Chapitre 1

STRUCTURES ALGÉBRIQUES USUELLES

1.1 Groupes et sous-groupes

Définition 1.1 Groupe

Un ensemble G muni d'une loi $*$ a une structure de groupe si :

- ✓ la loi $*$ est associative : $(x * y) * z = x * (y * z)$ pour tout $(x, y, z) \in G^3$,
- ✓ la loi $*$ admet un élément neutre noté e : $\forall\, x \in G,\ x * e = e * x = x$,
- ✓ tout élément de G admet un symétrique : $\forall\, x \in G,\ \exists\, y \in G\ :\ x * y = y * x = e$.□

- ❑ Un groupe est dit **abélien** (ou commutatif) si la loi $*$ est commutative.
- ❑ Si G est un groupe, alors il existe un unique élément neutre et tout élément admet un unique symétrique.
- ❑ **Groupe produit :** étant donné deux groupes $(G_1, *)$ et $(G_2, *)$, on définit sur le produit cartésien $G = G_1 \times G_2$ l'opération

$$(x_1, x_2) \times (y_1, y_2) \quad = \quad (x_1 * y_1\ ,\ x_2 * y_2).$$

L'opération $\times$ définit sur G une structure de groupe.

Définition 1.2 Sous-groupe

Soit H une partie du groupe $(G, *)$. On dit que H est un sous-groupe de G si :

- ✓ H est stable par la loi $*$: $\forall\, (x, y) \in H^2,\ x * y \in H$,
- ✓ H est un groupe pour la loi induite sur H par la loi $*$ □

Proposition 1.1 Soit H une partie de G, alors H est un sous-groupe de $(G,*)$ si :

$$\begin{cases} e \in H, \\ \forall\,(x,y) \in H^2,\ x*y \in H, \\ \forall\, x \in H,\ x^{-1} \in H, \end{cases} \qquad \text{ou} \qquad \begin{cases} H \neq \varnothing, \\ \forall\,(x,y) \in H^2,\ x*y^{-1} \in H. \end{cases}$$

- Une intersection de sous-groupes d'un groupe G est un sous-groupe de G.
- Le centre $Z(G)$ d'un groupe G est un sous-groupe de G. On rappelle que

$$Z(G) \quad := \quad \{g \in G\ ,\ \forall h \in G\ :\ gh\ =\ hg\}.$$

Définition 1.3 **Sous-groupe engendré par une partie**
Soit A une partie du groupe G. L'intersection de tous les sous-groupes de G contenant A est un sous-groupe, il s'appelle le sous-groupe engendré par A et il est noté $\langle A\rangle$. □

Définition 1.4 **partie génératrice**
Une partie A du groupe G est une partie génératrice si $\langle A\rangle\ =\ G$. □

- Le sous-groupe engendré par la partie vide est $\{e\}$.
- Le sous-groupe engendré par une partie à un élément $\{a\}$ est $\{a^k\ :\ k \in \mathbb{Z}\}$. On le note $a\mathbb{Z}$ ou $\mathbb{Z}a$ si G est un groupe additif.
- Le sous-groupe engendré par un ensemble fini $\{a_1, \cdots, a_n\}$ d'éléments commutants deux à deux est

$$\{a_1^{k_1} \cdots a_n^{k_n}\ :\ (k_1, \cdots, k_n)\ \in\ \mathbb{Z}^n\}.$$

  On le note $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$ ou $\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$ si G est un groupe additif.
- L'ensemble $\{(1,i)\ :\ i \in [\![2,n]\!]\}$ engendre $\mathcal{S}_n$.
- L'ensemble $\{(1,2,i)\ :\ i\ \in\ [\![3,n]\!]\}$ engendre $\mathcal{A}_n$.
- Soit E un espace euclidien, alors l'ensemble des réflexions est une partie génératrice du groupe orthogonal $\mathcal{O}(E)$.

Théorème 1.1 **Sous-groupes de** $(\mathbb{Z},+)$
Les sous-groupes de $(\mathbb{Z},+)$ *sont les ensembles* $n\mathbb{Z}$ *avec* $n \in \mathbb{Z}$. □

Définition 1.5 **Congruence modulo n**
Soit $n \in \mathbb{N}$ fixé. Les entiers $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ sont dits congrus modulo n si $b - a \in n\mathbb{Z}$. On note alors $a \mathcal{R} b$. □

☞ La relation $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$. L'ensemble dont les éléments sont les classes d'équivalences selon la relation $\mathcal{R}$ se note $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} \quad = \quad \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

☞ Muni de l'addition $\overline{a+b} = \overline{a}+\overline{b}$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif.

