

Chapitre 4

Structures algébriques

4.1 Loi de composition interne

Définition 4.1 On appelle loi de composition interne (LCI) sur un ensemble E tout application $*$: $E \times E \longrightarrow E$.

Un sous ensemble F de E est dite "stable" par rapport à la loi $*$ si

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

Exemple 4.1 1. $\cap$ et $\cup$ sont des lois de compositions internes sur $P(E)$.

2. La somme "+" et le produit " $\times$ " sont des LCI sur $\mathbb{N}, \mathbb{N}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, mais pas sur $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*$,

3. La différence "-" sur $\mathbb{R}, \mathbb{C}$.

4. La composition " $\circ$ " des applications sur F^F (applications définies de F dans F).

Exemple 4.2 Soit $E = \{1, 2, 3\}$, et $F = \{\{1, 2\}, \{2, 3\}, \{1, 3\}\} \subset P(E)$

F n'est pas stable par rapport à l'intersection $\cap$ et la réunion $\cup$ car :

$$\exists \{1, 2\}, \{2, 3\} \in F; \{1, 2\} \cap \{2, 3\} = \{2\} \notin F,$$

$$\exists \{1, 2\}, \{2, 3\} \in F; \{1, 2\} \cup \{2, 3\} = \{1, 2, 3\} \notin F.$$

Définition 4.2 Soient $*$ et ∇ deux lois de composition internes (LCI) sur un ensemble E , on dit que:

1. $*$ est commutative si: $\forall x, y \in E; x * y = y * x$,

2. $*$ est associative si: $\forall x, y, z \in E; (x * y) * z = x * (y * z)$,

3. $e \in E$ est un élément neutre à gauche (respectivement à droite) de la loi $*$ si

$$\forall x \in E; e * x = x \text{ (respectivement } x * e = x)$$

- Si e est un élément neutre à droite et à gauche de $*$ on dit que e est un élément neutre de $*$.

4. Soit $e \in E$ est un élément neutre, on dit qu'un élément $x \in E$ est inversible, ou symétrisable, à droite (respectivement à gauche) de $*$ si

$$\exists x' \in E, x * x' = e \text{ (respectivement } x' * x = e)$$

x est inversible (ou symétrisable) s'il est inversible à droite et à gauche de $*$. et x' est dit un inverse (ou un symétrique) à droite (respectivement à gauche) de x .

5. $*$ est distributive par rapport à ∇ si : $\forall x, y, z \in E$,

$$x * (y \nabla z) = (x * y) \nabla (x * z) \text{ et } (y \nabla z) * x = (y * x) \nabla (z * x).$$

6. On dit qu'un élément $r \in E$ est régulier à droite (respectivement à gauche) de Soit $*$ si

$$\forall x, y \in E; x \star r = y \star r \implies x = y$$

$$(\text{respectivement } \forall x, y \in E; r \star x = r \star y \implies x = y)$$

Exemple 4.3 1. La somme et le produit sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ est associative et commutative, et admettent pour neutres respectifs 0 et 1.

2. La différence n'est ni associative ni commutative sur $\mathbb{R}$.

3. La loi " $\circ$ " est associative, mais n'est pas commutative sur F^F , elle admet un neutre, qui est l'application Id_F .

4. Les lois $\cap, \cup, \Delta$ sur $P(E)$ sont associatives et commutatives. Elles admettent pour neutres respectifs $E, \emptyset, \emptyset$

Remarque 4.1 1. Si $*$ est une loi de composition interne associative sur E qui admet un élément neutre, alors ce neutre est unique

2. L'élément neutre e est inversible (ou symétrisable) et son unique inverse (ou symétrique) est e .

3. Si l'élément symétrique x' de x existe, il est unique. On le note généralement x^{-1} .

4.2 Les groupes

Définition 4.3 Un groupe est un ensemble non vide G muni d'une loi de composition interne $*$, noté $(G, *)$ tels que :

1. $*$ est associative ;

2. $*$ admet un élément neutre e ;

3. tout élément de G est symétrisable (admet un symétrique) pour $*$.

