

Groupes

1. Définition

Un **groupe** (G, \star) est un ensemble G auquel est associée une opération \star (la **loi de composition**) vérifiant les quatre propriétés suivantes :

- pour tout $x, y \in G$, $x \star y \in G$ (\star est une **loi de composition interne**)
- pour tout $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$ (la loi est **associative**)
- il existe $e \in G$ tel que $\forall x \in G, x \star e = x$ et $e \star x = x$ (e est l'**élément neutre**)
- pour tout $x \in G$ il existe $x' \in G$ tel que $x \star x' = x' \star x = e$ (x' est l'**inverse** de x et est noté x^{-1})

Si de plus l'opération vérifie

$$\text{pour tout } x, y \in G, \quad x \star y = y \star x,$$

on dit que G est un groupe **commutatif** (ou **abélien**).

Exemples.

- $(\mathbb{R}^*, \times), (\mathbb{Q}^*, \times), (\mathbb{C}^*, \times)$ sont des groupes commutatifs.
- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes commutatifs.
- L'ensemble des matrices $n \times n$ inversibles, muni de la multiplication des matrices \times , forme un groupe (\mathcal{GL}_n, \times) , il est non-commutatif car en général $M \times M' \neq M' \times M$.

Puissance. Soit un groupe (G, \star) et $x \in G$.

- $x^n = \underbrace{x \star x \star \dots \star x}_{n \text{ fois}}$,
- $x^0 = e$,
- $x^{-n} = \underbrace{x^{-1} \star \dots \star x^{-1}}_{n \text{ fois}}$.

Pour $x, y \in G$ et $m, n \in \mathbb{Z}$ nous avons :

- $x^m \star x^n = x^{m+n}$,
- $(x^m)^n = x^{mn}$,
- $(x \star y)^{-1} = y^{-1} \star x^{-1}$, attention à l'ordre!
- Si (G, \star) est **commutatif** alors $(x \star y)^n = x^n \star y^n$.

2. Sous-groupes

Soit (G, \star) un groupe. Une partie $H \subset G$ est un **sous-groupe** de G si :

- $e \in H$,
- pour tout $x, y \in H$, on a $x \star y \in H$,
- pour tout $x \in H$, on a $x^{-1} \in H$.

Notez qu'un sous-groupe H est aussi un groupe (H, \star) . La façon la plus rapide de montrer que (H, \star) est un groupe est donc de montrer que c'est un sous-groupe d'un groupe (G, \star) .

Critère pratique pour prouver que H est un sous-groupe de G est :

- H contient au moins un élément,
- et pour tout $x, y \in H$, $x \star y^{-1} \in H$.

Exemples :

- (\mathbb{R}_+^*, \times) est un sous-groupe de (\mathbb{R}^*, \times) .
- (\mathbb{U}, \times) est un sous-groupe de (\mathbb{C}^*, \times) , où $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
- $\{e\}$ et G sont les **sous-groupes triviaux** du groupe G .

Proposition. Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{Z}$.

L'ensemble $n\mathbb{Z}$ désigne l'ensemble des multiples de n : $n\mathbb{Z} = \{k \cdot n \mid k \in \mathbb{Z}\}$.

Soit (G, \star) un groupe et $E \subset G$ un sous-ensemble de G . Le **sous-groupe engendré** par E est le plus petit sous-groupe de G contenant E .

Exemple : dans $(\mathbb{Z}, +)$ et $E = \{a, b\}$, le sous-groupe engendré est $H = n\mathbb{Z}$ où $n = \text{pgcd}(a, b)$.

3. Morphismes de groupes

Soient (G, \star) et (G', \diamond) deux groupes. Une application $f : G \rightarrow G'$ est un **morphisme de groupes** si :

$$\text{pour tout } x, x' \in G \quad f(x \star x') = f(x) \diamond f(x')$$

Exemple : $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$, $\exp(x + x') = \exp(x) \times \exp(x')$.

Pour un morphisme

- $f(e_G) = e_{G'}$,
- pour tout $x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

Un morphisme bijectif est un **isomorphisme**. Deux groupes G, G' sont **isomorphes** s'il existe un morphisme bijectif $f : G \rightarrow G'$.

Exemple : $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ est un isomorphisme bijectif, sa bijection réciproque étant le morphisme : $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$ avec $\ln(x \times x') = \ln(x) + \ln(x')$.

Noyau et image

Soit $f : G \rightarrow G'$ un morphisme de groupes.

- Le **noyau** de f est

$$\text{Ker } f = \{x \in G \mid f(x) = e_{G'}\}$$

Le noyau est donc l'ensemble des éléments de G qui s'envoient par f sur l'élément neutre de G' .

- L'**image** de f est

$$\text{Im } f = \{f(x) \mid x \in G\}$$

Ce sont les éléments de G' qui ont (au moins) un antécédent par f .

Proposition. Soit $f : G \rightarrow G'$ un morphisme de groupes.

- $\text{Ker } f$ est un sous-groupe de G .
- $\text{Im } f$ est un sous-groupe de G' .
- f est injectif si et seulement si $\text{Ker } f = \{e_G\}$
- f est surjectif si et seulement si $\text{Im } f = G'$.

4. Le groupe $\mathbb{Z}/n\mathbb{Z}$

Fixons $n \geq 1$. $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

où \bar{p} désigne la classe d'équivalence de p modulo n .

$$\bar{p} = \bar{q} \iff p \equiv q \pmod{n}$$

ou encore $\bar{p} = \bar{q} \iff \exists k \in \mathbb{Z} \quad p = q + kn$.

L'**addition** sur $\mathbb{Z}/n\mathbb{Z}$ est définie par : $\bar{p} + \bar{q} = \overline{p+q}$.

Proposition. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif de cardinal n

L'élément neutre est $\bar{0}$. L'opposé de \bar{k} est $-\bar{k} = \overline{-k} = \overline{n-k}$.

Groupes cycliques de cardinal fini

Un groupe (G, \star) est un groupe **cyclique** s'il existe un élément $a \in G$ tel que :

$$\text{pour tout } x \in G, \text{ il existe } k \in \mathbb{Z} \text{ tel que } x = a^k$$

Autrement dit le groupe G est engendré par un seul élément a .

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique. En effet il est engendré par $a = \bar{1}$, car tout élément \bar{k} s'écrit $\bar{k} = \underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{k \text{ fois}} = k \cdot \bar{1}$.

Théorème. Si (G, \star) un groupe cyclique de cardinal n , alors (G, \star) est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

5. Le groupe des permutations

Fixons un entier $n \geq 2$.

Proposition. L'ensemble des bijections de $\{1, 2, \dots, n\}$ dans lui-même, muni de la composition des fonctions est un groupe, noté (\mathcal{S}_n, \circ) . Le cardinal de \mathcal{S}_n est $n!$.

Une bijection de $\{1, 2, \dots, n\}$ (dans lui-même) s'appelle une **permutation**. Le groupe (\mathcal{S}_n, \circ) s'appelle le **groupe des permutations** (ou le **groupe symétrique**).

L'élément neutre du groupe est l'identité id , le produit est ici la composition et l'inverse correspond à la bijection réciproque.