

# Théorie des groupes

## Table des matières

<b>1. Groupes</b>	<b>2</b>
<b>2. Sous-groupes</b>	<b>3</b>
2.1. Définitions . . . . .	3
2.2. Générateurs . . . . .	4
2.3. Ordre d'un élément . . . . .	5
<b>3. Morphismes de groupes</b>	<b>6</b>
3.1. Définitions . . . . .	6
3.2. Image et noyau . . . . .	7
<b>4. Groupes symétriques</b>	<b>8</b>
4.1. Définitions . . . . .	8
4.2. $k$ -cycles . . . . .	8
4.3. Permutations conjuguées . . . . .	9
4.4. Signature d'une permutation . . . . .	10
4.5. Groupes alternés . . . . .	11
<b>5. Groupes quotients</b>	<b>12</b>
5.1. Relations d'équivalence . . . . .	12
5.2. Classes modulo un sous-groupe . . . . .	13
5.3. Théorème du nombre de classes et théorème de Lagrange . . . . .	14
5.4. Sous-groupes distingués et groupes quotients . . . . .	14
<b>6. Actions de groupes</b>	<b>17</b>
6.1. Définitions . . . . .	17

# 1. Groupes

**Définition 1.1.** test Soit  $G$  un ensemble et  $\star : G \times G \longrightarrow G$  une loi de composition interne. On dit que le couple  $(G, \star)$  forme un *groupe* s'il vérifie les propriétés suivantes

1. la loi  $\star$  est associative,  $\forall x, y, z \in G, (x \star y) \star z = x \star (y \star z)$ ,
2. il existe un neutre  $e_G \in G, \forall x \in G, x \star e_G = e_G \star x = x$ ,
3. existence d'un inverse,  $\forall x \in G, \exists x^{-1} \in G, x \star x^{-1} = x^{-1} \star x = e_G$ .

**Exemple 1.2.** Le couple  $(\mathbb{Z}, +)$  est un groupe, le neutre est 0 et pour  $n \in \mathbb{Z}$  un inverse est  $-n$ . Le couple  $(\mathbb{R}, \cdot)$  n'est pas un groupe, 0 n'admet pas d'inverses.

**Proposition 1.3.** Soit  $(G, \star)$  un groupe. Alors

1. le neutre  $e_G$  est unique,
2. soit  $x \in G$ , alors son inverse  $x^{-1}$  est unique.

*Démonstration.*

1. Soit  $e \in G$  vérifiant  $\forall x \in G, x \star e = e \star x = x$ . Alors

$$e = e \star e_G = e_G.$$

2. Soit  $y \in G$  vérifiant  $x \star y = y \star x = e_G$ . Alors

$$y = e_G \star y = (x^{-1} \star x) \star y = x^{-1} \star (x \star y) = x^{-1} \star e_G = x^{-1}.$$

□

**Définition 1.4.** Soit  $(G, \star)$  un groupe. On dit qu'il est *commutatif* ou *abélien* s'il vérifie

$$\forall x, y \in G, x \star y = y \star x.$$

**Exemple 1.5.** Le groupe  $(\mathbb{Z}, +)$  est commutatif.

**Définition 1.6.** Soit  $(G, \star)$  un groupe. On appelle *ordre* de  $G$  le cardinal de  $G$ , si  $G$  est un ensemble fini on dit que  $G$  est d'*ordre fini*, sinon on dit que  $G$  est d'*ordre infini*.

**Remarque 1.7.** Soit  $(G, \star)$  un groupe d'ordre fini. On note  $G = \{e_G, g_1, \dots, g_n\}$ , alors on peut donner sa table de multiplication

$\star$	$e_G$	$g_1$	$\dots$	$g_j$	$\dots$	$g_n$
$e_G$	$e_G$	$g_1$	$\dots$	$g_j$	$\dots$	$g_n$
$g_1$	$g_1$	$g_1 \star g_1$	$\dots$	$g_1 \star g_j$	$\dots$	$g_1 \star g_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$g_i$	$g_i$	$g_i \star g_1$	$\dots$	$g_i \star g_j$	$\dots$	$g_i \star g_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$g_n$	$g_n$	$g_n \star g_1$	$\dots$	$g_n \star g_j$	$\dots$	$g_n \star g_n$

où chaque ligne et chaque colonne contient tous les éléments de  $G$ .

**Notation 1.8.** Soit  $(G, \star)$  un groupe. Lorsqu'il ne peut pas y avoir de confusions, on notera

- $e := e_G$  pour le neutre,
- $\forall x, y \in G, xy := x \star y$  pour la loi  $\star$ ,
- $\forall x \in G, \forall n \in \mathbb{Z}$ , si  $n > 0, x^n := \underbrace{x \star \dots \star x}_{n \text{ fois}}$ , si  $n = 0, x^0 := e$ , si  $n < 0, x^n := x^{-1} \star \dots \star x^{-1}$ .

## 2. Sous-groupes

### 2.1. Définitions

**Définition 2.1.** Soit  $(G, \star)$  un groupe et  $H$  un sous-ensemble de  $G$ . On dit que  $H$  est un *sous-groupe* de  $G$ , noté  $H < G$ , s'il vérifie les propriétés suivantes

1. le neutre appartient à  $H$ ,  $e \in H$ ,
2.  $H$  est stable par  $\star$ ,  $\forall x, y \in H, x \star y \in H$ ,
3.  $H$  est stable par inverse,  $\forall x \in H, x^{-1} \in H$ .

**Définition 2.2.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . On dit que  $H$  est *distingué* ou *normal*, noté  $H \triangleleft G$ , s'il vérifie

$$\forall g \in G, \forall h \in H, g \star h \star g^{-1} \in H.$$

**Proposition 2.3.** Soit  $(G, \star)$  un groupe et  $H$  un sous-ensemble de  $G$ . Alors  $H$  est un sous-groupe de  $G$  si et seulement s'il vérifie les propriétés suivantes

1. le neutre appartient à  $H$ ,  $e \in H$ ,
2.  $H$  est stable par  $\star$  et par inverse,  $\forall x, y \in H, x \star y^{-1} \in H$ .

*Démonstration.*

$\Rightarrow$  : Supposons que  $H$  est un sous-groupe de  $G$ . Alors

1. le neutre appartient à  $H$ ,
2. soit  $x, y \in H$ , alors  $y^{-1} \in H$  et  $x \star y^{-1} \in H$ .

$\Leftarrow$  : Supposons que  $H$  vérifie les deux propriétés. Alors

1. le neutre appartient à  $H$ ,
3. soit  $x \in H$ , alors  $x^{-1} = e \star x^{-1} \in H$ ,
2. soit  $x, y \in H$ , alors  $y^{-1} \in H$  et  $x \star y = x \star (y^{-1})^{-1} \in H$ .

□

**Proposition 2.4.** Soit  $(G, \star)$  un groupe et  $H$  un sous-ensemble de  $G$ . Alors  $H$  est un sous-groupe de  $G$  si et seulement s'il vérifie les propriétés suivantes

1.  $H$  est stable par  $\star$ ,  $\forall x, y \in H, x \star y \in H$ ,
2. le couple  $(H, \star)$  forme un groupe.

*Démonstration.*

$\Rightarrow$  : Supposons que  $H$  est un sous-groupe de  $G$ . Alors

1.  $H$  est stable par  $\star$ ,  $\forall x, y \in H, x \star y \in H$ ,
2. On considère le couple  $(H, \star)$ ,
  1. soit  $x, y, z \in H$ , alors  $x, y, z \in G$  donc  $(x \star y) \star z = x \star (y \star z)$ ,
  2. on pose  $e_H = e_G$ , alors  $e_H \in H$ ,
  3. soit  $x \in H$ , alors  $x^{-1} \in H$ .

