

Groupes

I Groupes

I. A Définition et exemples

Définition 1.1

Soit G un ensemble et $*$ une loi de composition interne sur G .
On dit que $(G, *)$ est un **groupe** lorsque :

- $*$ est associative ;
- $(G, *)$ possède un élément neutre ;
- tout élément de G possède un symétrique dans G .

Si de plus $*$ est commutative, le groupe est dit **commutatif** ou **abélien**.

Proposition 1.2

Soit $(G, *)$ un groupe.

- Le neutre est unique.
- Le symétrique d'un élément a de G est unique : noté a^{-1} .
- $(a^{-1})^{-1} = a$.
- Les éléments de G sont réguliers pour la loi $*$.

Exemples 1.3 : • $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathcal{M}_{n,p}(\mathbb{C}), +)$, (\mathbb{R}^*, \times) sont des groupes commutatifs.

- $(\text{GL}_n(\mathbb{C}), \times)$ avec $n \geq 2$ est un groupe non commutatif.
- Soit X un ensemble est S_X l'ensemble des bijections de X dans X , (S_X, \circ) est le groupe des permutations de X .
- (S_n, \circ) avec $n \geq 3$ est un groupe non commutatif.

Proposition 1.4 (groupe produit)

Soit $(G_1, *)$ et (G_2, \circ) deux groupes. On définit sur $G_1 \times G_2$ la loi \otimes par :

$$\forall (a, b) \in G_1 \times G_2, \forall (c, d) \in G_1 \times G_2, (a, b) \otimes (c, d) = (a * c, b \circ d).$$

Alors $(G_1 \times G_2, \otimes)$ est un groupe appelé le **groupe produit** des groupes $(G_1, *)$ et (G_2, \circ) .

Remarque 1.5 : Pour $(G_1, *) = (G_2, \circ) = (\mathbb{R}, +)$ on obtient $(\mathbb{R}^2, +)$, et plus généralement, on obtient des structures naturelles de groupes pour $(\mathbb{R}^n, +)$ et $(\mathbb{C}^n, +)$.

I. B Sous-groupes

Définition 1.6

Soit $(G, *)$ un groupe. On dit que H est un **sous-groupe** de G lorsque : H est une partie de G stable par $*$ et H muni de la loi induite par $*$ est un groupe.

Remarque 1.7 : Si H est un sous-groupe de $(G, *)$, alors le neutre de H est le neutre de G .

Proposition 1.8 (caractérisation d'un sous-groupe)

Soit $(G, *)$ un groupe dont le neutre est noté e , H est un sous-groupe de G si et seulement si :

1. $H \subset G$;
2. $e \in H$;
3. $\forall (a, b) \in H^2, a * b \in H$;
4. $\forall a \in H, a^{-1} \in H$.

Proposition 1.9 (caractérisation d'un sous-groupe (V2))

Soit $(G, *)$ un groupe dont le neutre est noté e , H est un sous-groupe de G si et seulement si :

1. $H \subset G$;
2. $e \in H$;
3. $\forall (a, b) \in H^2, a * b^{-1} \in H$.

Remarque 1.10 : Dans les caractérisations ci-dessus des sous-groupe, on peut remplacer la condition $e \in H$ par $H \neq \emptyset$.

Méthode 1.11

Pour montrer qu'un ensemble muni d'une loi de composition interne est un groupe, on montre le plus souvent que c'est un sous-groupe.

Exemples 1.12 :

- Chaîne de groupes pour l'addition : $\{0\} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- Chaîne de groupes pour la multiplication : $\{1\} \subset \{1, -1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$.
- Si E est un espace vectoriel, $\text{GL}(E)$ est un sous-groupe de S_E .

Proposition 1.13 (intersection de sous-groupes)

Soit $(G, *)$ un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de G ;
alors $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Remarque 2.7 : Avec les notation de la définition, $\text{Ker } f$ est un sous-groupe de _____ et $\text{Im } f$ est un sous-groupe de _____.

