

GROUPES ET GROUPES SYMÉTRIQUES

eric.vasserot@imj-prg.fr

Table des matières

1. Introduction.....	1
1.1. Groupe abstrait.....	1
1.2. Groupe commutatif.....	2
1.3. Exemples.....	2
2. Sous-groupe.....	3
2.1. Sous-groupe.....	3
2.2. Ordre d'un groupe et d'un élément.....	4
3. Morphisme de groupes.....	5
3.1. Morphisme de groupes.....	5
3.2. Image et noyau.....	5
4. Groupe symétrique.....	6
4.1. Groupe de permutations.....	6
4.2. Transpositions et cycles.....	6
4.3. Décomposition des cycles.....	7

1. INTRODUCTION

1.1. Groupe abstrait

DÉFINITION 1.1. —

Un groupe est la donnée d'un couple (G, \cdot) où G est un ensemble et $\cdot : G \times G \rightarrow G$ une loi de composition interne, telle que :

1. associativité :

$$\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c);$$

2. existence de l'élément neutre $e \in G$:

$$\forall g \in G, g \cdot e = e \cdot g = g;$$

3. existence de l'inverse :

$$\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e.$$

NOTATIONS. — Pour un groupe multiplicatif on note ab l'élément $a \cdot b$, l'élément neutre est noté 1 et l'inverse de a est noté de a^{-1} .

DÉMONSTRATION 1.1 (Unicité de l'élément neutre et de l'inverse)

Soient e, e' deux éléments neutres. Alors

$$e' = e \cdot e' = e.$$

Soient b, c inverses de a . Alors :

$$b = b \cdot a \cdot c = c.$$

1.2. Groupe commutatif

DÉFINITION 1.2 (Groupe commutatif (ou Abélien)). —

Un groupe G est commutatif si la loi de composition l'est :

$$\forall x, y \in G, xy = yx.$$

NOTATIONS. — En général la loi de composition d'un tel groupe est notée comme un groupe additif $(G, +)$. Le neutre est alors 0 et l'inverse de x est $-x$.

1.3. Exemples

- Le couple $(\mathbf{Z}, +)$ est un groupe abélien où $+$ est l'addition usuelle des entiers.
- $(\mathbf{R}, +)$ et $(\mathbf{Q}, +)$ sont également des groupes abéliens.
- $(\mathbf{R} \setminus \{0\}, \times)$ et $(\mathbf{Q} \setminus \{0\}, \times)$ sont des groupes abéliens.
- $\text{GL}(n, \mathbf{R})$ est un groupe pour la composition de matrices en tant que loi de composition. Ce n'est pas un groupe commutatif.

2. SOUS-GROUPE

2.1. Sous-groupe

DÉFINITION 2.1 (Sous-groupe). —

Soit G un groupe (multiplicatif) et $H \subset G$ un sous-ensemble de G . H est un sous-groupe de G si c'est un groupe avec la loi de composition et d'inverse astreintes à H ^(1§).

PROPOSITION 2.1. —

Soit G un groupe.

Si $(H_i)_{i \in I}$ est une famille de sous-groupes de G alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

DÉFINITION 2.2. —

Pour tout $i \in I$, H_i vérifie la propriété de sous-groupe et donc l'intersection aussi.

REMARQUE. — Généralement la réunion de sous-groupes n'est pas un sous-groupe. En effet si $x \in H_1$ et $y \in H_2$ alors il n'y a aucune raison que $xy \in \bigcup H_i$.

Pour une équivalence il faut rajouter une hypothèse. Si H, K sont deux sous-groupes de G alors $H \cup K$ est un sous-groupe si, et seulement si, $H \subset K$ ou $K \subset H$.