Donc  $(H, \star)$  forme un groupe.

$\Leftarrow$  : Supposons que  $H$  vérifie les deux propriétés. Alors

1. soit  $x \in H$ , alors  $x \in G$  et  $x \star e_G = x = x \star e_H$ , en multipliant à gauche par  $x^{-1} \in G$ , on obtient donc  $e_G = e_H \in H$ .
2.  $H$  est stable par  $\star$ ,
3. soit  $x \in H$ , alors  $x^{-1} \in H$ .

□

**Proposition 2.5.** Soit  $(G, \star)$  un groupe et  $H_1, H_2$  deux sous-groupes de  $G$ . Alors  $H_1 \cap H_2$  est un sous-groupe de  $G$ .

*Démonstration.*

1.  $e \in H_1$  et  $e \in H_2$ , donc  $e \in H_1 \cap H_2$ ,
2. soit  $x, y \in H_1 \cap H_2$ , alors  $x, y \in H_1$ , puisque  $H_1$  est un sous-groupe de  $G$  on a  $x \star y^{-1} \in H_1$ , de la même manière on a  $x \star y^{-1} \in H_2$ , donc  $x \star y^{-1} \in H_1 \cap H_2$ .

Donc d'après la Proposition 2.3,  $H_1 \cap H_2$  est un sous-groupe de  $G$ .  $\square$

## 2.2. Générateurs

**Définition 2.6.** Soit  $(G, \star)$  un groupe et  $S$  un sous-ensemble non-vide de  $G$ . On appelle *sous groupe engendré par  $S$* , noté  $\langle S \rangle$ , le plus petit sous-groupe de  $G$  contenant  $S$ .

**Notation 2.7.** Si  $S = \{x_1, \dots, x_n\}$ , on note  $\langle x_1, \dots, x_n \rangle := \langle S \rangle$ .

**Proposition 2.8.** Soit  $(G, \star)$  un groupe et  $S$  un sous-ensemble non-vide de  $G$ . Alors

$$\langle S \rangle = \bigcap_{\substack{H < G \\ S \subset H}} H$$

ou encore  $\langle S \rangle = \{x_1 \star \dots \star x_n \mid n \in \mathbb{N} \setminus \{0\}, \forall i \in \{1, \dots, n\}, x_i \in S \text{ ou } x_i^{-1} \in S\}$ .

*Démonstration.* Notons  $F := \{H < G \mid S \subset H\}$  et  $H_S := \bigcap_{H \in F} H$ . Puisque  $G \in F$ , l'intersection est non-vide, et d'après la Proposition 2.5,  $H_S$  est un sous-groupe de  $G$ . De plus  $H_S$  contient évidemment  $S$ . Enfin si  $H_0$  est un sous-groupe de  $G$  contenant  $S$ , on a  $H_0 \in F$ , donc  $H_0 \subset H_S$ . Donc  $H_S$  est bien le plus petit sous-groupe de  $G$  contenant  $S$ .

Notons  $K_S := \{x_1 \star \dots \star x_n \mid n \in \mathbb{N} \setminus \{0\}, \forall i \in \{1, \dots, n\}, x_i \in S \text{ ou } x_i^{-1} \in S\}$ . On remarque que  $K_S$  est stable par multiplication, par inverse et contient le neutre de  $G$ , donc d'après la Proposition 2.3,  $K_S$  est un sous-groupe de  $G$ . De plus  $K_S$  contient  $S$ , donc  $\langle S \rangle \subset K_S$ . Réciproquement, puisque  $\langle S \rangle$  est un groupe, on en déduit que  $\forall x \in K_S, x \in \langle S \rangle$ , donc  $K_S \subset \langle S \rangle$ . Par double inclusion  $\langle S \rangle = K_S$ .  $\square$

**Définition 2.9.** Soit  $(G, \star)$  un groupe et  $S$  un sous-ensemble de  $G$ . Si  $G = \langle S \rangle$ , on dit que  $G$  est engendré par  $S$  et on appelle  $S$  un *système de générateurs* pour  $G$ .

- Si  $S$  est fini, on dit que  $G$  est *finiment engendré*.
- Si  $S$  ne contient qu'un élément, on dit que  $G$  est *monogène*, si de plus  $G$  est fini, on dit que  $G$  est *cyclique*.

**Exemple 2.10.**

1. Soit  $(G, \star)$  un groupe,  $G$  a au moins un système de générateur  $S := G$ .
2. On considère le groupe  $(\mathbb{Z}, +)$ , il est engendré par  $\mathbb{N}$ , et par  $\{1\}$ , donc il est monogène.
3. On considère le groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$ , il est engendré par  $\{\bar{1}\}$  et est fini, donc il est cyclique.

**Proposition 2.11.** On considère le groupe  $(\mathbb{Z}, +)$ , alors

1.  $\forall n \in \mathbb{Z}, \langle n \rangle = n\mathbb{Z}$ ,
2. soit  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$ , alors il existe  $n \in \mathbb{Z}$  tel que  $H = n\mathbb{Z}$ ,
3. soit  $a, b \in \mathbb{Z}$  avec  $b \neq 0$ , alors  $b$  divise  $a$  si et seulement si  $\langle a \rangle \subset \langle b \rangle$ ,
4. soit  $a, b \in \mathbb{Z} \setminus \{0\}$ , alors  $\langle a, b \rangle = \text{pgcd}(a, b)\mathbb{Z}$  et  $\langle a \rangle \cap \langle b \rangle = \text{ppcm}(a, b)\mathbb{Z}$ .

*Démonstration.*

1. Soit  $n \in \mathbb{Z}$ , alors  $\langle n \rangle = \{k \cdot n \mid k \in \mathbb{Z}\} = n\mathbb{Z}$ .
2. • Si  $H = \{0\}$ , alors  $H = 0\mathbb{Z}$ .

- Sinon,  $H \setminus \{0\}$  est non-vide, on prend  $n$  le plus petit entier strictement positif de  $H$ .  
Puisque  $n \in H$ , on a  $n\mathbb{Z} \subset H$ . Réciproquement, soit  $m \in H$ , par division euclidienne il existe  $q, r \in \mathbb{Z}$  tels que  $m = nq + r$  et  $0 \leq r < n$ , puisque  $r = m - nq \in H$ , on a nécessairement  $r = 0$ , d'où  $m \in n\mathbb{Z}$ , donc  $H \subset n\mathbb{Z}$ . Donc  $H = n\mathbb{Z}$ .
- 3. On sait que  $b$  divise  $a$  si et seulement il existe  $q \in \mathbb{Z}$  tel que  $a = bq$  si et seulement  $a \in \langle b \rangle$  si et seulement si  $\langle a \rangle \subset \langle b \rangle$ .
- 4. *TODO* : Voir TD.

□

### 2.3. Ordre d'un élément

**Définition 2.12.** Soit  $(G, \star)$  un groupe et  $x \in G$ . On appelle *ordre de  $x$* , noté  $\text{ord}(x)$ , le cardinal du sous-groupe engendré par  $\{x\}$ .

**Proposition 2.13.** Soit  $(G, \star)$  un groupe et  $x \in G$ . Alors

$$\text{ord}(x) = \inf(\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\})$$

de plus si  $n \in \mathbb{Z}$  vérifie  $x^n = e$ , alors  $\text{ord}(x)$  divise  $n$ .