Si $*$ est commutative, on dit que $(G, *)$ est commutatif, ou encore abélien.

Exemple 4.4 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de la somme sont des groupes abéliens,

2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, Un munis du produit sont des groupes abéliens,

3. $P(E)$ muni de Δ est un groupe abélien.

Exemple 4.5 (à démontrer) Les couples suivants ne sont pas des groupes :

1. $(\mathbb{N}, +), (\mathbb{R}, \times), (\mathbb{Z}, \times),$

2. $(P(E), \cap), (P(E), \cup).$

4.2.1 Sous-groupes

Définition 4.4 *Un sous-groupe d'un groupe $(G, *)$ est une partie non vide H de G telle que :*

1. $*$ induit sur H une loi de composition interne.
2. H muni cette loi est un groupe.

En pratique, pour montrer qu'une partie non vide H de G en constitue un sous-groupe, il suffit de vérifier l'une des propositions suivantes:

Proposition 4.1 *Soient $(G, *)$ un groupe et $H \subset G$ alors,*

$$H \text{ est un sous groupe de } G \iff \begin{cases} i. H \neq \emptyset \\ ii. \forall x, y \in H, x * y \in H. \text{ (} H \text{ est stable par rapport à } * \text{)} \\ iii. \forall x \in H, x^{-1} \in H \text{ (} x^{-1} \text{ le symétrique de } x \text{)} \end{cases}$$

Proposition 4.2 *Soient $(G, *)$ un groupe et $H \subset G$ alors,*

$$H \text{ est un sous groupe de } G \iff \begin{cases} i. H \neq \emptyset \\ ii. \forall x, y \in H, x * y^{-1} \in H. \end{cases}$$

Remarque 4.2 *Si e est l'élément neutre d'un groupe $(G, *)$, alors tout sous groupe de G contient e et on déduit la propriété suivante:*

Proposition 4.3 *Soient $(G, *)$ un groupe, e l'élément neutre de $*$ et H un sous ensemble de G alors,*

$$H \text{ est un sous groupe de } G \iff \begin{cases} i. e \in H \\ ii. \forall x, y \in H, x * y^{-1} \in H. \end{cases}$$

Exemple 4.6 1. Considérons le groupe $(\mathbb{C}^*, \times)$, et soit $U = \{z \in \mathbb{C}, |z| = 1\}$,

- Montrer que U est un sous groupe de $\mathbb{C}^*$.

► i) $|1| = 1$ donc $1 \in U$, d'où $U \neq \emptyset$.

ii) soient $z_1, z_2 \in \mathbb{C}$, $\left| z_1 \times (z_2)^{-1} \right| = \left| \frac{z_1}{z_2} \right| = \frac{1}{1} = 1$, d'où $z_1 \times (z_2)^{-1} \in U$.

Alors $(U, \times)$ est un sous groupe de $\mathbb{C}^*$.

2. Soit $n \in \mathbb{N}$, $n\mathbb{Z} = \{np, p \in \mathbb{Z}\}$ est un sous groupe de $(\mathbb{Z}, +)$.

► i) $0 \in n\mathbb{Z}$ car $\exists p = 0$, $n0 = 0 \in n\mathbb{Z}$ donc $n\mathbb{Z} \neq \emptyset$,

ii) $\forall x, y \in n\mathbb{Z}$, $\exists p_1, p_2 \in \mathbb{Z}$, $x = np_1$, $y = np_2$ alors,

$$x - y = np_1 - np_2 = n(p_1 - p_2) = nh \quad (h = p_1 - p_2 \in \mathbb{Z}), \text{ D'où } x - y \in n\mathbb{Z}$$

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

4.2.2 Homomorphisme de groupes

Définition 4.5 *Soient $(G, *)$ et (G', T) deux groupes. Une application f de G dans G' est un "homomorphisme de groupes" lorsque :*

$$\forall x, y \in G; f(x * y) = f(x)Tf(y).$$

- Si $G = G'$ et $*$ = T , on parle d'endomorphisme.
- Si f est bijective, on parle d'isomorphisme.
- Si f est un endomorphisme bijectif, on parle d'automorphisme.

