, $A \in \mathcal{P}(G)$, $\langle A\rangle$ est (au sens de l'inclusion) le plus petit sous-groupe de G contenant A.*

Preuve

1. D'après la proposition 6.2.2, $\langle A\rangle$ est un sous-groupe de G contenant A.
2. Réciproquement, soit H un sous-groupe de G contenant A. Par définition de $\langle A\rangle$, on a $\langle A\rangle \subset H$, donc $\langle A\rangle$ est inclus dans tout sous-groupe de G contenant A.

Définition 6.2.4 (groupe monogène)**.** *Un groupe G est dit **monogène** si et seulement s'il existe $a \in G$ tel que $G = \langle a\rangle$.*

*Si G est un groupe monogène, on appelle **générateur** de G tout élément a de G tel que $G = \langle a\rangle$.*

*Un groupe G est dit **cyclique** si et seulement s'il est monogène et fini.*

Exemple 6.2.4. *$(\mathbb{Z}, +)$ est un groupe monogène, dont un générateur est 1 (ou -1).*

$(\mathbb{Z}/3\mathbb{Z}, +)$ est un groupe monogène, dont un générateur est, par exemple, 2.

$(\mathbb{R}, +)$ n'est pas un groupe monogène.

Définition 6.2.5. *Etant donnés deux groupes $(G, *)$ et $(G', \perp)$, on appelle **morphisme** de groupes (ou homomorphisme) de $(G, *)$ dans $(G', \perp)$ toute application $f : G \longrightarrow G'$ telle que :*

$$\forall (x, y) \in G^2, f(x * y) = f(x) \perp f(y)$$

*Si de plus f est une bijection de G dans G', alors on dit que f est un **isomorphisme** de groupes.*

*Un **endomorphisme** d'un groupe $(G, *)$ est un morphisme de groupes de $(G, *)$ dans $(G, *)$.*

*Un **automorphisme** d'un groupe $(G, *)$ est un endomorphisme bijectif d'un groupe $(G, *)$.*

Exemple 6.2.5. *La fonction logarithme $ln : x \longmapsto ln(x)$ est un isomorphisme de $((R)_+^*, \cdot)$ dans $(\mathbb{R}, +)$.*

Proposition 6.2.4. *Soient deux groupes $(G, *)$ et $(G', \top)$, et $f : G \longrightarrow G'$ un morphisme de groupes, Si e est l'élément neutre de G et e' l'élément neutre de G' alors $f(e) = e'$, et pour tout élément x de G, on a $f(x^{-1}) = [f(x)]^{-1}$.*

Preuve

1. Montrons que $f(e) = e'$:

$$\begin{aligned} f(e) \top f(e) &= f(e * e) \\ &= f(e) \\ &= f(e) \top e' \end{aligned}$$

Donc on a :

$$\begin{aligned} f(e) \top f(e) &= f(e) \top e' \\ (f(e)^{-1} \top f(e)) \top f(e) &= (f(e)^{-1} \top f(e)) \top e' \\ e' \top f(e) &= e' \top e' \\ f(e) &= e' \end{aligned}$$

2. Montrons que $f(x^{-1}) = [f(x)]^{-1}$

$$\begin{aligned} e &= x * x^{-1} \\ f(e) &= f(x * x^{-1}) \\ e' &= f(x) \top f(x^{-1}) \end{aligned}$$

même calcul pour la deuxième égalité.
Donc $f(x^{-1}) = [f(x)]^{-1}$.