*Démonstration.*

- Si  $\text{ord}(x) = +\infty$ , supposons par l'absurde qu'il existe  $d \in \mathbb{N} \setminus \{0\}$  tel que  $x^d = e$ .  
Alors  $\langle x \rangle = \{e, x, \dots, x^{d-1}\}$  est fini, d'où une contradiction.
- Sinon  $\text{ord}(x) \in \mathbb{N} \setminus \{0\}$ .  
Puisque  $\langle x \rangle$  est fini, il existe  $m, n \in \mathbb{N} \setminus \{0\}$  tels que  $n < m$  et  $x^m = x^n$ , alors  $x^{m-n} = e$ , donc l'ensemble  $\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\}$  est non-vide. Posons  $d := \inf(\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\})$ , puisque  $x^d = e$ , on obtient  $\langle x \rangle = \{e, x, \dots, x^{d-1}\}$ , donc  $\text{ord}(x) = |\{e, x, \dots, x^{d-1}\}| = d$ .
- Soit  $n \in \mathbb{Z}$  tel que  $x^n = e$ . Par division euclidienne il existe  $q, r \in \mathbb{Z}$  tels que  $n = \text{ord}(x)q + r$  et  $0 \leq r < d$ , alors  $x^r = x^{n - \text{ord}(x)q} = x^n \star x^{\text{ord}(x) \cdot (-q)} = e$ , par définition de  $\text{ord}(x)$  on a nécessairement  $r = 0$ , donc  $\text{ord}(x)$  divise  $n$ .

□

### 3. Morphismes de groupes

#### 3.1. Définitions

**Définition 3.1.** Soit  $(G, \star)$  et  $(H, \cdot)$  deux groupes. Une application  $\varphi : G \longrightarrow H$  est un *morphisme de groupes* si elle vérifie

$$\forall x, y \in G, \varphi(x \star y) = \varphi(x) \cdot \varphi(y).$$

- Si  $H = G$ , on dit que  $\varphi$  est un *endomorphisme*.
- Si  $\varphi$  est une bijection, on dit que  $\varphi$  est un *isomorphisme*, et  $G$  et  $H$  sont *isomorphes*, noté  $G \simeq H$ .

**Proposition 3.2.** Soit  $(G, \star)$  et  $(H, \cdot)$  deux groupes, et  $\varphi : G \longrightarrow H$  un morphisme de groupes.

1. le neutre est envoyé sur le neutre,  $\varphi(e_G) = e_H$ ,
2. l'inverse est envoyé sur l'inverse,  $\forall x \in G, \varphi(x^{-1}) = \varphi(x)^{-1}$ .

*Démonstration.*

1. On a  $\varphi(e_G) = \varphi(e_G \star e_G) = \varphi(e_G) \cdot \varphi(e_G)$ , donc  $\varphi(e_G) = e_H$ ,
2. soit  $x \in G$ , alors  $e_H = \varphi(e_G) = \varphi(x \star x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$ , donc  $\varphi(x^{-1}) = \varphi(x)^{-1}$ .

□

**Proposition 3.3.** Soit  $(G, \star)$  et  $(H, \cdot)$  deux groupes, et  $\varphi : G \longrightarrow H$  un isomorphisme. Alors son inverse, noté  $\varphi^{-1}$ , est un isomorphisme.

*Démonstration.* Soit  $x, y \in H$ . Puisque  $\varphi$  est un morphisme de groupes on a

$$\varphi(\varphi^{-1}(x \cdot y)) = x \cdot y = \varphi(\varphi^{-1}(x)) \cdot \varphi(\varphi^{-1}(y)) = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(y))$$

et par injectivité de  $\varphi$ , on obtient  $\varphi^{-1}(x \cdot y) = \varphi^{-1}(x) \star \varphi^{-1}(y)$ , donc  $\varphi^{-1}$  est un morphisme. □

**Proposition 3.4.** Soit  $(G, \star)$ ,  $(H, \cdot)$  et  $(K, \blacksquare)$  trois groupes, et  $\varphi : G \longrightarrow H$  et  $\psi : H \longrightarrow K$  deux morphismes de groupes. Alors  $\psi \circ \varphi$  est un morphisme de groupes.

*Démonstration.* Soit  $x, y \in G$ . Alors

$$\begin{aligned} (\psi \circ \varphi)(x \star y) &= \psi(\varphi(x \star y)) \\ &= \psi(\varphi(x) \cdot \varphi(y)) \\ &= \psi(\varphi(x)) \blacksquare \psi(\varphi(y)) \\ &= (\psi \circ \varphi)(x) \blacksquare (\psi \circ \varphi)(y) \end{aligned}$$

donc  $\psi \circ \varphi$  est un morphisme de groupes. □

**Proposition 3.5.** Soit  $(G, \star)$  et  $(H, \cdot)$  deux groupes isomorphes. Alors

1.  $G$  et  $H$  ont le même ordre,
2.  $G$  est abélien si et seulement si  $H$  est abélien,
3.  $G$  est monogène si et seulement si  $H$  est monogène,
4.  $\forall \varphi : G \longrightarrow H$  isomorphisme,  $\forall x \in G, \text{ord}(x) = \text{ord}(\varphi(x))$ .

*Démonstration.* Soit  $\varphi : G \longrightarrow H$  un isomorphisme.

1.  $G$  et  $H$  sont en bijection, donc  $|G| = |H|$ .
2.  $\Rightarrow$  : Supposons que  $G$  est abélien. Soit  $x, y \in H$ , puisque  $\varphi$  est un isomorphisme

$$\varphi^{-1}(x) \star \varphi^{-1}(y) = \varphi^{-1}(y) \star \varphi^{-1}(x) \Rightarrow x \cdot y = y \cdot x$$

donc  $H$  est abélien.

$\Leftarrow$  : On montre la réciproque de la même manière.

3.  $\Rightarrow$  : Supposons que  $G$  est monogène. Alors il existe  $x \in G$  tel que  $G = \langle x \rangle$ , ainsi

$$H = \varphi(G) = \varphi(\langle x \rangle) = \langle \varphi(x) \rangle$$

donc  $H$  est monogène.

$\Rightarrow$  : On montre la réciproque de la même manière.

4. Soit  $x \in G$ , alors  $\forall d \in \mathbb{N} \setminus \{0\}, x^d = e_G \Leftrightarrow \varphi(x)^d = e_H$ , donc  $\text{ord}(x) = \text{ord}(\varphi(x))$ .

□

### 3.2. Image et noyau

**Définition 3.6.** Soit  $(G, \star)$  et  $(H, \cdot)$  deux groupes, et  $\varphi : G \rightarrow H$  un morphisme de groupes.

- On appelle *image* de  $\varphi$  l'ensemble  $\text{im}(\varphi) := \varphi(G)$ .
- On appelle *noyau* de  $\varphi$  l'ensemble  $\ker(\varphi) := \varphi^{-1}(e_H)$ .

**Proposition 3.7.** Soit  $(G, \star)$  et  $(H, \cdot)$  deux groupes, et  $\varphi : G \rightarrow H$  un morphisme de groupes. Alors  $\text{im}(\varphi)$  est un sous-groupe de  $H$  et  $\ker(\varphi)$  est un sous-groupe de  $G$ . Plus généralement si  $G'$  est un sous groupe de  $G$  et  $H'$  un sous-groupe de  $H$ , alors  $\varphi(G')$  est un sous-groupe de  $H$  et  $\varphi^{-1}(H')$  est un sous-groupe de  $G$ .