1.2 Morphismes de groupes

Définition 1.6 Soient $(G_1, \perp)$ et $(G_2, *)$ deux groupes et φ une application de G_1 dans G_2. On dit que φ est un morphisme de $(G_1, \perp)$ dans $(G_2, *)$ si

$$\forall (x, y) \in G_1 \times G_1, \qquad \varphi(x \perp y) = \varphi(x) * \varphi(y).$$

On note $\mathrm{Hom}(G_1, G_2)$ l'ensemble des morphismes de $(G_1, \perp)$ dans $(G_2, *)$. □

Proposition 1.2 **Sous-groupes et morphismes**
Soient $(G_1 \perp)$ et $(G_2, *)$ des groupes d'éléments neutres e_1 et e_2 et $\varphi \in \mathrm{Hom}(G_1, G_2)$. Alors :

- ✓ $\varphi(e_1) = e_2$ et pour tout $x \in G_1$ on a : $\varphi(x^{-1}) = (\varphi(x))^{-1}$,
- ✓ si H_1 est un sous-groupe de $(G_1, \perp)$ alors $\varphi(H_1)$ est un sous-groupe de $(G_2, *)$,
- ✓ si H_2 est un sous-groupe de $(G_2, *)$ alors $\varphi^{-1}(H_2)$ est un sous-groupe de $(G_1, \perp)$. □

Proposition 1.3 **Noyau et image**
Soit φ un morphisme de $(G_1, \perp)$ dans $(G_2, *)$.

- ✓ Le sous-groupe $\varphi(G_1)$ de G_2 est l'image du morphisme φ, noté $\mathrm{Im}(\varphi)$.
- ✓ Le sous-groupe $\varphi^{-1}(\{e_1\})$ de G_1 est le noyau du morphisme φ, noté $\ker(\varphi)$.
- ✓ Le morphisme φ est injectif si, et seulement si, $\ker(\varphi) = \{e_1\}$. □

Proposition 1.4 **Composition de morphismes**

Soient $(G_1, \times)$, $(G_2, \times)$ et $(G_3, \times)$ des groupes.

- ✓ Si $\varphi_1 \in \mathrm{Hom}(G_1, G_2)$ et $\varphi_2 \in \mathrm{Hom}(G_2, G_3)$, alors $\varphi_2 \circ \varphi_1 \in \mathrm{Hom}(G_1, G_3)$.
- ✓ $(\mathrm{Aut}(G_1), \circ)$ est un groupe. (On note $\mathrm{Aut}(G_1)$ l'ensemble des automorphismes de G_1, i.e. des endomorphismes bijectifs). □

❑ L'application

$$\varepsilon : \mathcal{S}_n \longrightarrow \{-1, +1\}, \qquad \sigma \longmapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

est un morphisme de groupes, appelé la signature. Son noyau, $\ker(\varepsilon)$, est un sous-groupe d'ordre $\frac{n!}{2}$, $(n \geq 2)$, on le note $\mathcal{A}_n$ et on l'appelle le groupe alterné d'indice n.

❑ L'application

$$\det : (\mathrm{GL}_n(\mathbb{K}), \times) \longrightarrow (\mathbb{K}^*, \times), \qquad A \longmapsto \det(A)$$

est un morphisme de groupes dont le noyau (l'ensemble des matrices carrées de déterminant égal à 1) est un sous-groupe de $(\mathrm{GL}_n(\mathbb{K}), \times)$ noté $\mathrm{SL}_n(\mathbb{K})$ (groupe spécial linéaire). $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1.3 Groupes monogènes et cycliques

Définition 1.7

- ✓ On dit qu'un groupe G est monogène s'il est engendré par une partie à un seul élément.
- ✓ On dit qu'un groupe G est cyclique s'il est monogène et fini. □

☞ Soit G un groupe monogène. On dit qu'un élément a est un élément générateur de G si $\{a\}$ est une partie génératrice de G. En général, un groupe monogène possède plusieurs générateurs.

☞ Tout groupe monogène est commutatif.

❑ Le groupe $\mathbb{Z}$ est monogène, il a deux générateurs $+1$ et -1.

❑ L'ensemble des racines n-ièmes de l'unité de $\mathbb{C}$:

$$\mathbb{U}_n \quad = \quad \{z \in \mathbb{C} \ : \ z^n = 1\}$$

est un sous-groupe de $\mathbb{C}$, il est constitué des éléments :

$$1,\ e^{\frac{2i\pi}{n}},\ e^{2\frac{2i\pi}{n}},\ \cdots,\ e^{(n-1)\frac{2i\pi}{n}},$$

il est engendré par $e^{\frac{2i\pi}{n}}$, c'est un groupe cyclique à n éléments.

