Chapitre 1

Structures algébriques

Ce chapitre est consacré à l'étude des structures algébriques préalablement introduites en première année en cours d'algèbre, à savoir les groupes, les anneaux, les corps et les algèbres. Des notions nouvelles et plus approfondies concernant toutes ces structures seront abordées tout au long de chapitre, accompagnées de plusieurs exemples basiques et simples rendant plus accessible la compréhension de ces notions.

Dans ce chapitre $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$.

1.1 Groupes

Définition 1.1.1 – Groupe Soit G un ensemble non vide muni d'une loi de composition interne notée "$*$". On dit que $(G,*)$ est un groupe si
- La loi "$*$" est associative.
- La loi "$*$" admet un élément neutre.
- Tout élément $x \in G$ admet un élément symétrique.

Si de plus la loi "$*$" est commutative, on dit que $(G,*)$ est un groupe abélien.

■ **Exemple 1.1.2 – Groupes de référence**
$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont tous des groupes abéliens.

■ **Exemple 1.1.3 – Groupe des racines n-ièmes de l'unité $\mathbb{U}_n$**
Pour tout $n \in \mathbb{N}^*$, l'ensemble

$$\mathbb{U}_n = \{z \in \mathbb{C}^* \,|\, z^n = 1\} = \left\{ e^{\frac{2i\pi k}{n}} \,|\, 0 \leqslant k \leqslant n-1 \right\}$$

est un groupe abélien pour la multiplication usuelle sur $\mathbb{C}$. À titre d'exemple, $\mathbb{U}_1 = \{1\}$, $\mathbb{U}_2 = \{-1,1\}$, $\mathbb{U}_3 = \{1, j, \bar{j}\}$ et $\mathbb{U}_4 = \{-1,1,-i,i\}$.

■ Exemple 1.1.4 – Groupe symétrique $\mathfrak{S}_n$
Pour tout $n \in \mathbb{N}^*$, on note $[\![1,n]\!] = \{k \in \mathbb{N} \mid 1 \leqslant k \leqslant n\}$. Alors, l'ensemble $\mathfrak{S}_n$ des permutations de $[\![1,n]\!]$ est un groupe pour la composition des applications appelé groupe symétrique. À titre d'exemple, $\mathfrak{S}_1 = \{\mathrm{Id}_{\{1\}}\}$
et $\mathfrak{S}_2 = \{\mathrm{Id}_{\{1,2\}}, \tau_{1,2}\}$.

■ Exemple 1.1.5 – Groupe "cercle unité"
L'ensemble

$$\mathbb{U} = \{z \in \mathbb{C}^* \mid |z| = 1\} = \left\{e^{i\theta} \mid \theta \in \mathbb{R}\right\},$$

est un groupe abélien pour la multiplication usuelle sur $\mathbb{C}$.

■ Exemple 1.1.6 – Groupe des polynômes
1) L'ensemble $\mathbb{K}[X]$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ est un groupe abélien pour la somme des polynômes.
2) Pour tout $n \in \mathbb{N}$, l'ensemble $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leqslant n\}$ est un groupe abélien pour la somme des polynômes.

■ Exemple 1.1.7 – Groupe des matrices $\mathscr{M}_{n,p}(\mathbb{K})$
Pour tous $n, p \in \mathbb{N}^*$, l'ensemble $\mathscr{M}_{n,p}(\mathbb{K})$ des matrices de type (n,p) à coefficients dans $\mathbb{K}$ est un groupe abélien pour la somme usuelle des matrices.

■ Exemple 1.1.8 – Groupe général linéaire $GL_n(\mathbb{K})$
Pour tout $n \in \mathbb{N}^*$, l'ensemble $GL_n(\mathbb{K})$ des matrices carrées inversibles d'ordre n est un groupe pour la multiplication matricielle.