*Démonstration.* On considère  $\varphi(G')$ ,

1.  $e_H = \varphi(e_G)$ , donc  $e_H \in \varphi(G')$ ,
2. soit  $x, y \in \varphi(G')$ , il existe  $u, v \in G'$  tels que  $x = \varphi(u)$  et  $y = \varphi(v)$ , alors

$$x \cdot y^{-1} = \varphi(u) \cdot \varphi(v)^{-1} = \varphi(u \star v^{-1})$$

puisque  $G'$  est un sous-groupe de  $G$ , on a  $u \star v^{-1} \in G'$ , donc  $x \cdot y^{-1} \in \varphi(G')$ .

D'après la Proposition 3.3,  $\varphi(G')$  est un sous-groupe de  $H$ .

On considère  $\varphi^{-1}(H')$ ,

1.  $e_G = \varphi(e_H)$ , donc  $e_G \in \varphi^{-1}(H')$ .
2. soit  $x, y \in \varphi^{-1}(H')$ , alors  $\varphi(x), \varphi(y) \in H'$  et

$$x \star y^{-1} \in \varphi^{-1}(H') \Leftrightarrow \varphi(x \star y^{-1}) \in H' \Leftrightarrow \varphi(x) \cdot \varphi(y)^{-1} \in H'$$

puisque  $H'$  est un sous-groupe de  $H$ , on a  $\varphi(x) \cdot \varphi(y)^{-1} \in H'$ , donc  $x \star y^{-1} \in \varphi^{-1}(H')$ .

D'après la Proposition 3.3,  $\varphi^{-1}(H')$  est un sous-groupe de  $G$ .

□

**Proposition 3.8.** Soit  $(G, \star)$  et  $(H, \cdot)$  deux groupes, et  $\varphi : G \rightarrow H$  un morphisme de groupes.

- $\varphi$  est surjectif si et seulement si  $\text{im}(\varphi) = H$ .
- $\varphi$  est injectif si et seulement si  $\ker(\varphi) = \{e_G\}$ .

*Démonstration.*

- Par définition.
- $\Rightarrow$  : Supposons que  $\varphi$  est injectif. Soit  $x \in \ker(\varphi)$ , alors  $\varphi(x) = e_H$ , donc  $x = e_G$ .  
 $\Leftarrow$  : Supposons que  $\ker(\varphi) = \{e_G\}$ . Soit  $x, y \in G$  tels que  $\varphi(x) = \varphi(y)$ , puisque  $\varphi$  est un morphisme on a  $\varphi(x \star y^{-1}) = e_H$ , et  $\ker(\varphi) = \{e_G\}$  d'où  $x \star y^{-1} = e_G$ , donc  $x = y$  et  $\varphi$  est injectif.

□

## 4. Groupes symétriques

### 4.1. Définitions

**Définition 4.1.** Soit  $n \in \mathbb{N}$ . On appelle *groupe symétrique*, noté  $S_n$ , l'ensemble de toutes les bijections de  $\{1, \dots, n\}$  dans lui-même muni de la composition.

- On appelle *permutations* les éléments de  $S_n$ .
- Soit  $\sigma$  une permutation, on la note

$$\sigma := \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}.$$

**Définition 4.2.** Soit  $\sigma \in S_n$  une permutation. On appelle *support* de  $\sigma$  l'ensemble

$$\text{supp}(\sigma) := \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}.$$

**Lemme 4.3.** Soit  $\sigma_1, \sigma_2 \in S_n$  deux permutations. Si  $\sigma_1$  et  $\sigma_2$  sont de supports disjoints, alors elles commutent.

*Démonstration.* Soit  $i \in \{1, \dots, n\}$ . Alors

- si  $i \notin \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$ , on a  $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$ ,
- si  $i \in \text{supp}(\sigma_1)$ , alors  $i \notin \text{supp}(\sigma_2)$  et  $\sigma_1(i) \notin \text{supp}(\sigma_2)$ , et on a  $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$ ,
- si  $i \in \text{supp}(\sigma_2)$ , de la même manière  $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$ .

Donc  $\sigma_1$  et  $\sigma_2$  commutent. □

### 4.2. $k$ -cycles

**Définition 4.4.** Soit  $a_1, \dots, a_k \in \{1, \dots, n\}$  deux à deux distincts. On appelle  *$k$ -cycle*, noté  $(a_1, \dots, a_k)$ , la permutation définie par

$$\forall i \in \{1, \dots, n\}, (a_1, \dots, a_k)(i) := \begin{cases} a_{j+1} & \text{si } j \in \{1, \dots, k-1\} \text{ avec } i = a_j \\ a_1 & \text{si } i = a_k \\ i & \text{sinon} \end{cases}$$

- On dit que  $k$  est sa *longueur*.
- On appelle *transposition* un 2-cycle.

**Proposition 4.5.** Soit  $(a_1, \dots, a_k) \in S_n$  un  $k$ -cycle. Alors l'inverse de  $(a_1, \dots, a_k)$  est  $(a_k, \dots, a_1)$ .

*Démonstration.* Soit  $i \in \{1, \dots, n\}$ . Alors

- s'il existe  $j \in \{1, \dots, k-1\}$  tel que  $i = a_j$ , on a

$$(a_k, \dots, a_1)((a_1, \dots, a_k)(a_j)) = (a_k, \dots, a_1)(a_{j+1}) = a_j = i,$$

- si  $i = a_k$ , on a

$$(a_k, \dots, a_1)((a_1, \dots, a_k)(a_k)) = (a_k, \dots, a_1)(a_1) = a_k = i,$$

- sinon on a

$$(a_k, \dots, a_1)((a_1, \dots, a_k)(i)) = (a_k, \dots, a_1)(i) = i.$$

Donc  $(a_k, \dots, a_1)$  est l'inverse de  $(a_1, \dots, a_k)$ . □

**Proposition 4.6.** Soit  $(a_1, \dots, a_k) \in S_n$  un  $k$ -cycle. Alors on peut l'écrire comme une composition de  $k-1$  transpositions.

*Démonstration.* On écrit  $(a_1, \dots, a_k) = (a_1, a_2) \circ \dots \circ (a_{k-1}, a_k)$ . □



### 4.3. Permutations conjuguées

**Définition 4.7.** Soit  $\sigma_1, \sigma_2 \in S_n$  deux permutations. On dit que  $\sigma_1$  et  $\sigma_2$  sont conjuguées s'il existe  $\tau \in S_n$  telle que  $\sigma_1 = \tau \circ \sigma_2 \circ \tau^{-1}$ .

**Lemme 4.8.** Soit  $(a_1, \dots, a_k) \in S_n$  un  $k$ -cycle. Alors

$$\forall \sigma \in S_n, \sigma \circ (a_1, \dots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$$

*Démonstration.* Soit  $\sigma \in S_n$ . Soit  $i \in \{1, \dots, n\}$ , alors

- s'il existe  $j \in \{1, \dots, k-1\}$  tel que  $i = \sigma(a_j)$ , alors  $\sigma^{-1}(i) = a_j$  et on a

$$\sigma((a_1, \dots, a_k)(\sigma^{-1}(i))) = \sigma((a_1, \dots, a_k)(a_j)) = \sigma(a_{j+1}),$$

- si  $i = \sigma(a_k)$ , alors  $\sigma^{-1}(i) = a_k$  et on a

$$\sigma((a_1, \dots, a_k)(\sigma^{-1}(i))) = \sigma((a_1, \dots, a_k)(a_k)) = \sigma(a_1),$$

- sinon on a

$$\sigma((a_1, \dots, a_k)(\sigma^{-1}(i))) = \sigma(\sigma^{-1}(i)) = i.$$

Donc  $\sigma \circ (a_1, \dots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$ . □

**Corollaire 4.9.** Soit  $(a_1, \dots, a_k) \in S_n$  un  $k$ -cycle. Alors il est conjugué à  $(1, \dots, k)$ .

*Démonstration.* On prend  $\sigma \in S_n$  telle que  $\forall i \in \{1, \dots, k\}, \sigma(a_i) = i$ . □

**Théorème 4.10.** Soit  $\sigma \in S_n$  une permutation. On peut écrire  $\sigma$  comme une composition de cycles à supports disjoints  $\tau_1, \dots, \tau_m \in S_n$ . De plus cette écriture est unique à l'ordre des cycles près, et leurs longueurs  $k_1, \dots, k_m$  vérifient  $\sum_{l=1}^m k_l = n$ .

