Chapitre 4

Structure algébrique

4.1 Lois de composition internes

Définition 4.1. *Soit E un ensemble non vide. Une loi de composition interne $*$ sur E est une application de $E \times E$ dans E qui a tout couple (a, b) de $E \times E$ associe un élément de E noté $a * b$:*

$$\begin{array}{rcl} * : E \times E & \longrightarrow & E \\ (a, b) & \longmapsto & a * b \end{array}$$

Exemples 4.1.

— *les opérations usuelles $+$ et $\times$ constituent des lois de composition internes sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, ...*

— *Soit $*$ définie sur $\mathbb{Q}$ par :*

$$a * b = \frac{a+b}{2}$$

alors $*$ est une loi de composition interne.

— *Soit $*$ définie sur $\mathbb{R}$ par :*

$$a * b = \frac{1}{a+b}$$

alors $*$ n'est pas une loi de composition interne car $(-1, 1) \in \mathbb{R} \times \mathbb{R}$. n'admet pas une image.

4.2 Propriétés des opérations internes

4.2.1 Associativité

Définition 4.2. *On dit que $*$ est associative si :*

$$\forall (a,b,c) \in E^3 : a * (b * c) = (a * b) * c$$

Exemple 4.1. *Soit $*$ une loi de composition interne définie sur $\mathbb{R}$ par :*

$$a * b = a + b - 1$$

on a

$$\begin{aligned} (a * b) * c &= (a + b - 1) + c - 1 \\ &= a + b + c - 2 \text{.....(1)} \\ a * (b * c) &= a + (b + c - 1) - 1 \\ &= a + b + c - 2 \text{.....(2)} \end{aligned}$$

lorsque $(1) = (2)$ alors $*$ est associative.

4.2.2 Commutativité

Définition 4.3. *On dit que $*$ est commutative si :*

$$\forall (a,b) \in E^2 : a * b = b * a$$

Exemple 4.2. *Soit $*$ une loi de composition interne définie sur $\mathbb{R}$ par :*

$$a * b = a + b - 1$$

on a

$$\begin{aligned} a * b &= a + b - 1 \\ &= b + a - 1 \\ &= b * a \end{aligned}$$

Alors $*$ est commutative.

4.2.3 Élément neutre

Définition 4.4. *La loi de composition interne $*$ admet sur E un élément neutre si :*

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

Remarque 4.1. *L'élément neutre, s'il existe, il est unique. En effet , soit e' un autre élément neutre pour $*$, alors*

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

Exemple 4.3. *Soit $*$ une loi de composition interne définie sur $\mathbb{R}$ par :*

$$a * b = a + b - 1$$

on a

$$\begin{aligned} a * e = a &\implies a + e - 1 = a \\ &\implies e = 1 \end{aligned}$$

Alors $e = 1$ est un élément neutre.

4.2.4 Élément symétrique

Définition 4.5. *On suppose que E admet un élément neutre e pour $*$. Soient a et a' deux éléments de E. On dit que a' est symétrique de a (pour la loi $*$) si :*

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

Exemple 4.4. *Soit $*$ une loi de composition interne définie sur $\mathbb{R}$ par :*

$$a * b = a + b - 1$$

on a

$$\begin{aligned} a * a' = 1 &\implies a + a' - 1 = 1 \\ &\implies a' = (2 - a) \in \mathbb{R} \end{aligned}$$

Alors $a' = 2 - a$ est un élément symétrique.

4.2.5 Distributivité

Définition 4.6. *Étant données deux lois de composition internes $*$ et $\top$ définies sur E.*

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

$$\forall (a,b,c) \in E^3 : a\top(b*c) = (a\top b)*(a\top c)$$

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

$$\forall (a,b,c) \in E^3 : (b*c)\top a = (b\top a)*(c\top a)$$

La loi $\top$ est dite distributive par rapport à la loi $*$ si elle est distributive à la fois à gauche et à droite par rapport à $*$.