■ Exemple 1.1.9 – Groupe spécial linéaire $SL_n(\mathbb{K})$
Pour tout $n \in \mathbb{N}^*$, l'ensemble $SL_n(\mathbb{K}) = \{M \in GL_n(\mathbb{K}) \mid \det(M) = 1\}$
est un groupe pour la multiplication matricielle.

■ Exemple 1.1.10 – Groupe orthogonal $\mathscr{O}(n)$
Pour tout $n \in \mathbb{N}^*$, l'ensemble $\mathscr{O}(n) = \left\{M \in GL_n(\mathbb{R}) \mid M^{-1} = {}^tM\right\}$
est un groupe pour la multiplication matricielle.

■ Exemple 1.1.11 – Groupe spécial orthogonal $SO(n)$
Pour tout $n \in \mathbb{N}^*$, l'ensemble $SO(n) = \{M \in \mathscr{O}(n) \mid \det(M) = 1\}$
est un groupe pour la multiplication matricielle.

■ **Exemple 1.1.12 – Groupe $\mathbb{Z}/n\mathbb{Z}$**
Soit $n \in \mathbb{N}^*$, on munit l'ensemble $\mathbb{Z}$ de la relation d'équivalence notée "$\equiv$" dite "congruence modulo n" et définie par

$$\forall p,q \in \mathbb{Z},\ p \equiv q[n] \text{ si } n|p-q.$$

Pour tout $p \in \mathbb{Z}$, la classe d'équivalence de p est définie par

$$\dot{p} = \{p + nk \mid k \in \mathbb{Z}\}$$

et l'ensemble quotient est donné par

$$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \ldots, \widehat{\dot{n-1}}\right\}.$$

On munit $\mathbb{Z}/n\mathbb{Z}$ de la loi de composition interne $''+''$ définie par

$$\forall \dot{p},\dot{q} \in \mathbb{Z}/n\mathbb{Z},\ \dot{p}+\dot{q} = \widehat{\dot{p+q}}.$$

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

Théorème 1.1.13 – Produit direct de groupes Soient $(G,*)$ et $(G',.)$ deux groupes et "#" la loi de composition interne définie sur le produit cartésien $G \times G'$, par

$$\forall (x,y),(x',y') \in G \times G',\ (x,y)\#(x',y') = (x*x', y.y').$$

Alors, $(G \times G', \#)$ est un groupe, appelé groupe produit direct de G et G'.

Démonstration. — $G \times G' \neq \varnothing$ car G et G' le sont.

— La loi "#" est associative car les lois "$*$" et "." le sont.

— Si e et e' sont respectivement les éléments neutres de G et G', alors pour tout $(x,y) \in G \times G'$, on a

$$(x,y)\#(e,e') = (x*e, y.e') = (x,y)$$

et de la même manière

$$(e,e')\#(x,y) = (x*e, y.e') = (x,y).$$

Par conséquent, (e,e') est l'élément neutre de $G \times G'$ pour la loi "#".

— Soit $(x,y) \in G \times G'$ et soient x^{-1} et y^{-1} respectivement les éléments symétriques de x et y. Alors,

$$(x,y)\#(x^{-1},y^{-1}) = (x*x^{-1}, y.y^{-1}) = (e,e'),$$

de la même manière

$$(x^{-1},y^{-1})\#(x,y) = (x^{-1}*x, y^{-1}.y) = (e,e').$$

■

▪ Exemple 1.1.14 – Groupe de Klein
Le groupe produit direct $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est appelé groupe de Klein, ci-après sa table d'addition

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

TABLE 1.1 – Table d'addition du groupe de Klein

Définition 1.1.15 – Sous groupe Soient $(G,*)$ un groupe et $H \subset G$ une partie non vide de G. On dit que H est un sous-groupe de G, si
— H est stable par la loi "$*$". Autrement dit, pour tout $x,y \in H$, $x*y \in H$.
— H est stable par symétrie. Autrement dit, pour tout $x \in H$, $x^{-1} \in H$.