*Démonstration.* On raisonne par récurrence sur le cardinal de  $\text{supp}(\sigma)$ .

- Pour  $|\text{supp}(\sigma)| = 0$ , on a  $\sigma = \text{id}$ .
- Pour  $|\text{supp}(\sigma)| > 0$ , supposons que la propriété soit vérifiée pour toute permutation dont le cardinal du support est inférieur.

Soit  $i \in \text{supp}(\sigma)$ , puisque  $\sigma \in S_n$ , il existe  $p \in \{1, \dots, n\}$  minimal tel que  $\sigma^p(i) = i$ , alors on pose  $\tau_1 = (i, \sigma(i), \dots, \sigma^{p-1}(i))$ . Alors  $\tau_1$  agit comme  $\sigma$  sur l'ensemble  $\{i, \sigma(i), \dots, \sigma^{p-1}(i)\}$ , donc on a  $|\text{supp}(\tau_1^{-1} \circ \sigma)| < |\text{supp}(\sigma)|$ . Par hypothèse de récurrence, on peut écrire  $\tau_1^{-1} \circ \sigma$  comme une composition de cycles à supports disjoints  $\tau_2, \dots, \tau_m \in S_n$ , et  $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_m$ .

Soit  $i \in \{1, \dots, n\}$ , puisque les supports sont disjoints,  $i$  se trouve dans le support d'un seul des cycles, d'où l'unicité de l'écriture et  $\sum_{l=1}^m k_l = n$ . □

**Définition 4.11.** Soit  $\sigma \in S_n$  et  $\tau_1, \dots, \tau_m \in S_n$  la décomposition de  $\sigma$  en cycles à supports disjoints, ordonnés par longueur  $k_1 \leq \dots \leq k_m$ . On appelle  $(k_1, \dots, k_m)$  le *type* de  $\sigma$ .

**Théorème 4.12.** Soit  $\sigma_1, \sigma_2 \in S_n$  deux permutations. Alors  $\sigma_1$  et  $\sigma_2$  sont conjuguées si et seulement si elles ont le même type.

*Démonstration.*

$\Rightarrow$  : Supposons que  $\sigma_1$  et  $\sigma_2$  sont conjuguées. D'après le [Lemme 4.8](#),  $\sigma_1$  et  $\sigma_2$  ont le même type.

$\Leftarrow$  : Supposons que  $\sigma_1$  et  $\sigma_2$  ont le même type  $(k_1, \dots, k_m)$ .

D'après le [Corollaire 4.9](#),  $\sigma_1$  et  $\sigma_2$  sont conjuguées à

$$\sigma_3 := (1, \dots, k_1) \circ (k_1 + 1, \dots, k_1 + k_2) \circ \dots \circ (k_1 + \dots + k_{m-1} + 1, \dots, k_m)$$

donc il existe  $\tau_1, \tau_2 \in S_n$  telles que  $\sigma_1 = \tau_1 \circ \sigma_3 \circ \tau_1^{-1}$  et  $\sigma_2 = \tau_2 \circ \sigma_3 \circ \tau_2^{-1}$ .

Alors  $\sigma_1 = (\tau_1 \circ \tau_2^{-1}) \circ \sigma_2 \circ (\tau_2 \circ \tau_1^{-1})$ , donc  $\sigma_1$  et  $\sigma_2$  sont conjuguées. □

**Corollaire 4.13.** Soit  $\sigma \in S_n$  une permutation. On peut écrire  $\sigma$  comme une composition de transpositions.

*Démonstration.* On peut écrire  $\sigma$  comme une composition de cycles à supports disjoints, et chaque cycle comme une composition de transpositions.  $\square$

#### 4.4. Signature d'une permutation

**Définition 4.14.** Soit  $\sigma \in S_n$  une permutation. On appelle *signature* de  $\sigma$  le nombre rationnel

$$\text{sign}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

**Exemple 4.15.** On calcule la signature de la transposition  $(1, 2)$

$$\begin{aligned} \text{sign}((1, 2)) &= \frac{\sigma(2) - \sigma(1)}{2 - 1} \cdot \prod_{2 < j \leq n} \frac{\sigma(j) - \sigma(1)}{j - 1} \cdot \prod_{2 < j \leq n} \frac{\sigma(j) - \sigma(2)}{j - 2} \cdot \prod_{3 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \\ &= \frac{2 - 1}{1 - 2} \cdot \prod_{2 < j \leq n} \frac{j - 2}{j - 1} \cdot \prod_{2 < j \leq n} \frac{j - 1}{j - 2} \cdot 1 \\ &= -1 \end{aligned}$$

**Théorème 4.16.** L'application  $\text{sign} : (S_n, \circ) \rightarrow (\{-1, 1\}, \cdot)$  est un morphisme de groupes.

*Démonstration.* Soit  $\sigma \in S_n$ . Alors on calcule

$$|\text{sign}(\sigma)| = \prod_{1 \leq i < j \leq n} \frac{|\sigma(j) - \sigma(i)|}{|j - i|}$$

puisque  $\sigma$  est une bijection, on a  $\{\{\sigma(i), \sigma(j)\} \mid 1 \leq i < j \leq n\} = \{\{i, j\} \mid 1 \leq i < j \leq n\}$ , alors

$$|\text{sign}(\sigma)| = \prod_{1 \leq i < j \leq n} \frac{|j - i|}{|j - i|} = 1$$

donc  $\text{sign}(\sigma) \in \{-1, 1\}$ .

Soit  $\tau \in S_n$ . Alors

$$\begin{aligned} \text{sign}(\sigma \circ \tau) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} \end{aligned}$$

puisque  $\tau$  est une bijection, de la même manière on a

$$\begin{aligned} \text{sign}(\sigma \circ \tau) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \cdot \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \text{sign}(\sigma) \cdot \text{sign}(\tau) \end{aligned}$$

donc  $\text{sign}$  est un morphisme de groupes.  $\square$

**Corollaire 4.17.**

- Soit  $(a, b) \in S_n$  une transposition. Alors  $\text{sign}((a, b)) = -1$ .
- Soit  $(a_1, \dots, a_k) \in S_n$  un  $k$ -cycle. Alors  $\text{sign}((a_1, \dots, a_k)) = (-1)^{k-1}$ .
- Soit  $\sigma \in S_n$  une permutation de type  $(k_1, \dots, k_m)$ . Alors  $\text{sign}(\sigma) = \prod_{l=1}^m (-1)^{k_l-1}$ .

*Démonstration.* Puisque  $\text{sign}$  est un morphisme de groupes.

- Comme  $(a, b)$  est conjuguée à  $(1, 2)$ ,  $\text{sign}((a, b)) = \text{sign}((1, 2)) = -1$ .
- Comme  $(a_1, \dots, a_k) = (a_1, a_2) \circ \dots \circ (a_{k-1}, a_k)$ , on a

$$\text{sign}((a_1, \dots, a_k)) = \text{sign}((a_1, a_2)) \dots \text{sign}((a_{k-1}, a_k)) = (-1)^{k-1}.$$

- De la même manière,  $\sigma$  se décompose en cycles à supports disjoints,  $\text{sign}(\sigma) = \prod_{i=1}^m (-1)^{k_i-1}$ .