- ❑ Tout sous-groupe de $\mathbb{Z}$ est monogène. Il possède un seul générateur (0 s'il est réduit à $\{0\}$) et deux générateurs non nuls opposés sinon.
- ❑ Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique de cardinal n. Le morphisme canonique

$$\pi_n\ :\ \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \qquad\qquad x \longmapsto \overline{x}$$

est surjectif et de noyau le sous-groupe $n\mathbb{Z}$.

- ❑ Le groupe des isométries d'un espace euclidien E_2 de dimension 2 est engendré par les réflexions.

1.4 Ordre d'un élément dans un groupe

Soit a un élément du groupe G. L'application

$$\varphi_a\ :\ \mathbb{Z} \longrightarrow G, \qquad\qquad k \longmapsto a^k$$

est un morphisme de groupes d'image le sous-groupe $\langle a \rangle$. Lorsque G est un groupe additif, cette application est $k \longmapsto ka$. Le noyau $\ker(\varphi_a)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un unique entier $n \in \mathbb{N}$.

Définition 1.8 On dit que $a \in G$ est :

- ✓ d'ordre fini si $\ker(\varphi_a) \neq \{0\}$,
- ✓ d'ordre infini si $\ker(\varphi_a) = \{0\}$.

Lorsque a est d'ordre fini, on appelle ordre de a, et l'on note $\omega(a)$, le générateur positif de $\ker(\varphi_a)$. □

- ☞ $\omega(a)$ est le plus petit entier $k \in \mathbb{N}^*$ tel que $a^k = e$.
- ☞ $\omega(a)$ est l'unique entier de $\mathbb{N}^*$ tel que :

$$\forall k \in \mathbb{Z}, \qquad\qquad \omega(a) \,|\, k \quad \Longleftrightarrow \quad a^k = e.$$

L'ordre $\omega(a)$ est le plus petit entier naturel non nul k (au sens de la divisibilité) vérifiant $a^k = e$.

❑ L'ordre du neutre d'un groupe G est égal à 1.
❑ Un élément $z \in (\mathbb{C}, +)$ est d'ordre infini.

Proposition 1.5 Si $a \in G$ est d'ordre fini n, alors l'ordre de l'élément a^r (avec $r \in \mathbb{Z}$) est égal à :

$$\frac{n}{n \wedge r}.$$

✍ Le cardinal du sous-groupe $\langle a \rangle$ est égal à l'ordre de l'élément a. Donc, un élément a d'un groupe G de cardinal n engendre G si, et seulement si, il est d'ordre n.
✍ Si $z \in \mathbb{C}^*$ est d'ordre infini, le sous-groupe $\langle z \rangle$ de $(\mathbb{C}^*, \times)$ est isomorphe à $(\mathbb{Z}, +)$. Si z est d'ordre n, il appartient à $\mathbb{U}_n$. On en déduit $\langle z \rangle \subset \mathbb{U}_n$ et en fait $\langle z \rangle = \mathbb{U}_n$ puisque ces deux groupes ont n éléments.
✍ Si G possède n éléments, alors l'ordre de tout élément $a \in G$ est fini et divise n, en particulier $a^n = e$.
✍ Le groupe multiplicatif $(\mathbb{C}^*, \times)$ possède un unique sous-groupe de cardinal n, à savoir, le groupe $\mathbb{U}_n$.
✍ Les sous-groupes de $\mathbb{U}_n$ sont les $\mathbb{U}_k$ lorsque k parcourt l'ensemble des diviseurs positifs de n. On a :

$$\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m} \qquad \text{et} \qquad \langle \mathbb{U}_n \cup \mathbb{U}_m \rangle = \mathbb{U}_{n \vee m}.$$

Théorème 1.2 *Soit G un groupe monogène.*
✓ *Si G est infini, il est isomorphe à $\mathbb{Z}$.*
✓ *Si G est d'ordre n, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.* □

☞ Tout groupe dont le cardinal est un nombre premier est cyclique. Il est engendré par n'importe lequel de ses éléments différents du neutre.

Proposition 1.6 Soit G un groupe cyclique d'ordre n et a l'un de ses générateurs, alors

$$\langle a^r \rangle = G, \ r \in \mathbb{Z} \qquad \Longleftrightarrow \qquad r \wedge n = 1.$$

✍ Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\overline{k} = k\,\overline{1}$ avec $k \in [\![0, n-1]\!]$ premier avec n.
✍ Les générateurs de $\mathbb{U}_n$ sont les nombres complexes $e^{2i\pi\frac{r}{n}} = \left(e^{\frac{2i\pi}{n}}\right)^r$ avec $r \in [\![0, n-1]\!]$ premier avec n.