Remarque 1.1.16
1) Au vu de la Définition 1.1.15, on en déduit que tout sous-groupe est un groupe.
2) Si $(G, *)$ est un groupe d'élément neutre e, alors $\{e\}$ et G sont des sous-groupes de G, appelés les sous-groupes triviaux de G. Tout sous-groupe non trivial de G est appelé sous-groupe propre.

▪ Exemple 1.1.17 – Exemples de référence
1) Pour l'addition usuelle, $\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$ qui est un sous-groupe de $\mathbb{R}$ qui est lui même un sous-groupe de $\mathbb{C}$.
2) Pour la multiplication usuelle, $\mathbb{Q}^*$ est un sous-groupe de $\mathbb{R}^*$ qui est un sous-groupe de $\mathbb{C}^*$.
3) Pour la multiplication matricielle $\mathscr{O}(n)$ et $SL_n(\mathbb{R})$ sont des sous-groupe de $GL_n(\mathbb{R})$.
4) Pour la multiplication matricielle, $SO(n)$ est un sous-groupe de $\mathscr{O}(n)$ appelé groupe spécial orthogonal.

5) Pour la multiplication usuelle, $\mathbb{U}_n$ $(n \in \mathbb{N}^*)$ est un sous-groupe de $\mathbb{U}$ qui est un sous-groupe de $\mathbb{C}^*$.
6) Pour l'addition des polynômes, $\mathbb{K}_n[X]$, $n \in \mathbb{N}^*$, est un sous-groupe de $\mathbb{K}[X]$.
7) Pour la composition des applications, l'ensemble

$$\mathscr{A}_n = \{\sigma \in \mathfrak{S}_n \mid \varepsilon(\sigma) = 1\}$$

des permutations paires de $\mathfrak{S}_n$ est un sous-groupe de $\mathfrak{S}_n$ appelé sous-groupe alterné.

▪ Exemple 1.1.18 – Centre d'un groupe
Soit $(G, *)$ un groupe. On appelle centre de G, l'ensemble

$$Z(G) = \{k \in G \mid h*k = k*h, \forall h \in G\}.$$

Alors,

— Si on désigne par e l'élément neutre de G, alors $e \in Z(G)$ et donc $Z(G) \neq \varnothing$.
— $Z(G) \subseteq G$.
— Soient $x, y \in Z(G)$, alors pour tout $z \in G$, on a

$$(x*y)*z = x*(y*z) = x*(z*y) = (x*z)*y = (z*x)*y = z*(x*y)$$

et donc $x*y \in Z(G)$.
— Soit $x \in Z(G)$, alors pour tout $z \in G$, on a

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

et par suite

$$\forall z \in G,\ x^{-1}*z = z*x^{-1}$$

ce qui entraîne que $x^{-1} \in Z(G)$.

Ainsi, d'après la Définition 1.1.15, on en déduit que $Z(G)$ est un sous-groupe de G. Par ailleurs, il est clair que G est abélien si et seulement si $Z(G) = G$.

Théorème 1.1.19 – Caractérisation d'un sous-groupe Soient $(G, *)$ un groupe et $H \subset G$ une partie non vide de G. Alors, H est un sous-groupe de G, si et seulement si pour tout $x, y \in H$, $x*y^{-1} \in H$.

Démonstration. — Si H est un sous-groupe de G, alors pour tous $x, y \in H$, on a $x \in H$ et $y^{-1} \in H$ et par suite $x*y^{-1} \in H$.

— Réciproquement, supposons que pour tous $x, y \in H$, on a $x * y^{-1} \in H$. Soit $x \in H$, alors $x * x^{-1} = e \in H$, en particulier pour tout $x \in H$, on a $e * x^{-1} = x^{-1} \in H$ et par suite H est stable par symétrie. Par ailleurs, pour tous $x, y \in H$, on a $y^{-1} \in H$ et donc $x * y = x * (y^{-1})^{-1} \in H$, ce qui implique que H est stable par la loi "$*$" et donc H est un sous-groupe de G.

