

# Théorie des groupes

## Table des matières

<b>1. Introduction.</b>	<b>2</b>
1.1. Groupes. . . . .	2
1.2. Sous-groupes. . . . .	3

# 1. Introduction.

## 1.1. Groupes.

**Définition 1.1.** Un *groupe* est un ensemble non vide  $G$  avec une opération  $*$  :  $G \times G \rightarrow G$  et qui vérifie les propriétés :

- (1) d'associativité :  $\forall a, b, c \in G, (a * b) * c = a * (b * c)$ .
- (2) d'existence d'un élément neutre :  $\exists e \in G, \forall x \in G, x * e = e * x = x$ .
- (3) d'existence d'un inverse :  $\forall x \in G, \exists y \in G, x * y = y * x = e$ . On note  $y = x^{-1}$

### Exemple 1.2.

1.  $(\mathbb{Z}, +)$  est un groupe.  $+$  :  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ;  $(a, b) \mapsto a + b$  est associatif, l'élément neutre est 0, l'inverse d'un  $n \in \mathbb{Z}$ , est  $n^{-1} := -n$ .
2.  $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +) \dots$
3.  $(\mathbb{R}, \cdot)$  n'est pas un groupe car 0 n'admet pas d'inverse.
4.  $(\mathbb{N}, +)$  n'est pas un groupe car il n'y a pas d'inverse.
5.  $(GL_n, \cdot), GL_n(\mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) \mid \det A \neq 0\}$  est un groupe : le  $+$  est associatif (exo), l'élément neutre est la matrice identité de taille  $n$ , et l'inverse de  $A$  est  $A^{-1}$  et on a bien  $AA^{-1} = A^{-1}A$

**Définition 1.3** (Abélien). Soit  $(G, *)$  un groupe. On dit que  $a \in G$ , et  $b \in G$  *commute* si  $a * b = b * a$ , et que  $G$  est *abélien* ou *commutatif* si  $\forall x, y \in G, x * y = y * x$ .

**Définition 1.4.** On appelle *monoïde* un ensemble non vide  $G$  avec une opération  $*$  :  $G \times G \rightarrow G$  qui satisfait seulement l'associativité et l'existence d'un élément neutre. (sans inverse).

**Remarque 1.5.**  $\{\text{monoïdes}\} \subset \{\text{groupes}\} \subset \{\text{groupes abéliens}\}$

### Notation 1.6.

- (1) On utilise  $*$  ou  $\cdot$  pour l'opération d'un groupe et  $+$  pour un groupe abélien.
- (2) On utilise  $e, e_G, 1, 1_G$  pour l'élément neutre d'un groupe, et 0 lorsqu'il est abélien.
- (3)  $x^{-1} := -x$  dans un groupe abélien.
- (4)  $a * b * c = (a * b * c) = a * (b * c) = abc$
- (5) On définit la puissance d'un groupe  $(G, *)$  par,  $\forall x \in G, n \in \mathbb{Z}, x^n = \begin{cases} e & \text{si } n=0 \\ x * \dots * x & \text{si } n > 0 \\ x^{-1} * \dots * x^{-1} & \text{si } n < 0 \end{cases}$ .

**Exemples 1.7.** Soit  $X$  est un ensemble non-vidé,

1.  $(S_X = \{f : X \rightarrow X \mid f \text{ bijective}\}, \circ)$  forme un groupe non abélien de symétrie  $X$ .
2.  $Y \subset X$  ( $S_Y := \{f : X \rightarrow X \text{ bijective} \mid f(y) = y\}, \circ$ ) forme un groupe

**Exemple 1.8.** Pour  $X = \{1, \dots, n\}_{n \in \mathbb{N} \setminus \{0\}}$ . On note  $S_X = S_n := \{f : X \rightarrow X \text{ bijectives}\}$  le groupe de permutations de  $n$  éléments  $e = \text{id}_f, f^{-1}$  = la réciproque de  $f$ . On note  $\sigma := \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$  Quelques exemples on a  $S_2 := \left\{ \text{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}, S_3 := \left\{ \text{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$ .  $S_2$  est abélien tandis que  $S_3$  ne l'est pas car :  $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ .

**Remarque 1.9.** On montrera que si  $(G, *)$  tel que  $\text{Card } G \leq 5$  alors  $G$  est abélien.

**Exemple 1.10.**  $(\mathbb{Z}/n\mathbb{Z}) := \{\overline{x} = \overline{y} := n \mid (x - y)\} = \{\overline{0}, \dots, \overline{n-1}\}$  est un groupe abélien fini à  $n$  éléments. On a  $\overline{a} + \overline{b} = \overline{a + b}$ . Le  $+$  est associatif dans  $\mathbb{Z}/n\mathbb{Z}$  car il l'est dans  $\mathbb{Z}$ . L'élément neutre est le  $\overline{0}$ . l'inverse de  $\overline{x} = \overline{n - x} = \overline{-x}$

**Définition 1.11** (Ordre). Soit  $(G, *)$  un groupe. On appelle *ordre* de  $G$  son cardinal et on peut écrire sa table de multiplication pour  $*$ .  $G = \{e, g_1, \dots, g_n\}$ .