En effet supposons $H \not\subset K$ et que $H \cup K$ est un sous-groupe. Si $K \not\subset H$ alors on peut choisir $x \in K - K \cap H$ et $y \in H - K \cap H$. On a $x, y \in K \cup H$ et donc par hypothèse $xy \in H \cup K$ et donc il existe des inverses respectifs x^{-1}, y^{-1} . Supposons $xy \in H$: $H \ni (xy)y^{-1} = xe = x \in H$ absurde.

DÉFINITION 2.3 (Groupe engendré). —

Si G est un groupe et X une partie de G alors on appelle sous-groupe de G engendré par X le plus petit sous-groupe de G contenant X . On le notera ici $\langle X \rangle$.

On a de plus si on note \mathbb{G} l'ensemble des sous-groupes de G :

$$\langle X \rangle = \bigcap_{H \in \mathbb{G} \text{ et } H \supset X} H.$$

EXEMPLE. — Soit G un groupe et $x \in G$. Alors :

$$\langle x \rangle = \{x^k \mid k \in \mathbf{Z}\}.$$

En effet c'est un sous-groupe de $\langle x \rangle$ et le plus petit.

^{1§}. C'est-à-dire si H est stable par l'application $(x, y) \mapsto xy^{-1}$.

2.2. Ordre d'un groupe et d'un élément

DÉFINITION 2.4 (Ordre d'un groupe). —

Si G est un groupe fini, on appelle *ordre de G* son cardinal, on le note généralement $|G|$ ou $\sharp G$.

Si G est un groupe et $x \in G$ alors on appelle *ordre de x* le cardinal de son sous-groupe engendré (s'il est fini).

Dans le cas où le groupe en question ne serait pas fini, on dit que l'ordre est infini.

EXEMPLES. —

— Dans \mathbf{Z} , tous les éléments non nuls sont d'ordre infini.

— Dans $\mathbf{Z}/n\mathbf{Z}$ pour $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ est d'ordre n puisque toute classe admet un représentant dans $\{0, \dots, n-1\}$.

— Ordre des éléments de $\mathbf{Z}/4\mathbf{Z}$:

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$ x $	1	4	2	4

THÉORÈME 2.1 (Théorème de LAGRANGE). —

Pour tout groupe G et tout sous-groupe H de G , l'ordre (i.e. le cardinal) de H divise l'ordre de G :

$$\sharp H \mid \sharp G.$$

DÉMONSTRATION 2.1 (Théorème de LAGRANGE). —

Le cardinal de l'ensemble G/H est appelé *indice* de H dans G et est noté $[G : H]$. De plus, ses classes forment une partition de G et chacune d'entre elles a le même cardinal que H .

On a alors :

$$\sharp G = \sharp H \times [G : H].$$

3. MORPHISME DE GROUPES

3.1. Morphisme de groupes

DÉFINITION 3.1. —

Soient G, H deux groupes. Une application $f : G \rightarrow H$ est un morphisme de groupes si :

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

PROPOSITION 3.1. —

Soient $f : G \rightarrow H$ un morphisme de groupes. Alors :

1. $f(e_G) = e_H$;
2. $\forall x \in G, f(x^{-1}) = f(x)^{-1}$

3.2. Image et noyau

DÉFINITION 3.2. —

Soit $f : G \rightarrow H$ un morphisme de groupes. On définit :

1. $\text{Ker}(f) = \{x \in G \mid f(x) = e\}$;
2. $\text{Im}(f) = \{f(x) \mid x \in G\}$.

PROPOSITION 3.2. —

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

1. $\text{Ker}(f)$ et $\text{Im}(f)$ sont des sous-groupes de G et H respectivement ;
2. f est injective si, et seulement si, $\text{Ker}(f) = \{e\}$;
3. f est surjective si, et seulement si, $\text{Im}(f) = H$.

DÉMONSTRATION 3.1. —

Point par point :

1. On a bien entendu $f(e) = e$ et $f(x)^{-1} = f(x^{-1})$ pour tout $x \in G$. Ainsi $\text{Im}(f) = f(G)$ est un sous-groupe de H .