■

Remarque 1.1.20 — Méthode. Étant donné que tout sous-groupe est un groupe, pour montrer qu'un doublet $(G, *)$ est un groupe, il suffit de montrer que c'est un sous-groupe d'un groupe connu.

■ **Exemple 1.1.21 – Groupe des entiers de Gauss** $\mathbb{Z}[i]$
Soit

$$\mathbb{Z}[i] = \{a + ib \,|\, a,\ b \in \mathbb{Z}\}.$$

Alors,

— $\mathbb{Z}[i] \subset \mathbb{C}$.
— $0 = 0 + i.0 \in \mathbb{Z}[i]$, en particulier $\mathbb{Z}[i] \neq \varnothing$.
— Soit $a + ib, c + id \in \mathbb{Z}[i]$, alors

$$(a + ib) - (c + id) = (a - c) + i(b - d) \in \mathbb{Z}[i].$$

Par conséquent, $\mathbb{Z}[i]$ est un sous-groupe de $\mathbb{C}$, en particulier $(\mathbb{Z}[i], +)$ est un groupe abélien.

Théorème 1.1.22 – Sous groupes de $\mathbb{Z}$ Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.

Démonstration. — Il est clair que pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
— Réciproquement, soit H un sous-groupe de $\mathbb{Z}$.
— Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
— Si $H \neq \{0\}$, alors il existe $x \in H$ tel que $x > 0$. Soit $H^+ = \{x \in H | x > 0\}$, alors H^+ est une partie non vide de $\mathbb{N}$, qui admet donc un plus petit élément $n > 0$. Comme $n \in H$ et H est un sous-groupe de $\mathbb{Z}$, on en déduit que $n\mathbb{Z} \subset H$. Soit maintenant $x \in H^+$ et soient q et r respectivement le quotient et le reste de la division euclidienne de x par n.

Alors, $x = nq + r$ avec $0 \leqslant r < n$, comme $n \in H$, alors
$nq = \underbrace{n + \cdots + n}_{\text{q fois}} \in H$ et par suite $r = x - nq \in H$ ce qui signifie que $r = 0$
(Autrement on aurait $r \in H^+$ et $r < n$ ce qui contredit le fait que n est le plus petit élément de H^+). Ainsi, tout élément $x \in H^+$ s'écrit sous la forme nq avec $q \in \mathbb{N}$, ce qui implique que $H \subset n\mathbb{Z}$.

■

Proposition 1.1.23 – Intersection d'une famille de sous-groupes.
Soient $(G, *)$ un groupe et I un ensemble non vide. Si $(F_i)_{i\in I}$ est une famille de sous-groupes de G, alors $\bigcap_{i\in I} F_i$ est un sous-groupe de G.

Démonstration. Soit e l'élément neutre de G, alors $e \in \bigcap_{i\in I} F_i$ et donc $\bigcap_{i\in I} F_i \neq \varnothing$.
D'autre part, pour tous $x, y \in \bigcap_{i\in I} F_i$, on a $x * y^{-1} \in F_i$ pour tout $i \in I$ et par suite $x * y^{-1} \in \bigcap_{i\in I} F_i$ ce qui implique d'après le Théorème 1.1.19 que $\bigcap_{i\in I} F_i$ est un sous-groupe de G. ■

▪ Exemple 1.1.24
1) Pour tous $n, m \in \mathbb{N}^*$, on a $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n\wedge m}$ où $n \wedge m$ désigne le PGCD de n et m.
2) Pour tout $n \in \mathbb{N}^*$, on a $SL_n(\mathbb{R}) \cap \mathscr{O}(n) = SO(n)$.
3) Pour tous $n, m \in \mathbb{N}^*$, on a $n\mathbb{Z} \cap m\mathbb{Z} = (n \vee m)\mathbb{Z}$ où $n \vee m$ désigne le PPCM de n et m.
4) Pour tous $n, m \in \mathbb{N}^*$, on a $\mathscr{A}_n(\mathbb{R}) \cap S_n(\mathbb{R}) = \{0\}$.