Exemple 4.5. *Soit $*$ une loi de composition interne définie sur $\mathbb{R}$ par :*

$$a*b = a+b-1,$$

et soit $\top$ une loi de composition interne définie sur $\mathbb{R}$ par :

$$a\top b = a+b-ab$$

Alors la loi $\top$ est distributive par rapport à $*$. Lorsque $\top$ est commutative alors il se fait de démontrer que $\top$ est distributive à gauche par rapport à la loi $*$.

$$\begin{aligned} a\top(b*c) &= a\top(b+c-1) \\ &= 2a+b+c-ab-ac-1 \text{.....(1)} \\ (a\top b)*(a\top c) &= (a+b-ab)*(a+c-ac) \\ &= 2a+b+c-ab-ac-1 \text{.....(2)} \end{aligned}$$

Lorsque (1) = (2) alors la loi $\top$ est distributive par rapport à la loi $*$.

4.3 Stabilité

Définition 4.7. *Soit E un ensemble muni d'une loi interne $*$. Un sous-ensemble F de E est dit stable pour cette loi interne si et seulement si :*

$$\forall a,b \in F : a*b \in F$$

Exemple 4.6. $\mathbb{N}$ *est un sous-ensemble de $\mathbb{R}$ stable pour les lois de composition internes $+$ et $\times$.*

4.4 Groupe

Définition 4.8. *Soit la loi de composition interne $*$ définie sur un ensemble G, on dit que le couple $(G,*)$ est un groupe si :*

1. *La loi $*$ est associative*

$$\forall (a,b,c) \in G^3 : a*(b*c) = (a*b)*c$$

2. *Il existe un élément neutre e*

$$\exists e \in G,\ \forall a \in G :\ e*a = a*e = a.$$

3. *Toute élément de G a un symétrique*

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

On dit aussi que l'ensemble G possède une structure de groupe pour la loi $*$.

Exemple 4.7. 1. *$(\mathbb{N},\times)$ n'est pas un groupe.*

2. *$(\mathbb{Z},+)$ est un groupe.*

3. *$(\mathbb{Z},\times)$ n'est pas un groupe.*

4. *$(\mathbb{R},+)$ est un groupe.*

4.4.1 Sous-groupe

Définition 4.9. *Soit $(G,*)$ un groupe. Une partie non vide H de G est un sous groupe de G si :*

$$\begin{cases} \forall (a,b) \in H\times H & \Longrightarrow & a*b \in H \text{.....(1)} \\ \forall a \in H & \Longrightarrow & a' \in H \text{.....(2)} \end{cases}$$

Exemple 4.8. *Soit $(\mathbb{Z},+)$ un groupe, alors $3\mathbb{Z}$ est un sous- groupe de $\mathbb{Z}$.*

Ona :

$$\begin{aligned} 3\mathbb{Z} &= \{3z / z \in \mathbb{Z}\} \\ &= \{\ldots,-6,-3,0,3,6,\ldots\} \end{aligned}$$

1. *Soit $a, b \in 3\mathbb{Z}$, alors $\exists z_1 \in \mathbb{Z}$ tel que $a = 3z_1$ et $\exists z_2 \in \mathbb{Z}$ tel que $b = 3z_2$, donc $a + b = 3(z_1 + z_2) \in 3\mathbb{Z}$.*
2. *Soit $a \in 3\mathbb{Z}$, alors $-a = -3z_1 = 3(-z_1) \in 3\mathbb{Z}$.*

De (1) et (2), alors $3\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Théorem 4.1. *Soit H une partie non vide d'un groupe G, alors H est un sous groupe de G si et seulement si :*

$$\forall (a, b) \in H \times H \Longrightarrow a * b' \in H.$$

4.4.2 Homomorphisme

Définition 4.10. *Soient $(G_1, *)$ et $(G_2, \top)$ deux groupes, on appelle homomorphisme de $(G_1, *)$ dans $(G_2, \top)$ toute application $f : G_1 \longrightarrow G_2$ telle que*

$$\forall (x, y) \in G_1^2 : \ f(x * y) = f(x) \top f(y).$$

Remarques 4.1.
— *Si f est bijective, alors on dit que f est isomorphisme.*
— *On appelle endomorphisme un homomorphisme de $(G_1, *)$ dans lui-même.*
— *On appelle automorphisme un endomorphisme bijective de $(G_1, *)$ dans lui-même.*