Soient $x, y \in G$, alors $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = f(x)f(y)^{-1} = e$ donc $xy^{-1} \in \text{Ker}(f)$. De plus $f(e) = e$ donc $\text{Ker}(f)$ est un sous-groupe de G .

2. Soient $x, y \in G$:

$$(f(x) = f(y) \iff x = y) \iff (f(xy^{-1}) = e \iff xy^{-1} = e).$$

3. Par définition, si $\text{Im}(f) = H$ alors f est surjective et réciproquement.

4. GROUPE SYMÉTRIQUE

4.1. Groupe de permutations

DÉFINITION 4.1. —

Soit E un ensemble. On définit :

$$S_E = \{\text{bijections } E \rightarrow E\}.$$

La loi étant la composition des applications. Elle est associative, admet un élément neutre (application identité) et toute application admet une application inverse par définition.

PROPOSITION 4.1. —

Si $\sharp E = n$ alors S_E est isomorphe (au sens de groupes) à $S_{\{1,2,\dots,n\}} := S_n$.

DÉMONSTRATION 4.1. —

Puisque $\sharp E = n$ il existe une bijection $\phi : E \rightarrow \{1, 2, \dots, n\}$. On considère alors l'application de $\theta : S_E \rightarrow S_n$ définie par : $\omega \mapsto \phi \circ \omega \circ \phi^{-1}$. Comme ω, ϕ sont des bijections, l'application $\phi \circ \omega \circ \phi^{-1}$ est une bijection. L'application θ est bien définie.

On a :

$$\theta(\omega' \circ \omega) = \phi \circ (\omega' \circ \omega) \circ \phi^{-1}$$

$$\theta(\omega' \circ \omega) = \phi \circ \omega' \circ \text{id} \circ \omega \circ \phi^{-1}$$

$$\theta(\omega' \circ \omega) = \theta(\omega') \circ \theta(\omega).$$

θ est bien un morphisme de groupes. On a $\theta^{-1}(\omega) = \phi^{-1} \circ \omega \circ \phi$ qui fait de θ une bijection.

DÉFINITION 4.2 (Groupe symétrique). —

On appelle S_n le *groupe symétrique*.

REMARQUE. — On omet la notation \circ . Si $\omega \in S_n$ on décrit son action sur $\{1, 2, \dots, n\}$ par :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \omega(1) & \omega(2) & \dots & \omega(n) \end{pmatrix}.$$

EXEMPLE DE COMPOSITION. — Dans S_4 :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

4.2. Transpositions et cycles

DÉFINITION 4.3 (Transposition). —

Une *transposition* de S_n est une permutation qui échange deux éléments et laisse invariants les $n - 2$ autres.

NOTATION. — Pour tous $i, j \in \{1, 2, \dots, n\}$ avec $i \neq j$ on note (ij) la transposition :

$$(ij) : \begin{cases} i \mapsto j \\ j \mapsto i \\ k \mapsto k, \forall k \neq i, j \end{cases}.$$

REMARQUE. — Une transposition est une involution. C'est à dire que l'ordre d'une transposition est 2.

PROPOSITION 4.2. —

$\#S_n = n!$.

DÉFINITION 4.4 (Cycle). —

On appelle *cycle* de longueur $r > 1$ (noté r -cycle) (dans S_n) une permutation ω telle qu'il existe $x_1, x_2, \dots, x_r \in \{1, 2, \dots, n\}$ vérifiant :

1. $\omega(x_1) = x_2, \omega^n(x_1) = x_{1+n}$ avec $n < r$;
2. $\omega(x_r) = x_1$;
3. $\omega(x) = x$ si $x \notin \{x_1, x_2, \dots, x_r\}$.

NOTATION. — On note un tel cycle : $(x_1 \ x_2 \ \dots \ x_r)$.

REMARQUE. — Les 2-cycles sont exactement les transpositions.