Remarque 1.1.25 — Réunion de deux sous-groupes. Le résultat précédent n'est pas vrai en général pour la réunion, en effet $2\mathbb{Z}$ et $3\mathbb{Z}$ sont deux sous-groupes de $\mathbb{Z}$, cependant $2, 3 \in (2\mathbb{Z} \cup 3\mathbb{Z})$ et $5 = 2 + 3 \notin (2\mathbb{Z} \cup 3\mathbb{Z})$, en d'autres termes $(2\mathbb{Z} \cup 3\mathbb{Z})$ n'est même pas stable par l'addition.

▪ Exemple 1.1.26 – Réunion de deux sous-groupes
Soit $(G, *)$ un groupe et soient H et K deux sous-groupes de G. Alors, $H \cup K$ est un sous-groupe de G si et seulement si, $H \subset K$ ou $K \subset H$.

En effet,

— Supposons que $H \cup K$ est un sous-groupe de G. Si $H \not\subset K$ alors il existe $x \in H$ tel que $x \notin K$, soit $y \in K$, alors $x, y \in H \cup K$ et par suite comme $H \cup K$ est un sous-groupe , il s'en suit que $xy \in H \cup K$ et donc $xy \in H$ ou $xy \in K$. Comme $x \notin K$ on en déduit que $xy \notin K$ par suite $xy \in H$ et donc $y \in H$ ce qui implique $K \subset H$.

— Réciproquement, si $H \subset K$ ou $K \subset H$, alors $H \cup K = H$ ou $H \cup K = K$ et dans les deux cas $H \cup K$ est un sous-groupe de G.

Définition 1.1.27 – Sous groupe engendré par une partie Soient $(G, *)$ un groupe et $A \subset G$ une partie de G. On appelle sous-groupe engendré par A qu'on note $\langle A \rangle$, l'intersection de tous les sous-groupes de G contenant A.

Remarque 1.1.28 Soient $(G, *)$ un groupe d'élément neutre e et $A \subset G$, alors d'après la Définition 1.1.27, on en déduit que

1) Le sous-groupe $\langle A \rangle$ est le plus petit sous-groupe de G au sens de l'inclusion contenant A. Ainsi, si F est un sous-groupe de G alors $A \subset F$, si et seulement si $\langle A \rangle \subset F$.

2) A est un sous-groupe de G si et seulement si $\langle A \rangle = A$.

Proposition 1.1.29 – Caractérisation du sous-groupe engendré par une partie. Soient $(G, *)$ un groupe d'élément neutre e et $A \subset G$ une partie de G. Alors,

i) Si $A = \varnothing$, alors $\langle \varnothing \rangle = \{e\}$.

2i) Si $A \neq \varnothing$, alors

$$\langle A \rangle = \left\{ x_1^{\alpha_1} * \cdots * x_n^{\alpha_n} \mid x_1, \ldots, x_n \in A,\ \alpha_1, \ldots, \alpha_n \in \mathbb{Z},\ n \in \mathbb{N}^* \right\}.$$

Démonstration. i) Trivial.

2i) Si $A \neq \varnothing$, on note

$$H = \left\{ x_1^{\alpha_1} * \cdots * x_n^{\alpha_n} \mid x_1, \ldots, x_n \in A,\ \alpha_1, \ldots, \alpha_n \in \mathbb{Z},\ n \in \mathbb{N}^* \right\},$$

alors H est un sous-groupe de G contenant A et par suite $\langle A \rangle \subset H$. Réciproquement, pour tout $x \in H$, il existe $n \in \mathbb{N}^*$, $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ et $x_1, \ldots, x_n \in A$ tels que $x = x_1^{\alpha_1} * \cdots * x_n^{\alpha_n}$, comme $x_1, \ldots, x_n \in A \subset \langle A \rangle$ et $\langle A \rangle$ est un sous-groupe de G, on en déduit que $x \in \langle A \rangle$ et donc $H \subset \langle A \rangle$.

■