Définition 6.2.6 (noyau d'un morphisme)**.** *Soient $(G, *)$, $(G', \perp)$ deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes. On appelle noyau de f l'ensemble des éléments de G qui ont pour image l'élément neutre e' de G'. On note*

$$\ker(f) = \{x \in G / f(x) = e'\}$$

Théorème 6.2.1. *Le noyau d'un morphisme de groupes $f : G \longrightarrow G'$ est un sous-groupe de G.*

Preuve

Pour tout x et y de $\ker(f)$, on a :

$$\begin{aligned} f(x * y^{-1}) &= f(x) \perp f(y^{-1}) = f(x) \perp [f(y)]^{-1} \\ &= e' \perp e' = e' \end{aligned}$$

donc $x * y^{-1} \in \ker(f)$

Théorème 6.2.2. *Soit $f : G \longrightarrow G'$ un morphisme de groupes, alors f est injective si et seulement si $\ker(f) = \{e\}$.*

Preuve

– f est injective $\implies \ker(f) = \{e\}$
Pour tout x appartenant à $\ker(f)$ on a $f(x) = e'$ donc $f(x) = f(e)$, or f étant injective on obtient $x = e$ donc $\ker(f) = \{e\}$ (l'inclusion réciproque étant évidente)

– $\ker(f) = \{e\} \implies f$ est injective.
Pour x, y dans G,

$$f(x) = f(y) \implies f(x) \perp [f(y)]^{-1} = e'$$

or f est un morphisme alors

$$f(x) \perp [f(y)]^{-1} = f(x * y^{-1}$$

$$\begin{aligned} f(x) \perp [f(y)]^{-1} = f(x * y^{-1} = e' &\implies x * y^{-1} \in \ker(f) \\ &\implies x = y \end{aligned}$$

Définition 6.2.7 (image d'un morphisme)**.** *Soient $(G, *)$, $(G', \perp)$ deux groupes, $f : G \longrightarrow G'$ un morphisme de groupes. On appelle image de f l'ensemble des images, $f(G)$. On note :*

$$\mathrm{Im}(f) = \{y \in G' / \exists x \in G : y = f(x)\} = f(G)$$

Théorème 6.2.3. *L'image d'un morphisme de groupes $f : G \longrightarrow G'$ est un sous-groupe de G.*

Preuve : Exercice

Théorème 6.2.4. *Soit $f : G \longrightarrow G'$ un morphisme de groupes, alors f est surjective si et seulement si $\mathrm{Im}(f) = G'$.*

Preuve : Exercice

Proposition 6.2.5 (Transfert de la structure de groupe)**.** *Soient $(G, *)$ un groupe et G' un ensemble muni d'une lci $\perp$. S'il existe une application bijective $f : G \longrightarrow G'$ telle que :*

$$\forall x, y \in G, f(x * y) = f(x) \perp f(y)$$

alors $(G', \perp)$ est un groupe.

Preuve : Soit f de $(G, *)$ dans $(G', \perp)$ une application vérifiant les hypothèses de la proposition, notons e l'élément neutre de G.

Soient $x, y, z \in G'$, chacun de ces éléments possède un et un seul antécédent dans G puisque l'application f est bijective, soient $X = f^{-1}(x)$, $Y = f^{-1}(y)$ et $Z = f^{-1}(z)$.

1. $\perp$ associative :

$$\begin{aligned}(x \perp y) \perp z &= (f(X) \perp f(Y)) \perp f(Z) = f(X * Y) \perp f(Z) \\ &= f((X * Y) * Z) = f(X * (Y * Z)) \\ &= f(X) \perp f(Y * Z) = f(X) \perp (f(Y) \perp F(Z)) \\ &= x \perp (y \perp z)\end{aligned}$$

2. G' possède un neutre pour $\perp$

$$\begin{cases} x \perp f(e) = f(X) \perp f(e) = f(X * e) = f(X) = x \\ f(e) \perp x = f(e) \perp f(X) = f(e * X) = f(X) = x \end{cases}$$

3. Tous les éléments de G' sont symétrisables :
   Soit X' le symétrique de X, on a :

$$\begin{cases} x \perp f(X') = f(X) \perp f(X') = f(X * X') = f(e) \\ f(X') \perp x = f(X') \perp f(X) = f(X' * X) = f(e) \end{cases}$$

Définition 6.2.8 (Structure d'anneau)**.** *Soit A un anneau muni de deux lois de composition internes. On dit que A est un anneau si :*
– *La première loi définit sur A une structure de groupe commutatif.*
– *La seconde loi est associative.*
– *La seconde loi est distributive par rapport à la première.*

Dans un anneau, on note habituellement la première loi additivement (groupe commutatif) et la seconde multiplicativement.

