4 Structures algébriques.

4.1 Lois De Composition Internes

4.1.1 Définition et exemples

Définition 4.1. Soit E un ensemble. Une **loi de composition interne** sur E est une application de $E \times E$ dans E. Si on la note

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

On dit que $(a * b)$ est le composé de a et b pour la loi $*$.

Exemples 4.1. On pose que $E = \mathbb{Z}$

- ☞ L'addition définie par :

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\longmapsto a + b, \end{aligned}$$

est une loi de composition interne sur $\mathbb{Z}$.

- ☞ L'addition définie par :

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\longmapsto a - b, \end{aligned}$$

est une loi de composition interne sur $\mathbb{Z}$.

☞ L'addition définie par :

$$\begin{aligned}\mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z}\\ (a,b) &\longmapsto a \times b,\end{aligned}$$

est une loi de composition interne sur $\mathbb{Z}$.

☞ L'addition définie par :

$$\begin{aligned}\mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z}\\ (a,b) &\longmapsto \frac{a}{b},\end{aligned}$$

n'est pas loi de composition interne sur $\mathbb{Z}$. Car $\frac{a}{b}$ n'est pas défini pour tous les couples (a,b) d'entiers.

Définition 4.2. Soient $*$ une loi de composition interne sur E, on dit que :

1. $*$ est dite commutative si et seulement si :

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

2. Soit E un ensemble muni par une loi de composition interne $*$ et F une partie de E. On dit que F est une partie stable pour la loi $*$ si :

$$\forall (x,y) \in F \times F,\ x * y \in F,$$

3. $*$ est dite associative si et seulement si :

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

4. $*$ admet un élément neutre noté $\langle e \rangle$ si et seulement si :

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

5. $*$ admet un élément neutre e. Alors il existe un élément symétrique (Inverse), soient x et x' deux éléments sont symétriques pour la loi $*$ si :

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

4.2 Groupes

Définition 4.3. On appelle groupe un ensemble E muni d'une loi interne $*$ telle que :

1. $*$ est associative.
2. $*$ admet un élément neutre.
3. Tout élément de E admet un élément symétrique dans E.

Si de plus $*$ est commutatif, alors $(E, *)$ est un groupe commutatif ou abélien.

Exemple 4.1.
1. $(\mathbb{Z}, +)$ est un groupe commutatif.
2. $(\mathbb{R}_+^*, \times)$ est un groupe commutatif.
3. $(\mathbb{R}, \times)$ n'est pas un groupe car 0 n'admet pas d'élément symétrique.

4.2.1 Sous groupe

Définition 4.4. Soit $(G, *)$ un groupe et soit H une partie non vide de G. On dit que H est un sous-groupe de G si :

1. L'élément neutre e appartient a H,i.e : $(e \in H)$,
2. H est stable pour la lois $* : \forall (x, y) \in H \times H,\ x * y \in H$,
3. H est stable pour le passage à l'inverse $\forall x \in H, x' \in H$.

Remarque 4.1. Un critère pratique et plus rapide pour prouver que H est un sous-groupe de G est :
- H contient au moins un élément,
- $\forall (x, y) \in H \times H, x * y \in H$.

Exemple 4.2. ☞ $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$. En effet :

1. L'élément neutre $e = 1 \in \mathbb{R}_+^*$.
2. $\forall (x, y) \mathbb{R}_+^* \times \mathbb{R}_+^*,\ x \times y \in \mathbb{R}_+^*$,
3. $\forall x \in \mathbb{R}_+^*,\ x^{-1} = \frac{1}{x} \in \mathbb{R}_+^*$.

☞ $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

Théorème 4.1 (Caractérisation des sous-groupes)**.** *Soit $(G, *)$ un groupe et soit H une partie non vide de G. Alors H est un sous-groupe de G si et seulement si :*

$$\forall (x, y) \in H \times H,\ x * y' \in H$$

4.2.2 Homomorphisme de groupes

Définition 4.5. Soient $(G_1, *)$ et (G_2, Δ) deux groupes. On appelle homomorphisme (ou morphisme) de groupes de G_1 dans G_2, une application $f : G_1 \longrightarrow G_2$ telle que,

$$\forall x, y \in G_1,\ f(x * y) = f(x)\Delta f(y).$$

Exemple 4.3. Soit l'application f donnée par :

$$\begin{aligned} f :& \mathbb{R}^* \longrightarrow \mathbb{R} \\ & x \longmapsto f(x) = \ln(x) \end{aligned}$$