Exemple 4.7 1. $x \mapsto 2^x$ est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$,
 2. $x \mapsto 2x$ est un automorphisme de $(\mathbb{R}, +)$,
 3. $x \mapsto 3 \ln x$ est un isomorphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$,
 4. $z \mapsto |z|$ est un homomorphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$.

Exemple 4.8 Montrer que la composition de deux homomorphismes de groupes est un homomorphisme de groupes.

Proposition 4.4 Soient e, e' les éléments neutres de G, G' respectivement et soit $f : G \longrightarrow G'$ un homomorphisme de groupes, alors

1. $f(e) = e'$,
2. $\forall x \in G, (f(x^{-1})) = (f(x))^{-1}$. (x^{-1} est le symétrique de x).

Proposition 4.5 Soit $f : (G, *) \longrightarrow (G', T)$ un homomorphisme de groupes, alors

1. L'image d'un sous groupe de G par f est un sous groupe de G' .
2. L'image réciproque d'un sous groupe de G' par f est un sous groupe de G .

Preuve. 1. Soit H un sous groupe de G et montrons que $f(H)$ vérifie les deux conditions de la caractérisation des sous groupes.

- i) Comme H est un sous groupe de G , alors $e \in H$ donc $f(e) \in f(H)$, par suite $f(H) \neq \emptyset$.
- ii) Soient $x', y' \in f(H)$, alors il existe $x, y \in H$ tels que $x' = f(x)$ et $y' = f(y)$, donc d'après la deuxième propriété on aura

$$x'T(y')^{-1} = f(x)T(f(y))^{-1} = f(x)Tf(y^{-1}) = f(x * y^{-1})$$

et comme H est un sous groupe de G alors $(x * y^{-1}) \in H$, par suite $x'T(y')^{-1} = f(x * y^{-1}) \in f(H)$ de i) et ii) on déduit que $f(H)$ est un sous groupe de G' .

2. Soit H' un sous groupe de G' , alors

- i) D'après la première propriété $f(e) = e'$ et comme H' est un sous groupe de G' alors $e' \in H'$ donc $e \in f^{-1}(H')$.
- ii) Soient $x, y \in f^{-1}(H')$, alors $f(x), f(y) \in H'$ et comme H' est un sous groupe de G' alors $f(x)T(f(y))^{-1} \in H'$ et de la deuxième propriété on déduit que $f(x * y^{-1}) = f(x)Tf(y^{-1}) = f(x)T(f(y))^{-1} \in H'$, ce qui montre que $(x * y^{-1}) \in f^{-1}(H')$.

De i) et ii) on déduit que $f^{-1}(H')$ est un sous groupe de G . ■

Le noyau et l'image d'un homomorphisme

Définition 4.6 Soit f un homomorphisme de G dans G' , e, e' les éléments neutres de G, G' respectivement

- Le noyau de f , noté $\ker f$ est l'ensemble définie par:

$$\ker f = \left\{ x \in G; f(x) = e' \right\} = f^{-1}(e').$$

- L'image de f , noté $\operatorname{Im} f$ est l'ensemble définie par:

$$\operatorname{Im} f = \{ f(x), x \in G \} = f(G)$$

Corollaire 4.1 Comme cas particuliers de la proposition (4.2.5) on a:

1. $\operatorname{Im} f$ est un sous groupe de (G', T) ,
2. $\ker f$ est un sous groupe de $(G, *)$.

Le résultat suivant est bien plus intéressant, puisqu'il réduit énormément le travail, pour montrer qu'un homomorphisme est bijectif.

Proposition 4.6 Soit $f : (G, *) \longrightarrow (G', T)$ un homomorphisme de groupe, alors

1. f est injective si et seulement si $\ker f = \{e\}$, (où e est l'élément neutre de G)
2. f est surjective si et seulement si $\operatorname{Im} f = G'$.