Alors $(A, +, \cdot)$ *est un anneau si :*

1. $(A, +)$ *est un groupe commutatif (élément neutre noté* 0*).*
2. *La multiplication dans* A *est associative et distributive par rapport à l'addition.*

Si la multiplication est commutative, ont dit que l'anneau est commutatif, et si elle a un élément neutre (noté généralement 1*) on dit que l'anneau est unitaire.*

Définition 6.2.9 (Sous-anneau)**.** *Soit* A *un anneau et* H *une partie non vide de* A*, alors* H *est un sous-anneau de* A *si et seulement si :*

1. $\forall x, y \in H, x - y \in H$
2. $\forall x, y \in H, xy \in H$

La première propriété équivaut à dire que $(H, +)$ est un sous-groupe commutatif de A. La seconde équivaut à dire que la restriction de la multiplication de A à H est une loi de composition interne.

Définition 6.2.10. *Soit* $A \neq \{0\}$ *un anneau. S'il existe deux éléments* a *et* b *de* A *tels que :*

$$a \neq 0 \text{ et } b \neq 0, \text{ et } ab = 0$$

On dit alors que a *est diviseur de zéro à gauche, et que* b *est diviseur de zéro à droite de l'anneau* A*. On dit aussi que* a *et* b *sont des diviseurs de zéro.*

Dans le cas où l'anneau est commutatif, tout diviseur de zéro d'un côté est diviseur de zéro de l'autre.

Définition 6.2.11 (Anneau intègre)**.** *On dit qu'un anneau est intègre s'il est distinct de* $\{0\}$ *et s'il ne possède pas de diviseurs de zéro.*

Exemple 6.2.6.
1. $(\mathbb{Z}, +, \cdot)$ *est intègre.*
2. $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ *n'est pas intègre*

Calculs dans un anneau

Soit $(A, +, \cdot)$ un anneau unitaire. On note :
– 0 le neutre de $+$
– $-x$ le symétrique d'un élément x de A pour $+$.
– 1 (ou 1_A) le neutre de $\cdot$

On montre facilement les formules suivantes :

1. $\forall x \in A, 0 \cdot x = x \cdot 0 = 0$ (On dit que 0 est absorbant pour $\cdot$.
2. $\forall x \in A, (-1_A) \cdot x = x \cdot (-1_A) = -x$
3. $\forall (x, y) \in A^2, \begin{cases} (-x)y = x(-y) = -xy \\ (-x)(-y) = xy \end{cases}$

4. $\forall (x,y,z) \in A^3, \begin{cases} (x-y)z = xz - yz \\ z(x-y) = zx - zy \end{cases}$
5. $\forall n \in \mathbb{N}^*, \forall a \in A, (1_A - a)$,

$$\left(\sum_{k=0}^{n-1} a^k\right) = \left(\sum_{k=0}^{n-1} a^k\right)(1_A - a) = 1_A - a^k$$

6. $\forall p \in \mathbb{N}, \forall a \in A$,

$$(1_A + a)\left(\sum_{k=0}^{2p} (-1_A)^k a^k\right) = \left(\sum_{k=0}^{2p} (-1_A)^k a^k\right)(1_A + a) = 1_A + a^{2p+1}$$

7. $\forall a \in A, \forall n \in \mathbb{N}, \forall (x_1, ..., x_n) \in A^n$,

$$\sum_{k=1}^{n} a x_i = a \sum_{k=1}^{n} x_i \text{ et } \sum_{k=1}^{n} x_i a = \left(\sum_{k=1}^{n} x_i\right) a$$

8. $\forall n, p \in \mathbb{N}^*, \forall (x_1, ..., x_n) \in A^n, \forall (y_1, ..., y_p) \in A^p$,

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{p} x_i y_j\right) = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_i y_j\right) = \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{p} y_j\right)$$