Donc, f est un homomorphisme de $(\mathbb{R}^*, \times)$ dans $(\mathbb{R}, +)$ car :

$$\forall x, y \in \mathbb{R},\ f(x \times y) = \ln(x \times y) = \ln(x) + \ln(y) = f(x) + f(y).$$

Corollaire 4.1. *Soient $(G_1, *)$ et (G_2, Δ) deux groupes d'éléments neutres e_1 et e_2 et soit f un homomorphisme de G_1 dans G_2. Alors*

- ☞ *f est un isomorphisme de groupes si f est une bijection.*
- ☞ *f est un automorphisme de groupes si f est un isomorphisme et si $G_1 = G_2$, (même groupe au départ et à l'arrivée).*

Proposition 4.1. *Soient $(G_1, *)$ et (G_2, Δ) deux groupes d'éléments neutres e_1 et e_2 et soit f un homomorphisme de G_1 dans G_2. Alors*

1. $f(e_1) = e_2$,
2. $\forall x \in G_1,\ (f(x))' = f(x')$.

Exemple 4.4. Soit f un homomorphisme donné par :

$$\begin{aligned} f :& \mathbb{R} \longrightarrow \mathbb{R}_+ \\ & x \longmapsto f(x) = e^x \end{aligned}$$

Proposition 4.2. *Soient $(G_1, *)$ et (G_2, Δ) deux groupes d'éléments neutres e_1 et e_2 et soit f un homomorphisme de G_1 dans G_2. Alors*

1. *Si H est un sous-groupe de G_1, alors $f(H)$ est un sous-groupe de G_2 ,*
2. *Si L est un sous-groupe de G_2, alors $f^{-1}(L)$ est un sous-groupe de G_1.*

4.2.3 Image et noyau d'un homomorphisme

1- L'image d'un homomorphisme :

Définition 4.6. Soient $(G_1, *)$ et (G_2, Δ) deux groupes d'éléments neutres e_1 et e_2 et soit f un homomorphisme de G_1 dans G_2. Alors,
On appelle Image de f l'ensemble

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

.

2- Le noyau d'un homomorphisme :

Définition 4.7. Soient $(G_1, *)$ et (G_2, Δ) deux groupes d'éléments neutres e_1 et e_2 et soit f un homomorphisme de G_1 dans G_2. Alors,
On appelle noyau de f l'ensemble

$$Ker(f) = f^{-1}(e_2) = \{x \in G_1,\ f(x) = e_2\}$$

.

Exemple 4.5. Soit f un homomorphisme donné par :

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

✗ **L'image de** f est donnée par :

$$Im(f) = \{f(x),\ x \in \mathbb{R}\},$$

et, $y = f(x) \Rightarrow y = 2^x$, donc $y \in\ ]\,0, +\infty] = \mathbb{R}_+^*$.
D'où, $Im(f) = \mathbb{R}_+^*$.

✗ **Le noyau de** f est donnée par :

$$Ker(f) = \{x \in \mathbb{R}; f(x) = 1\} = \{x \in \mathbb{R}; 2^x = 1\} = \{0\}.$$

Théorème 4.2. *Soit f un homomorphisme de $(G_1, *)$ dans (G_2, Δ). 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 si et seulement si $Ker(f) = \{e_1\}$,*
4. *f est surjective si et seulement si $Im(f) = G_2$.*

4.3 Anneaux

Définition 4.8. Soit A un ensemble muni de deux lois de composition internes $*$, $\bullet$, on dit que $(A, *, \bullet)$ est un anneau si :

1. $(A, *)$ est un groupe commutatif.
2. Distributivité à gauche et à droite,

$$\forall x, y, z \in A, x\bullet(y * z) = (x \bullet y)*(x \bullet z)\,, \text{et } (x * y)\bullet z = (x \bullet z)*(y \bullet z)\,.$$

3. $\bullet$ est associative .

Remarque 4.2. On remarque :

- ✈ Si de plus $\bullet$ est commutative, on dit que $(A, *, \bullet)$ est un anneau commutatif.
- ✈ Si $\bullet$ admet un élément neutre, on dit que $(A, *, \bullet)$ est un anneau unitaire.

Exemple 4.6. ✓ $(\mathbb{Z}, +, \times)$ est un anneau commutatif et unitaire.