□

## 4.5. Groupes alternés

**Définition 4.18.** Soit  $\sigma \in S_n$  une permutation. On dit que  $\sigma$  est *paire* si  $\text{sign}(\sigma) = 1$ , ou *impaire* si  $\text{sign}(\sigma) = -1$ . On appelle *groupe alterné* l'ensemble

$$A_n := \{\sigma \in S_n \mid \sigma \text{ est paire}\} = \ker(\text{sign}).$$

**Proposition 4.19.** Soit  $\sigma \in S_n$  une permutation. Alors  $\sigma$  est paire si et seulement si elle peut s'écrire comme une composition de 3-cycles.

*Démonstration.*

$\Rightarrow$  : Supposons que  $\sigma$  est paire. Alors  $\sigma$  est la composition d'un nombre pair de transpositions.

On considère la permutation  $(a, b) \circ (c, d) \in S_n$ ,

- si  $\{a, b\} = \{c, d\}$ , alors  $(a, b) \circ (c, d) = \text{id}$ ,
- si  $\{a, b\} \cap \{c, d\} = \{b\} = \{c\}$ , alors  $(a, b) \circ (c, d) = (a, b, d)$ ,
- si  $\{a, b\} \cap \{c, d\} = \emptyset$ , alors  $(a, b) \circ (c, d) = (a, b, c) \circ (b, c, d)$ ,

donc  $(a, b) \circ (b, c)$  est un produit de 3-cycles.

$\Leftarrow$  : Supposons que  $\sigma$  est une composition de 3-cycles. Alors  $\text{sign}(\sigma) = 1$ , donc  $\sigma$  est paire. □

## 5. Groupes quotients

### 5.1. Relations d'équivalence

**Définition 5.1.** Soit  $E$  un ensemble. On appelle *relation* sur  $E$  un sous-ensemble  $R$  de  $E \times E$ . Si  $(x, y) \in R$ , on écrit  $xRy$ .

**Définition 5.2.** Soit  $R$  une relation sur un ensemble  $E$ . On dit que  $R$  est une *relation d'équivalence* si elle vérifie les propriétés suivantes

1.  $R$  est réflexive,  $\forall x \in E, xRx$ ,
2.  $R$  est symétrique,  $\forall x, y \in E, xRy \Rightarrow yRx$ ,
3.  $R$  est transitive,  $\forall x, y, z \in E, xRy$  et  $yRz \Rightarrow xRz$ .

Dans ce cas, on notera  $\sim$  pour  $R$ .

**Exemple 5.3.** Soit  $n \in \mathbb{N} \setminus \{0\}$ , on pose  $R_n := \{(a, b) \in \mathbb{Z}^2 \mid n|a - b\}$ .

1. Soit  $x \in \mathbb{Z}$ , alors  $n|0 = x - x$ , donc  $xR_n x$ ,
2. soit  $x, y \in \mathbb{Z}$ , si  $xR_n y$ , alors  $n|x - y$ , d'où  $n|y - x$ , donc  $yR_n x$ ,
3. soit  $x, y, z \in \mathbb{Z}$ , si  $xR_n y$  et  $yR_n z$ , alors  $n|x - y$  et  $n|y - z$ , d'où  $n|(x - y) + (y - z) = x - z$ , donc  $xR_n z$ .

Donc  $R_n$  est une relation d'équivalence, si  $(a, b) \in \mathbb{Z}^2$  on notera  $a \equiv b \pmod n$  pour  $aR_n b$ .

**Définition 5.4.** Soit  $\sim$  une relation d'équivalence sur un ensemble  $E$ .

- Soit  $x \in E$ . On appelle *classe d'équivalence* de  $x$ , notée  $\bar{x}$ , l'ensemble  $\bar{x} := \{y \in E \mid x \sim y\}$ .
- Soit  $x \in E$ . On appelle *représentant* de  $x$  tout élément de  $\bar{x}$ .
- On appelle *espace quotient* de  $E$  modulo  $\sim$  l'ensemble  $E/\sim := \{\bar{x} \mid x \in E\}$ .
- On appelle *projection canonique* de  $E$  sur  $E/\sim$  l'application  $\pi : E \rightarrow E/\sim, x \rightarrow \bar{x}$ .

**Exemple 5.5.** Soit  $n \in \mathbb{N}$ , on considère de nouveau la relation d'équivalence  $R_n$ . Alors

$$\forall x \in \mathbb{Z}, \bar{x} = \{y \in \mathbb{Z} \mid x \equiv y \pmod n\} = \{x + nk \mid k \in \mathbb{Z}\}$$

on notera  $\mathbb{Z}/n\mathbb{Z}$  pour  $\mathbb{Z}/R_n$ .

**Définition 5.6.** Soit  $E$  un ensemble. On appelle *partition* de  $E$  une famille  $(E_i)_{i \in I}$  de sous-ensembles de  $E$  qui vérifie les propriétés suivantes

1. les sous-ensembles sont deux à deux disjoints,  $\forall i, j \in I, i \neq j \Rightarrow E_i \cap E_j = \emptyset$ ,
2. l'union des sous-ensembles forme  $E$ ,  $\bigsqcup_{i \in I} E_i := \bigcup_{i \in I} E_i = E$ .

**Proposition 5.7.** Soit  $E$  un ensemble et  $\sim$  une relation d'équivalence sur  $E$ .

1. Soit  $x, y \in E$ , alors les énoncés suivants sont équivalents
  - (a)  $\bar{x} = \bar{y}$ ,
  - (b)  $x \in \bar{y}$ ,
  - (c)  $x \sim y$ .
2. L'espace quotient de  $E$  modulo  $\sim$  forme une partition de  $E$ .
3. Soit  $(E_i)_{i \in I}$  une partition de  $E$ . Alors  $R := \{(x, y) \in E \mid \exists i \in I, x, y \in E_i\}$  est une relation d'équivalence.

*Démonstration.*

1. (a)  $\Rightarrow$  (b) : Supposons que  $\bar{x} = \bar{y}$ , alors  $x \in \bar{x}$ , donc  $x \in \bar{y}$ .  
(b)  $\Rightarrow$  (c) : Supposons que  $x \in \bar{y}$ , alors  $y \in \bar{y}$ , donc  $x \sim y$ .  
(c)  $\Rightarrow$  (a) : Supposons que  $x \sim y$ . Soit  $z \in \bar{x}$ , alors  $z \sim x$ , et par transitivité  $z \sim y$ , donc  $z \in \bar{y}$ . Réciproquement si  $z \in \bar{y}$ , alors  $z \in \bar{x}$ , donc  $\bar{x} = \bar{y}$ .

2. Soit  $x, y \in E$ . Si  $\bar{x} \cap \bar{y} \neq \emptyset$ , il existe  $z \in \bar{x} \cap \bar{y}$  tel que  $z \sim x$  et  $z \sim y$ , donc  $x \sim y$  et  $\bar{x} = \bar{y}$ .  
Soit  $x \in E$ , alors  $x \in \bar{x} \subset \bigsqcup_{x \in E} \bar{x}$ , donc  $E = \bigsqcup_{x \in E} \bar{x}$ .
  3. 1. Soit  $x \in E$ , alors il existe  $i \in I$  tel que  $x \in E_i$ , donc  $xRx$ .  
2. Soit  $x, y \in E$ , alors si  $xRy$ , il existe  $i \in I$  tel que  $x, y \in E_i$ , donc  $yRx$ .  
3. Soit  $x, y \in E$ , alors si  $xRy$  et  $yRz$ , il existe  $i, j \in I$  tels que  $x, y \in E_i$  et  $y, z \in E_j$ , mais puisque  $(E_i)_{i \in I}$  est une partition, on a  $i = j$ , donc  $xRz$ .
- Donc  $R$  est une relation d'équivalence.