Notation 6.2.1. *Soit $(A, +, \cdot)$ un anneau unitaire. Pour tout $(n, x) \in \mathbb{Z} \times A$, on a :*

$$\begin{cases} nx = x + x + ... + x \text{ (n termes) si } n \in \mathbb{N} \\ nx = 0 \text{ si } n = 0 \\ nx = -(-n)x \text{ si } n \in \mathbb{Z}^*_- \end{cases}$$

Les formules suivantes sont faciles à démontrer :

1. $\forall (n,p) \in \mathbb{Z}, \forall x \in A, (n+p)x = nx + px$.
2. $\forall n \in \mathbb{Z}, \forall x \in A, n(-x) = (-n)x$, noté $-nx$.
3. $\forall n \in \mathbb{Z}, \forall (x,y) \in A^2, \begin{cases} n(x+y) = nx + ny \\ n(x-y) = nx - ny \end{cases}$
4. $\forall (n,p) \in \mathbb{Z}^2, \forall x \in A, (np)x = n(px)$.
5. $\forall n \in \mathbb{Z}, \forall (x,y) \in A^2, n(xy) = (nx)y = x(ny)$.
6. $\forall n \in \mathbb{Z}, \forall x \in A, nx = (n1_A)x = x(n1_A)$.

On note quelquefois n au lieu de $n1_A$, pour $n \in \mathbb{Z}$, s'il n'en résulte pas de confusion.

Définition 6.2.12 (Corps)**.** *On appelle corps un anneau unitaire A où tout élément non nul (différent du neutre pour la première loi) de A est inversible (possède un symétrique pour la deuxième loi).*

Si A est commutatif, on dit que le corps est commutatif.
Exemple 6.2.7. *$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition et la multiplication usuelles sont des corps commutatifs*
Exercice 6.8. *On considère les lci $\oplus$ et $\otimes$ définies sur le corps commutatif $(\mathbb{R}, +, \cdot)$ par :*

$$x \oplus y = x + y - 1$$

$$x \otimes y = x + y - xy$$

1. *Montrer que $(\mathbb{R}, \oplus, \otimes)$ est un anneau commutatif.*
2. *$(\mathbb{R}, \oplus, \otimes)$ est-il un corps ?*

Solution

1. On a montré précédemment que :
   (a) $(\mathbb{R}, \oplus)$ est un groupe commutatif, d'élément neutre 1.
   (b) $\otimes$ est associative et commutative.
   (c) $\otimes$ est distributive par rapport à $\oplus$.

   Ce qui donne que $(\mathbb{R}, \oplus, \otimes)$ est un anneau commutatif.
2. On a aussi montré que $\otimes$ admet un neutre qui est 0, et que tout élément de $\mathbb{R}$ sauf 1, qui est le neutre de $\oplus$, admet un symétrique pour $\otimes$, donc $(\mathbb{R}, \oplus, \otimes)$ est un corps.

Définition 6.2.13 (Sous-corps)**.** *Soit K un corps et H une partie non vide de K. On dit que H est un sous-corps de K si les restrictions à H des deux loi de K confèrent à H la structure de corps. C'est à dire si H est un sous-anneau de K, et le symétrique x^{-1} de tout élément x de H appartient à H.*

6.3 Exercices

Exercice 6.9. *Définir sur chacun des ensembles suivants une lci $+$ et une lci $\cdot$. Etudier les structures algébriques possibles que ces lois confèrent à ces ensembles, pour une loi et pour les deux lois.*
– *$\mathbb{R}^2$, $\mathbb{R}^3$, $\mathbb{R}^4$, $\mathbb{R}^5$, $\mathbb{R}^n$.*
– *L'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$: $\mathcal{F}(\mathbb{R}, \mathbb{R})$.*
– *L'ensemble des polynômes à une indéterminée à coefficients réels : $\mathbb{R}[X]$.*
– *L'ensemble des suites réelles : S.*

Exercice 6.10. *1. Chacun des ensembles suivants est un sous ensemble d'un ensemble de l'exercice précédent. Les lci de l'exercice précédent sont-elles internes dans ces sous-ensembles ?*