- ☞ Car, $(\mathbb{Z}, +)$ est un groupe commutatif.
- ☞ Et en plus la distributivité à gauche et à droite existe par rapport les deux lois de composition internes $+$, $\times$.

$$\forall x, y, z \in \mathbb{Z}, x\times(y + z) = (x \times y)+(x \times z)\,, \text{et } (x + y)\times z = (x \times z)+(y \times z)\,.$$

4.3.1 Sous-anneau

Définition 4.9. Soit $(A, +, \cdot)$ un anneau et soit B une partie de A. On dit que B est un sous-anneau de $(A, +, \cdot)$ si et seulement si :

1. $0_A \in B \Rightarrow B \neq \emptyset$,
2. $(B, +)$ est un sous-groupe de A,
3. B stable pour la loi $\cdot$,

Exemple 4.7.
1. $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$,
2. $(\mathbb{Q}, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$
3. $(\mathbb{R}, +, \times)$ est un sous-anneau de $(\mathbb{C}, +, \times)$

4.3.2 Homomorphisme d'anneaux

Définition 4.10. Soient $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux.
On dit quŠune application $f : A \longrightarrow B$ est un homomorphisme (ou morphisme) si :

1. $f(1_A) = 1_B$,
2. $\forall a,b \in A,\ f(a+b) = f(a)+f(b)$,
3. $\forall a,b \in A,\ f(a\cdot b) = f(a)\cdot f(b)$.

4.3.3 Règles de calculs dans un anneau

Dans $\mathbb{Z}$ la formule du binôme de Newton est une formule mathématique donnée par Isaac Newton pour trouver le développement d'une puissance entière quelconque d'un binôme. Elle est aussi appelée formule du binôme ou formule de Newton.

Proposition 4.3. *Soient $(A,+,\cdot)$ un anneau et $x,y \in A$, avec $a\cdot b = b\cdot a$, et pour $n \in \mathbb{N}$. Alors :*

☞ *Si x et y sont deux élément d'un anneau A qui commutent :*

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}.$$

Cette formule est connue sous le nom du 'binôme de Newton' ici :

$$C_n^k = \binom{n}{k} = \frac{n!}{(n-k)!k!.}$$

☞ *Remplaçant y par $-y$ et utilisant la relation simple dans la formule précédente ci-dessus, il vient :*

$$(x-y)^n = \sum_{k=0}^{n} C_n^k (-1)^{n-k} x^k y^{n-k}.$$

☞ *Toujours avec l'hypothèse que x et y commutent, $n \in \mathbb{N}$:*

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^{n-1-k} y^k.$$

☞ *En particulier, en faisant $x = 1$ dans la formule ci-dessus.*

$$1 - y^n = (1 - y) \sum_{k=0}^{n-1} y^k.$$

Démonstration. Pour prouver cette proposition, on utilise la démonstration par récurrence avec la formule du triangle de Pascal.

n \ k	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

FIGURE 4.1 – Le triangle de Pascal

□

4.4 Corps

Définition 4.11. Soit $\mathbb{B}$ un ensemble munie de deux lois de composition internes $*$, $\bullet$, on dit que $(\mathbb{B}, *, \bullet)$ est un corps si :

1. $(\mathbb{B}, *, \bullet)$ est un anneau.
2. Tout élément distinct de e est inversible pour la loi $\bullet$, où e est l'élément neutre de la loi $*$.

Remarque 4.3. Si de plus $\bullet$ est commutative, on parle de corps commutatif.

Exemple 4.8. ✓ $(\mathbb{R}, +, \times)$ est un corps commutatif.

1. $(\mathbb{R}, +, \times)$ est un corps, et plus :

- ✌ Car, $(\mathbb{R}, +, \times)$ est un anneau commutatif.
- ✌ Et en plus tout élément $x \neq 0$ est inversible pour la loi $\times$

2. $(\mathbb{Z}, +, \times)$ n'est pas un corps.

4.4.1 Sous-corps

Définition 4.12. Soit $(\mathbb{K}, +, \times)$ un corps et soit $\mathbb{L}$ une partie de $\mathbb{K}$. On dit que $\mathbb{L}$ est un sous corps de $\mathbb{K}$ lorsque :

1. $1_{\mathbb{K}} \in \mathbb{L}$,
2. $\mathbb{L}$ est stable par $+$ et $\times$,
3. $\forall x \in \mathbb{L}, (-x) \in \mathbb{L}$ et $\forall x \in \mathbb{L} - \{0_{\mathbb{K}}\}, x^{-1} \in \mathbb{L}$.

Exemple 4.9. $\mathbb{R}$ est un sous corps de $(\mathbb{C}, +, \times)$.