□

**Définition 5.8.** Soit  $E$  un ensemble et  $\sim$  une relation d'équivalence sur  $E$ . On appelle *système de représentants* pour  $\sim$  un sous-ensemble  $F$  de  $E$  tel que

$$\forall \alpha \in E / \sim, \exists ! x \in F, x \in \alpha$$

c'est-à-dire  $\pi|_F : F \rightarrow E / \sim$  est bijective.

**Définition 5.9.** Soit  $E$  et  $F$  deux ensembles, et  $f : E \rightarrow F$  une fonction. On dit que  $f$  est *bien définie* si

$$\forall x, y \in E, x \sim y \Rightarrow f(x) = f(y)$$

**Proposition 5.10.** Soit  $E$  et  $F$  deux ensembles, et  $\sim$  une relation d'équivalence. Soit  $f : E \rightarrow F$  une application,  $\pi : E \rightarrow E / \sim$  la projection canonique. Alors il existe  $\bar{f} : E / \sim \rightarrow F$  bien définie telle que  $\bar{f} \circ \pi = f$  si et seulement si

$$\forall x, y \in E, x \sim y \Rightarrow f(x) = f(y).$$

*Démonstration.*

$\Rightarrow$  : Supposons que  $\bar{f}$  soit bien définie et que  $\bar{f} \circ \pi = f$ . Soit  $x, y \in E$  tels que  $x \sim y$ , alors  $\pi(x) = \pi(y)$ , d'où  $\bar{f}(\pi(x)) = \bar{f}(\pi(y))$ , donc  $f(x) = f(y)$ .

$\Leftarrow$  : Supposons que  $\forall x, y \in E, x \sim y \Rightarrow f(x) = f(y)$ .

Soit  $\alpha \in E / \sim$ , on pose  $x_\alpha \in E$  un représentant de  $\alpha$ , on définit  $\bar{f}(\alpha) = f(x_\alpha)$ . Soit  $\beta \in E / \sim$ , si  $\beta = \alpha$ , alors  $x_\beta \sim x_\alpha$ , d'où  $f(x_\beta) = f(x_\alpha)$ , donc  $\bar{f}(\beta) = \bar{f}(\alpha)$ , c'est-à-dire  $\bar{f}$  est bien définie. □

## 5.2. Classes modulo un sous-groupe

**Définition 5.11.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . On appelle *relation modulo  $H$  à gauche*, la relation  $\sim_H$  sur  $G$  définie par

$$\forall x, y \in G, x \sim_H y \Leftrightarrow y \in xH \Leftrightarrow x^{-1} \star y \in H$$

où  $xH = \{x \star y \mid y \in H\}$ .

**Remarque 5.12.** On peut définir la *relation modulo  $H$  à droite*  $\sim^H$  d'une manière similaire.

**Proposition 5.13.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors  $\sim_H$  est une relation d'équivalence sur  $G$ , dont les classes d'équivalences sont  $\forall x \in G, \bar{x} = xH$ .

*Démonstration.*

1. Soit  $x \in G$ , alors  $x \star e \in xH$ , donc  $x \sim_H x$ .
2. Soit  $x, y \in G$ , alors si  $x \sim_H y$ , on a  $x^{-1} \star y \in H$ , d'où  $y^{-1} \star x = (x^{-1} \star y)^{-1} \in H$ , donc  $y \sim_H x$ .
3. Soit  $x, y, z \in G$ , alors si  $x \sim_H y$  et  $y \sim_H z$ , on a  $y \in xH$  et  $z \in yH$ , d'où  $z \in xH$ , donc  $x \sim_H z$ .

□

**Notation 5.14.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors on note les espaces quotients  $G/H := G / \sim_H$  et  $H \setminus G := G / \sim_H$ .

**Proposition 5.15.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors les ensembles  $G/H$  et  $H \setminus G$  sont isomorphes. En particulier si  $G$  est fini, on a  $|G/H| = |H \setminus G|$ .

*Démonstration.* On considère le morphisme  $\varphi : G/H \rightarrow H \setminus G, xH \rightarrow Hx^{-1}$ , il est bien définie et admet pour inverse  $\psi : H \setminus G \rightarrow G/H, Hx \rightarrow x^{-1}H$ , donc c'est un isomorphisme.  $\square$

### 5.3. Théorème du nombre de classes et théorème de Lagrange

**Définition 5.16.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . On appelle *indice* de  $H$  dans  $G$

$$[G : H] := |G/H|.$$

**Théorème 5.17.** (Théorème du nombre de classes) Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors si  $G$  est fini

$$|G| = [G : H]|H|$$

*Démonstration.* On pose  $n := [G : H]$  et on considère  $\{x_1, \dots, x_n\}$  un système de représentants pour  $\sim_H$ . On sait que la famille  $(x_i H)_{i \in \{1, \dots, n\}}$  forme une partition de  $G$ , d'où

$$|G| = \sum_{i=1}^n |x_i H| = \sum_{i=1}^n |H| = n|H|$$

c'est-à-dire  $|G| = [G : H]|H|$ .  $\square$

**Corollaire 5.18.** (Théorème de Lagrange) Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors si  $G$  est fini,  $|H|$  divise  $|G|$ , en particulier si  $x \in G$ ,  $\text{ord}(x)$  divise  $|G|$ .

**Corollaire 5.19.**

1. Soit  $(G, \star)$  un groupe fini d'ordre  $n$  et  $x \in G$ . Alors  $x^n = e$ .
2. Soit  $(G, \star)$  un groupe fini,  $H$  un sous-groupe de  $G$  et  $K$  un sous-groupe de  $H$ . Alors  $K$  est un sous-groupe de  $G$  et

$$[G : K] = [G : H][H : K].$$

*Démonstration.*

1. D'après le [Corollaire 5.18](#),  $\text{ord}(x)$  divise  $n$ , donc  $x^n = e$ .
2. D'après le [Théorème 5.17](#),

$$[G : K] = \frac{|G|}{|K|} = \frac{[G : H]|H|}{|K|} = \frac{[G : H][H : K]|K|}{|K|} = [G : H][H : K].$$

$\square$

### 5.4. Sous-groupes distingués et groupes quotients

**Théorème 5.20.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors les énoncés suivants sont équivalents

1.  $H$  est distingué.
2. Il existe un morphisme  $\varphi : G \rightarrow G$  tel que  $H = \ker(\varphi)$ .
3.  $G/H$  a une structure de groupes.

*Démonstration.*

1.  $\Rightarrow$  3. : Supposons que  $H$  est distingué.

On considère l'application  $\cdot : G/H \times G/H \rightarrow G/H, (xH, yH) \rightarrow xyH$ , alors elle est bien définie et  $(G/H, \cdot)$  forme un groupe.

3.  $\Rightarrow$  2. : Supposons que  $G/H$  a une structure de groupe.

Alors la projection canonique  $\pi : G \rightarrow G/H$  est un morphisme de groupes et  $\ker(\pi) = H$ .

2.  $\Rightarrow$  1. : Supposons qu'il existe un tel morphisme  $\varphi$ .

Soit  $h \in H$  et  $g \in G$ , alors

$$\varphi(g \star h \star g^{-1}) = \varphi(g) \star \varphi(h) \star \varphi(g)^{-1} = \varphi(x) \star \varphi(x)^{-1} = e$$

puisque  $H = \ker(\varphi)$ , on a  $g \star h \star g^{-1} \in H$ . □

**Corollaire 5.21.** Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Si  $G$  est abélien, alors  $G/H$  a une structure de groupes.