Exemple 4.9. *L'application*

$$\begin{array}{ccc} f : \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x) = 2^x \end{array}$$

est un homomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}, \times)$ puisque

$$\begin{array}{rcl} \forall (x, y) \in \mathbb{R}^2 : f(x + y) & = & 2^{x+y} \\ & = & 2^x \times 2^y \\ & = & f(x) \times f(y). \end{array}$$

Définition 4.11. *Soient $(G_1, *)$ et $(G_2, \top)$ deux groupes et $f : G_1 \longrightarrow G_2$ est un homomorphisme de $(G_1, *)$ dans $(G_2, \top)$.*

1. *On appelle noyau de f l'ensemble*

$$ker f = \{x \in G_1 \,/\, f(x) = e_2\}.$$

2. *On appelle image de f l'ensemble*

$$Im f = \{f(x) \in G_2 \,/\, x \in G_1\}.$$

Théorem 4.2. *Soit f un homomorphisme de $(G_1, *)$ dans $(G_2, \top)$, alors :*

1. *$ker f$ est un sous-groupe de G_1.*
2. *$Im f$ est un sous-groupe de G_2.*
3. *f est injective $\iff ker f = \{e_1\}$.*
4. *f est surjective $\iff Im f = G_2$.*

4.5 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Fixons $n \geqslant 1$. Rappelons que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p}, \ldots, \overline{n}\}$$

ou $\overline{p}$ désigne la classe d'équivalence de p modulo n. Autrement dit :

$$\overline{p} = \overline{q} \iff p \equiv q \ mod(n)$$

ou encore

$$\overline{p} = \overline{q} \iff \exists k \in \mathbb{Z} : p = q + kn.$$

On définit dans $\mathbb{Z}/n\mathbb{Z}$ deux lois de composition : une additivement et l'autre multiplicativement :

— Addition :

$$\overline{p} + \overline{q} = \overline{p + q}$$

— Multiplication :

$$\overline{p} \cdot \overline{q} = \overline{p \cdot q}$$

Exemple 4.10. *Dans $\mathbb{Z}/6\mathbb{Z}$, on a*

Soient $x, y \in \mathbb{Z}$

$$\begin{aligned} \overline{31} + \overline{46} &= \overline{31+46} \\ &= \overline{77} \\ &= \overline{5} \end{aligned}$$

et

$$\begin{aligned} \overline{31} \cdot \overline{46} &= \overline{31 \cdot 46} \\ &= \overline{1426} \\ &= \overline{4} \end{aligned}$$

Proposition 4.1. $(\mathbb{Z}/n\mathbb{Z}, +)$ *est un groupe commutatif.*

4.6 Anneaux

Définition 4.12. *Soit* A *un ensemble muni de deux lois de composition internes* $*$ *et* $\top$*, on dit que* $(A, *, \top)$ *est un anneau si :*

1. $(A, *)$ *est un groupe commutatif.*
2. *La loi* $\top$ *est associative.*
3. *La loi* $\top$ *est distributive par rapport à la loi* $*$*.*

Remarques 4.2.
— *Un anneau* $(A, *, \top)$ *s'appelle commutatif si l'opération* $\top$ *commutatif.*
— *Un anneau* $(A, *, \top)$ *est unitaire si l'opération* $\top$ *a un élément neutre.*

Exemple 4.11.
1. $(\mathbb{Z}, +, \times)$ *est anneau commutatif et unitaire.*
2. $(\mathbb{R}, +, \times)$ *est anneau commutatif et unitaire.*

4.7 Corps

Définition 4.13. *Soit* $\mathbb{K}$ *un ensemble muni de deux lois de composition internes* $*$ *et* $\top$*, on dit que* $(\mathbb{K}, *, \top)$ *est un corps si :*

1. $(\mathbb{K}, *, \top)$ *est un anneau unitaire.*
2. $(\mathbb{K} - \{e\}, \top)$ *est un, ou e est l'élément neutre de* $*$*.*

Exemple 4.12. *1.* $(\mathbb{Z}, +, \times)$ *n'est pas un corps.*

2. $(\mathbb{R}, +, \times)$ *est est un corps commutatif.*