✍ $\mathbb{Z}/n\mathbb{Z}$ et, par isomorphisme, tout groupe cyclique d'ordre n possède $\varphi(n)$ générateurs où φ est la fonction d'Euler.

Proposition 1.7 Soit G un groupe monogène à n éléments.

✓ Tout sous-groupe de G est monogène.

✓ Pour tout diviseur d de n, le groupe G contient un et un seul sous-groupe d'ordre d. □

1.5 Anneaux

Définition 1.9 Anneau

Un ensemble A muni de deux lois internes notées $+$ et $\times$ a une structure d'**anneau** si :

✓ $(A, +)$ est un groupe abélien,

✓ la loi $\times$ est associative, possède un élément neutre et est distributive par rapport à la loi $+$.

On note 1_A (resp. 0_A) l'élément neutre pour la multiplication (resp. l'addition).

A est dit commutatif si la loi $\times$ l'est. □

☞ Soit A un anneau commutatif alors on a pour tout $n \in \mathbb{N}^*$ et $(x, y) \in A^2$:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad \text{et} \qquad x^n - y^n = (x-y) \sum_{k=0}^{n-1} x^{n-k-1} y^k.$$

Théorème 1.3 *L'ensemble, noté $U(A)$, des éléments inversibles de A pour la multiplication est un groupe pour cette loi.* □

✍ $U(\mathbb{Z}) = \{-1, +1\}$, $U(\mathcal{L}(E)) = \mathrm{GL}(E)$, $U(\mathcal{M}_n(\mathbb{K})) = \mathrm{GL}_n(\mathbb{K})$.

✍ Si $x \in A$ est un élément nilpotent (i.e. il existe $k \in \mathbb{N}^*$ tel que $x^k = 0_A$), alors $1_A - x$ est inversible.

Définition 1.10 Sous-anneau

Soit $(A, +, \times)$ un anneau. Une partie B de A est un sous-anneau de A si :

✓ B est stable par les lois $+$ et $\times$,

✓ B est un anneau pour les lois induites sur B par $+$ et $\times$. □

Proposition 1.8 B est un sous-anneau de A si, et seulement si :
- ✓ $1_A \in B$,
- ✓ $\forall (x, y) \in B^2, \quad x - y \in B$,
- ✓ $\forall (x, y) \in B^2, \quad x \times y \in B$. □

- ❑ Si B_1 et B_2 sont deux sous-anneaux de A, alors $B_1 \cap B_2$ est un sous-anneau de A.
- ❑ Soit A un anneau commutatif. Un élément non nul $a \in A$ est appelé **diviseur de zéro** s'il existe un élément non nul $b \in A$ tel que $a \times b = 0$.
- ❑ Un anneau commutatif sans diviseurs de zéro est dit **intègre**.

Définition 1.11
Soient A et B deux anneaux. Une application $f : A \longrightarrow B$ est un **morphisme** d'anneaux si :
- ✓ $f(1_A) = 1_B$,
- ✓ $\forall (x, y) \in A^2, \quad f(x + y) = f(x) + f(y)$,
- ✓ $\forall (x, y) \in A^2, \quad f(x \times y) = f(x) \times f(y)$.

Un **isomorphisme** d'anneau est un morphisme d'anneaux bijectif. □

Soit f un morphisme d'un anneau A dans un anneau B, alors $f(A)$ est un sous-anneau de B.

Définition 1.12 **Caractéristique.** On considère l'ordre de 1_A dans le groupe $(A, +)$.
- ✓ Si l'ordre de 1_A est fini, on l'appelle caractéristique de l'anneau A.
- ✓ Si l'ordre de 1_A est infini, on dit que A est de caractéristique nulle. □

- ✍ Si l'ordre de 1_A est fini, la caractéristique de A est le plus petit entier k tel que
$$k1_A \quad = \quad 1_A + 1_A + \cdots + 1_A \quad = \quad 0_A.$$
- ✍ Si l'ordre de 1_A est infini, alors pour tout $n \in \mathbb{N}^*$ on a : $n1_A \neq 0_A$.

Définition 1.13 **Corps.** Un anneau commutatif dans lequel tout élément non nul possède un inverse s'appelle corps commutatif. □

- ☞ Si $\mathbb{K}$ est un corps, alors l'ensemble $U(\mathbb{K}) = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$ est un groupe pour la multiplication.