**Théorème 5.22.** (Propriété d'universalité du groupe quotient) Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe distingué de  $G$ . Soit  $(K, \cdot)$  un groupe,  $\pi : G \rightarrow G/H$  la projection canonique et  $\varphi : G \rightarrow K$  un morphisme de groupes. Alors il existe un morphisme  $\bar{\varphi} : G/H \rightarrow K$  tel que  $\bar{\varphi} \circ \pi = \varphi$ , si et seulement si  $H \subset \ker(\varphi)$ . Dans ce cas  $\text{im}(\bar{\varphi}) = \text{im}(\varphi)$  et  $\ker(\bar{\varphi}) = \ker(\pi(\varphi))$ .

*Démonstration.*

$\Rightarrow$  : Supposons qu'il existe un tel morphisme  $\bar{\varphi}$ .

Soit  $x \in H$ , alors  $\varphi(x) = \bar{\varphi}(\pi(x)) = \bar{\varphi}(\{e\}) = H$ , donc  $H \subset \ker(\varphi)$ .

$\Leftarrow$  : Supposons que  $H \subset \ker(\varphi)$ .

Soit  $x \in H$ , on définit  $\bar{\varphi}(xH) = \varphi(x)$ , alors  $\bar{\varphi}$  est bien définie. Puisque  $\bar{\varphi} \circ \pi = \varphi$  et  $\pi$  est surjectif, on a  $\text{im}(\bar{\varphi}) = \text{im}(\varphi)$  on a  $\ker(\bar{\varphi}) = \pi(\ker(\varphi))$ . □

**Corollaire 5.23.** (Théorème d'isomorphisme) Soit  $(G, \star)$  et  $(K, \cdot)$  deux groupes, et  $\varphi : G \rightarrow K$  un morphisme de groupes. Alors il existe un isomorphisme  $\bar{\varphi} : G/\ker(\varphi) \rightarrow \text{im}(\varphi)$ .

*Démonstration.* On pose  $H := \ker(\varphi)$ , alors par le **Théorème 5.22**, il existe  $\bar{\varphi} : G/\ker(\varphi) \rightarrow \text{im}(\varphi)$  telle que  $\bar{\varphi} \circ \pi = \varphi$ . Puisque  $\ker(\bar{\varphi}) = \pi(\ker(\varphi)) = \pi(H) = \{e\}$ ,  $\bar{\varphi}$  est injectif, et par définition  $\bar{\varphi}$  est surjectif. Donc  $\bar{\varphi}$  est un isomorphisme. □

**Proposition 5.24.** Soit  $(G, \star)$  un groupe. Alors si  $(G, \star)$  est monogène, il existe  $n \in \mathbb{N}$  tel qu'il est isomorphe à  $(\mathbb{Z}, +)$  ou à  $(\mathbb{Z}/n\mathbb{Z}, +)$ .

*Démonstration.* Soit  $x \in G$  un générateur et  $\varphi : \mathbb{Z} \rightarrow G, m \rightarrow x^m$ .

Alors  $\varphi$  est un morphisme de groupes et  $\text{im}(\varphi) = \langle x \rangle = G$ , donc  $\varphi$  est surjectif. Soit  $d := \text{ord}(x)$

- si  $d = +\infty$ , alors  $\varphi$  est injectif, et par le **Corollaire 5.23**,  $\mathbb{Z}/\ker(\varphi) \simeq \text{im}(\varphi)$ , c'est-à-dire  $\mathbb{Z} \simeq G$ ,
- sinon  $\ker(\varphi) = d\mathbb{Z}$ , et par le **Corollaire 5.23**,  $\mathbb{Z}/\ker(\varphi) \simeq \text{im}(\varphi)$ , c'est-à-dire  $\mathbb{Z}/d\mathbb{Z} \simeq G$ .

□

**Proposition 5.25.** Soit  $(G, \star)$  un groupe et  $x, y \in G$  tels que  $x \star y = y \star x$ . Notons  $a := \text{ord}(x)$  et  $b := \text{ord}(y)$ , alors  $\text{ord}(x \star y)$  divise  $\text{ppcm}(a, b)$ . De plus si  $\langle x \rangle \cap \langle y \rangle = \{e\}$ , on a  $\text{ord}(x \star y) = \text{ppcm}(a, b)$

*Démonstration.* Posons  $m := \text{ppcm}(a, b)$  et  $d := \text{pgcd}(a, b)$ .

Alors il existe  $a', b' \in \mathbb{Z}$  tels que  $a = da'$  et  $b = db'$ , d'où  $m = da'b'$ . Alors

$$(x \star y)^m = x^m \star y^m = (x^{da'})^{b'} \star (y^{db'})^{a'} = e$$

donc  $\text{ord}(x \star y)$  divise  $\text{ppcm}(a, b)$ . □

**Proposition 5.26.** Soit  $n, m \in \mathbb{Z}$ . Alors  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  est isomorphe à  $\mathbb{Z}/nm\mathbb{Z}$  si et seulement si  $\text{pgcd}(n, m) = 1$ .

*Démonstration.* Soit  $x \in \mathbb{Z}$ . Notons  $\bar{x}$  et  $[x]$  les classes respectives de  $x$  modulo  $n$  et  $m$ .

$\Rightarrow$  : Supposons que  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  est isomorphe à  $\mathbb{Z}/nm\mathbb{Z}$ . Alors  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  est cyclique. Soit  $(a, b)$  un générateur de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ , c'est-à-dire  $\text{ord}((a, b)) = nm$ , alors

$$\text{ppcm}(\text{ord}(a), \text{ord}(b)) \cdot (a, b) = (\bar{0}, [0])$$

donc  $nm | \text{ppcm}(\text{ord}(a), \text{ord}(b))$ , on en déduit  $nm | \text{ppcm}(n, m)$ , d'où  $\text{pgcd}(n, m) = 1$ .

$\Leftarrow$  : Supposons que  $\text{pgcd}(n, m) = 1$ . Posons  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, x \rightarrow (\bar{x}, [x])$ .

Alors  $\varphi$  est bien un morphisme, et on a

$$\begin{aligned} \ker(\varphi) &= \{k \in \mathbb{Z} \mid (\bar{k}, [k]) = (\bar{0}, [0])\} \\ &= \{k \in \mathbb{Z} \mid n|k \text{ et } m|k\} \\ &= \{k \in \mathbb{Z} \mid nm|k\} = nm\mathbb{Z} \end{aligned}$$

d'après le [Théorème 5.22](#), il existe un morphisme  $\bar{\varphi} : \mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  injectif. Enfin puisque  $|\mathbb{Z}/nm\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|$ , on en déduit que  $\bar{\varphi}$  est un isomorphisme.  $\square$



## 6. Actions de groupes

### 6.1. Définitions

**Définition 6.1.** Soit  $(G, \star)$  un groupe et  $X$  un ensemble. On appelle *action* de  $G$  sur  $X$  une application  $\psi : G \times X \longrightarrow X$  qui vérifie les propriétés suivantes

1.  $\forall x \in X, \psi(e, x) = x,$
2.  $\forall g, h \in G, \forall x \in X, \psi(g, \psi(h, x)) = \psi(gh, x).$

Dans ce cas, on notera  $\forall g \in G, \forall x \in X, g \star x := \psi(g, x).$

**Notation 6.2.** Soit  $(G, \star)$  un groupe et  $X$  un ensemble. Si  $G$  agit sur  $X$ , on note  $G \curvearrowright X$