2. *Lesquels sont des sous-groupes, sous-anneaux, sous-corps, des groupes, anneaux, corps correspondants ?*
   - *(a)* $E_1 = \{(x, y, z) \in \mathbb{R}^3 / x + y + z = 0\}$.
   - *(b)* $E_2 = \{(x, y, z, t) \in \mathbb{R}^4 / x = 2x = -t\}$.
   - *(c)* $E_3 = \{(x, y, z, t) \in \mathbb{R}^4 / z + t = 0\}$.
   - *(d)* $E_4 = \{(x, y, z) \in \mathbb{R}^3 / x = -2y$ *et* $z = y\}$.
   - *(e)* $E_5 = \{(x, y, z, t) \in \mathbb{R}^4 / x + 2y - t = 0$ *et* $2z - t = 0\}$.
   - *(f)* $E_6 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 / x_1 + x_2 + x_3 + x_4 = 0\}$.
   - *(g) L'ensemble des applications paires de* $\mathbb{R}$ *dans* $\mathbb{R}$.
   - *(h) L'ensemble des applications impaires de* $\mathbb{R}$ *dans* $\mathbb{R}$.
   - *(i) L'ensemble des polynômes de* $\mathbb{R}(X)$ *de degré* 5.
   - *(j) L'ensemble des polynômes de* $\mathbb{R}(X)$ *de degré inférieur ou égal à* 5.
   - *(k) L'ensemble des suites réelles convergentes.*
   - *(l) L'ensemble des suites réelles bornées.*

Exercice 6.11. *Soit* $(G, *)$ *un groupe d'élément neutre* e.

Montrer que si on a $\forall x \in G, x * x = e$ *alors* G *est abélien.*

Exercice 6.12. *Soit* D *un ensemble muni d'une lci associative* $*$.

1. *Montrer que s'il existe un élément neutre à droite* e *et un élément neutre à gauche* f*, alors* $e = f$.
2. *On pose* $a * D * a = \{a * x * a / x \in D\}$. *On suppose qu'il existe dans* D *un élément* a *tel que* $a * D * a = D$. *Montrer alors que* D *admet un élément neutre.*

Exercice 6.13. *Soit* G *un groupe multiplicatif d'élément neutre* e *et* H *un sous-groupe de* G.

1. *Montrer que les relations* $\mathcal{R}'$ *et* $\mathcal{R}''$*, définies sur* G *par :*

$$x\mathcal{R}'y \iff x^{-1}y \in H, \qquad x\mathcal{R}''y \iff xy^{-1} \in H$$

   sont des relations d'équivalence.

2. *On appelle classes à gauche modulo* H *les classes d'équivalence définies par* $\mathcal{R}'$*, et classes à droite modulo* H *les classes d'équivalence définies par* $\mathcal{R}''$.

   Donner une définition simple des classes modulo H *contenant un élément* x *donné de* G.

   Montrer qu'il existe au moins une bijection de H *sur toute classe à gauche (resp. à droite).*

3. *Si G est un groupe fini ayant n élément, H est un groupe fini. Montrer que le nombre p des éléments de H est un diviseur de n.*

Exercice 6.14. *A tout sous-groupe H d'un groupe G, on peut associer une relation d'équivalence $(x\mathcal{R}y \iff xy^{-1} \in H)$. Nous allons étudier la relation associé dans le groupe $(\mathbb{Z}, +)$ à tout sous-groupe $n\mathbb{Z}$ (ensemble des multiples d'un entier n), appelée congruence modulo n ($n > 0$).*

Pour $x, y \in \mathbb{Z}$, on dit que x est congru à y modulo n (on notera $x \equiv y[n]$) si $x - y$ est un élément de $n\mathbb{Z}$.

1. *Montrer que la congruence modulo n est une relation d'équivalence dans $\mathbb{Z}$.*
2. *Montrer que chaque classe C_a contient un élément unique a' tel que*

$$0 \leqslant a' < n$$

3. *Montrer que l'ensemble quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ comprend n éléments (appelés entiers modulo n) et qu'il a une structure d'anneau commutatif unitaire.*