1 Groupes

1.1 Définition

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

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

Si de plus l'opération vérifie

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

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 $(\mathscr{G}\ell_2,\times)$, il est non-commutatif car en général $M\times M' \neq M'\times M$.

Puissance. Soit un groupe $(G,\star)$ et $x \in G$.
- $x^n = \underbrace{x\star x\star\cdots\star x}_{n \text{ fois}}$,
- $x^0 = e$,
- $x^{-n} = \underbrace{x^{-1}\star\cdots\star x^{-1}}_{n \text{ fois}}$.

Pour $x,y \in G$ et $m,n \in \mathbb{Z}$ nous avons :
- $x^m \star x^n = x^{m+n}$,
- $(x^m)^n = x^{mn}$,
- $(x\star y)^{-1} = y^{-1}\star x^{-1}$, $\quad$ attention à l'ordre !
- **Si** $(G,\star)$ est **commutatif** alors $(x\star y)^n = x^n \star y^n$.

1.2 Sous-groupes

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

1. $e \in H$,
2. pour tout $x,y \in H$, on a $x\star y \in H$,
3. 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 : $n\mathbb{Z} = \left\{k\cdot n \mid k \in \mathbb{Z}\right\}$.

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 $n = \operatorname{pgcd}(a,b)$.

1.3 Morphismes de groupes

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

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

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

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

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

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

Noyau et image

Soit $f : G \longrightarrow G'$ un morphisme de groupes.
- Le ***noyau*** de f est
$$\boxed{\operatorname{Ker} f = \left\{x \in G \mid f(x) = e_{G'}\right\}}$$
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
$$\boxed{\operatorname{Im} f = \left\{f(x) \mid x \in G\right\}}$$
Ce sont les éléments de G' qui ont (au moins) un antécédent par f.

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

1. *$\operatorname{Ker} f$ est un sous-groupe de G.*
2. *$\operatorname{Im} f$ est un sous-groupe de G'.*
3. $\boxed{\textit{$f$ est injectif si et seulement si } \operatorname{Ker} f = \{e_G\}}$
4. *f est surjectif si et seulement si $\operatorname{Im} f = G'$.*

1.4 Le groupe $\mathbb{Z}/n\mathbb{Z}$

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

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0},\overline{1},\overline{2},\ldots,\overline{n-1}\right\}$$

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

$$\boxed{\overline{p} = \overline{q} \iff p \equiv q \pmod n}$$

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

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

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

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

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 $a = \overline{1}$, car tout élément $\overline{k}$ s'écrit $\overline{k} = \underbrace{\overline{1}+\overline{1}+\cdots\overline{1}}_{k \text{ fois}} = k\cdot\overline{1}$.

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

1.5 Le groupe des permutations

Fixons un entier $n \geqslant 2$.

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

Une bijection de $\{1,2,\ldots,n\}$ (dans lui-même) s'appelle une ***permutation***. Le groupe $(\mathscr{S}_n,\circ)$ 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.