$*$	$e$	$g_1$	$\dots$	$g_n$
$e$	$e * e$	$e * g_1$	$\dots$	$e * g_n$
$g_1$	$g_1 * e$	$g_1 * g_1$	$\dots$	$g_1 * g_n$
$g_i$	$g_i * g_j$			

$*$	$e$	$g_1$	$\dots$	$g_n$
$e$	$e * e$	$e * g_1$	$\dots$	$e * g_n$
$g_1$	$g_1 * e$	$g_1 * g_1$	$\dots$	$g_1 * g_n$
$g_i$	$g_i * g_j$			

**Proposition 1.12.** Soit  $(G, *)$  un groupe. Alors

- (1) L'élément neutre est unique.
- (2) Pour tout  $x \in G$ , l'inverse de  $x$  est unique.
- (3) En particulier,  $(x^{-1})^{-1} = x$ .

*Démonstration.*

- (1) Supposons que  $e, e' \in G$  sont des éléments neutres de  $G$  alors  $\forall x \in G, e * x = x * e = x = e' * x = x * e'$ . On prend  $x = e'$ . On a  $e' = e * e' = e$  car  $e$  et  $e'$  sont éléments neutre donc  $e' = e$ .
- (2) Soit  $x \in G, y, y' \in G$  deux inverses de  $x$  dans  $G$ .

$$(1) := x * y = y * x = e, (2) := x * y' = y' * x = e$$

$$. \text{ On a } y' = y' * e = y' * (x * y) \stackrel{\text{assoc}}{=} (y' * x) * y = e * y = y.$$

- (3) Comme  $x^{-1}$  est l'inverse de  $x$ ,  $x^{-1} * x = x * x^{-1} = e$  donc  $x$  est l'inverse de  $x^{-1}$  par (2).

□

**Définition 1.13.** Soit  $(G, *)$ ,  $(H, \cdot)$  sont deux groupes, le groupe produit  $(G \times H, \star)$  est défini par:  $\star : (G \times H) \times (G \times H) \rightarrow (G \times H); (g_1, h_1, g_2, h_2) \mapsto (g_1, h_1) \star (g_2, h_2) := (g_1 * g_2, h_1 \cdot h_2)$

- (1) L'associativité s'ensuit de l'associativité de  $*$ , et  $\cdot$ .
- (2) L'élément neutre est  $(e_G, e_H): (g, h) \star (e_G, e_H) = (g * e_G, h \cdot e_H) = (g, h) = (e_G, e_H) \star (g, h)$ .
- (3) L'inverse de  $(g, h) \in G \times H$  est  $(g^{-1}, h^{-1})$ .

## 1.2. Sous-groupes.

**Définition 1.14.** Soit  $(G, *)$  un groupe. On appelle sous-groupe de  $(G, *)$ , un sous-ensemble non vide  $H \subseteq G$  tel que :

- (1)  $e \in H$ ,
- (2)  $\forall x, y \in H, xy \in H$ ,
- (3)  $\forall x \in H, x^{-1} \in H$ .

**Notation 1.15.** On pourra noter pour un sous-groupe de  $G$ ,  $H < G$

**Exemple 1.16.**

1.  $\mathbb{Z} > (\mathbb{R}, +), \mathbb{Q} < (\mathbb{R}, +), \mathbb{R} < (\mathbb{C}, +)$ .
2.  $\mathbb{N}! < (\mathbb{Z}, +)$  car  $-1 \notin \mathbb{N}$ .
3. Soit  $H = 2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\} < \mathbb{Z}$ :
  - a.  $0 \in 2\mathbb{Z}$ .
  - b.  $a = 2m, b = 2n \in H \Rightarrow a + b = 2(m + n) \in H$

c.  $a = 2m \in H \Rightarrow -a = 2(-m) \in H$ .

**Proposition 1.17.** Soit  $(G, *)$  un groupe et  $H \subseteq G$ . Alors  $H$  est un sous groupe de  $G$  si et seulement si  $e \in H$ , et  $\forall x, y \in H, x * y^{-1} \in H$ .

*Démonstration.*

$\Rightarrow$  Supposons que  $H$  soit un sous groupe. Alors il vérifie (A). Montrons que  $H$  est satisfait.

Soit  $(x, y) \in H$ , alors  $y^{-1} \in H \Rightarrow x * y^{-1} \in H$ .

$\Leftarrow$ . Montrons que  $(H, *)$  est que A COMPLETER. Soit  $x \in H, a = e, b = x$ . Alors

$$a * b^{-1} = e * x^{-1} = x^{-1} \in H$$

Soit  $x, y \in H, a = x, b = y^{-1} \Rightarrow a * b^{-1} = x * (y^{-1})^{-1} = x * y \in H$ . □

**Proposition 1.18.** Soit  $(G, *)$  un groupe,  $H \subseteq G$ . Alors  $H < G$  si et seulement si  $(B) := \forall x, y \in H, x * y \in H$  et  $(E) := (H, *)$  forme un groupe.

*Démonstration.*

$\Rightarrow$  Supposons  $H < G$ , alors  $(B)$ . Montrons que  $(H, *)$  forme un groupe.