Proposition 2.8

Soit f un morphisme du groupe $(G, *)$ dans le groupe (H, \circ) .

- f est injectif si et seulement si $\text{Ker } f = \text{_____}$;
- f est surjectif si et seulement si $\text{Im } f = \text{_____}$.

III Groupes $\mathbb{Z}/n\mathbb{Z}$

III. A Congruence

Définition 3.1

Soit $n \in \mathbb{N}$. Deux entiers relatifs a et b sont dits **congrus modulo n** lorsque $a - b \in n\mathbb{Z}$. On note alors : $a \equiv b [n]$.

Proposition 3.2

La relation de congruence modulo n est une relation d'équivalence sur \mathbb{Z} .

Remarque 3.3 : Soit $n \in \mathbb{N}^*$. Les entiers a et b sont congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n . Il y a donc n classes d'équivalences pour la relation congru modulo n .

Notation : Pour $k \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on note \bar{k} la classe d'équivalence de k modulo n et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation d'équivalence congru modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \dots, \overline{(n-1)} \}.$$

III. B Structure de groupe

Dans la suite n est un entier naturel non nul.

Proposition 3.4

La loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ (\alpha, \beta) &\longmapsto \overline{(a+b)} \text{ avec } a, b \in \mathbb{Z} \text{ tels que } \bar{a} = \alpha, \bar{b} = \beta \end{aligned}$$

est bien définie.

Exemple 3.5 : table d'addition de $\mathbb{Z}/6\mathbb{Z}$.

Théorème 3.6

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

Remarque 3.7 : Soit $p, k \in \mathbb{Z}$, alors $p \cdot \bar{k} = \overline{pk}$.

III. C Générateurs de $\mathbb{Z}/n\mathbb{Z}$

Exemple 3.8 : Déterminer les générateurs de $\mathbb{Z}/6\mathbb{Z}$.

Théorème 3.9 (éléments générateurs de $\mathbb{Z}/n\mathbb{Z}$)

Soit $n \in \mathbb{N}^*$ et $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$. Alors :

$$\bar{k} \text{ est générateur de } \mathbb{Z}/n\mathbb{Z} \Leftrightarrow k \wedge n = 1.$$

III. D Groupes cycliques

Définition 3.10

On appelle **groupe cyclique** un groupe monogène fini.

Exemples 3.11 : • Pour tout $n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique : _____ est générateur ;

- Le groupe $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ _____
- Le groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ _____.
- Le groupe (\mathbb{U}_n, \times) des racines $n^{\text{ième}}$ de l'unité est cyclique : $e^{i \frac{2\pi}{n}}$ est générateur.

Théorème 3.12

Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.

Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Remarque 3.13 : L'image d'un générateur de groupe par un isomorphisme de groupe est un générateur.

En particulier, si un groupe G est isomorphe à un groupe monogène, alors G est monogène.

IV Ordre d'un élément dans un groupe

Définition 4.1

Soit G un groupe et $x \in G$. Si le sous-groupe engendré par x est fini, on appelle **ordre** de x le cardinal de $\text{gr}(x)$. Sinon x est dit d'ordre infini.

Théorème 4.2

Soit G un groupe (de loi notée multiplicativement) et $x \in G$,

1er cas : x est d'ordre infini alors :

- $\text{gr}(x) = \{x^k; k \in \mathbb{Z}\}$ est isomorphe à \mathbb{Z} ;
- $\forall k \in \mathbb{Z}, x^k = e \Leftrightarrow k = 0$.

2e cas : x est d'ordre fini alors, en notant n l'ordre de x :

- $\text{gr}(x) = \{e, x, x^2, \dots, x^{n-1}\}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$;
- $\forall k \in \mathbb{Z}, x^k = e \Leftrightarrow k \in n\mathbb{Z}$.

Théorème 4.3

Soit G un groupe fini et $x \in G$, alors l'ordre de x divise le cardinal de G .