(1)  $*$  est associatif.

(2)  $H < G \Rightarrow e \in H$  et  $\forall x \in H, x * e = e * x = x$ .

(3) Soit  $x \in H, H < G$  alors  $x^{-1} \in H$  et  $x * x^{-1} = e$ .

$\Leftarrow$  On suppose  $(B)$  et  $(E)$ . Montrons que  $H < G$  donc (A) et (C).

A MONTRER (A)  $(H, *)$  est un groupe, notons  $e_H$  son élément neutre,  $(G, *)$  est un groupe, notons  $e_G$  son élément neutre.

$\forall x \in H \subseteq G, e_G$  élément neutre de  $G$  donc  $x * e_G = e_G * x = x$

Preuve de (c) Soit  $x \in H$ , soit  $g$  l'inverse de  $x$  dans  $G$ ,  $y'$  l'inverse de  $x$  dans  $H$  alors  $x * y' = y' * x = e$  or l'inverse est unique donc  $y = y' \in H$ . □

**Proposition 1.19.** Soit  $(G, *)$  un groupe et  $H_1, H_2 \subseteq G$ . On a  $H_1 \cap H_2 < G$ .  
Plus généralement, si  $(G_i)_{i \in I}$  est une famille de sous-groupes de  $G$ , alors  $\bigcap_{i \in I} H_i < G$ .

*Démonstration.*  $\forall i \in I, e \in G_i, e \in \bigcap_{i \in I} H_i$  donc on a (A). De plus,  $\forall x, y \in \bigcap_{i \in I} H_i, x, y \in H_i \Rightarrow xy^{-1} \in H_i \forall i \in I \Rightarrow xy^{-1} \in \bigcap_{i \in I} H_i$ . □

**Remarque 1.20.** A FAIRE

**Définition 1.21.** Soit  $(G, *)$  un groupe,  $S \subset G$ . On appelle sous-groupe engendré par  $S$ , noté  $\langle S \rangle$  le plus petit sous-groupe de  $G$  contenant  $S$ .

**Remarque 1.22.** équivalent à si  $H < G$  et  $S \subset H$  alors  $\langle S \rangle \subseteq H$

**Proposition 1.23.**  $\langle S \rangle$  est bien défini et on a :

$$\langle S \rangle := \bigcap_{(H < G), S \subset H} H = \{g_1, \dots, g_n \mid g_i \in S \text{ ou } g_i^{-1} \in S\}$$

*Démonstration.*

(1) bien défini : Soit  $I = \{H < G \mid S \subset H\} \neq \{\}$  car  $G \in I$  Soit  $H_I = \bigcap_{H \in I} H < G$  par la prop précédente. Montrons que  $H_I$  est le plus petit ssgpe contenant

(a)  $S \subset H, \forall H \in I, S \subset H_I$

(b) Soit  $H < G$  tel que  $S \subset H \Rightarrow H_I < H$  Or  $H \in I$  donc  $I_I = H \cap \left( \bigcap_{H' \in I} H' \right) \subset H$  donc  $\langle S \rangle = H_I$ .

(2) Montrons que  $\langle S \rangle = H_S$  par double inclusion.

(a)  $H_S \subset \langle S \rangle$

$H_S < G$  car  $e = gg^{-1} \in H_S$  pour un  $g \in S$  Si  $x = (g_1)$

A FAIRE

□

### Définition 1.24.

(1) Si  $G = \langle S \rangle$ , on dit que  $G$  est engendré par  $S$  ou que  $S$  est un système de générateurs pour  $G$ .

(2) Si  $S = \{g_1, \dots, g_n\}$ , on note  $\langle S \rangle = \langle g_1, \dots, g_n \rangle$ .

(3) Si  $G = \langle x \rangle, x \in G$  on dit que  $G$  est monogène, si de plus  $G$  est fini, on dit qu'il est cyclique.

(4) On dit que  $G$  est finiment engendré si  $\exists S \subset G$  fini tel que  $G = \langle S \rangle$ .

### Exemple 1.25.

1.  $G = \langle G \rangle$

2.  $(\mathbb{Z}, +) = \langle 1 \rangle = \langle 2, 3 \rangle$  est monogène

3.  $(\mathbb{Z}^2, +) = \langle (1,0), (0,1) \rangle$ :  $1 = 3 - 2 \in \langle 2, 3 \rangle \Rightarrow \langle 1 \rangle \subseteq \langle 2, 3 \rangle$

4.  $(\mathbb{Z}/_3\mathbb{Z} \times \mathbb{Z}/_5\mathbb{Z}, +) = \langle (\bar{1}, \bar{1}) \rangle$ . (exo)

5.  $(\mathbb{Z}/_n\mathbb{Z}, +) = \langle \bar{1} \rangle$  est cyclique.

6.  $(S_n, \circ)$  n'est pas cyclique pour  $n > 2$

**Lemme 1.26.** Tout groupe monogène est abélien.

*Démonstration.*  $G$  monogène  $\Rightarrow \exists x \in G = \langle x \rangle = \{g_1, \dots, g_n\}$

□