EXEMPLE. — Dans S_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3) = \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}.$$

4.3. Décomposition des cycles

DÉFINITION 4.5 (Support). —

On appelle *support* du cycle ω le sous-ensemble :

$$\{x_1, x_2, \dots, x_r\} \subset \{1, 2, \dots, n\}.$$

LEMME 4.1. —

Deux cycles de supports disjoints commutent.

DÉMONSTRATION 4.2. —

Soient :

$$\begin{cases} v = (x_1, x_2, \dots, x_r) \\ w = (y_1, y_2, \dots, y_s) \end{cases}$$

avec $\{x_1, x_2, \dots, x_r\} \cap \{y_1, y_2, \dots, y_s\} = \emptyset$.

Sur un élément extérieur du support la permutation agit comme l'identité donc deux supports disjoints impliquent que les permutations associées permutent (puisque que l'identité permute).

LEMME 4.2. —

Un r -cycle est d'ordre r .

DÉMONSTRATION 4.3. —

Soit $w = \begin{pmatrix} x_1 & x_2 & \dots & x_r \end{pmatrix}$ un r -cycle. Il est clair qu'un élément du support est d'ordre r . Les autres restent fixés par w et donc w est d'ordre r .

PROPOSITION 4.3. —

Toute permutation de S_n est décomposable en produit de cycles de supports disjoints. Cette décomposition est unique à l'ordre des facteurs près.

EXEMPLES. — Soit :

$$S_5 \ni \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = w.$$

On peut décomposer w :

$$\begin{aligned} (1 \ 3 \ 5)(2)(4) &= (1 \ 3 \ 5). \\ S_8 \ni w &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 1 & 7 & 3 & 8 & 4 & 2 \end{pmatrix} = (1 \ 5 \ 3)(2 \ 6 \ 8)(4 \ 7). \end{aligned}$$

THÉORÈME 4.1. —

Le groupe symétrique est engendré par les transpositions.

DÉMONSTRATION 4.4. —

On procède par récurrence sur n .

1. $S_2 = \{1, (1 \ 2)\}$ est engendré par $(1 \ 2)$.
2. Soit $n > 2$, supposons que S_{n-1} est engendré par les transpositions de S_{n-1} . Soit $w \in S_n$:
 - (a) Soit $w(n) = n$ et alors on décompose w en cycles de tailles inférieures ou égales à S_{n-1} et c'est démontré.

- (b) Soit $w(n) \neq n$. On pose $m = w(n)$ et soit $t = \begin{pmatrix} n & m \end{pmatrix}$. On pose $v = tw$ et alors $v(n) = n$ et on lui applique le cas précédent. On a alors par unicité de la décomposition que w est elle-même engendrée par des transpositions et c'est démontré.

THÉORÈME 4.2. —

On a les propositions suivantes :

1. Si $w \in S_n$ est une permutation qui s'écrit de deux façons différentes comme produit de transpositions :

$$w = \tau_1 \tau_2 \dots \tau_r = \tau'_1 \tau'_2 \dots \tau'_{r'},$$

alors $(-1)^r = (-1)^{r'}$.

On appelle $(-1)^r$ la *signature* de w .

2. La signature est un morphisme de groupes de $S_n \rightarrow \{1, -1\} \cong \mathbf{Z}/2\mathbf{Z}$.

DÉMONSTRATION 4.5. —

Soit $w \in S_n$. On pose :

$$\begin{aligned} \varepsilon(w) &= \prod_{1 \leq i < j \leq n} \frac{w(i) - w(j)}{i - j} \\ \varepsilon(w) &= \frac{\prod_{1 \leq i < j \leq n} (w(i) - w(j))}{\prod_{1 \leq i < j \leq n} (i - j)} \\ \varepsilon(w) &= \frac{N}{D}. \end{aligned}$$

Avec

$$N = \prod_{1 \leq i, j \leq n ; w^{-1}(i) < w^{-1}(j)} (i - j) = \pm D.$$

D'où :

$$\varepsilon(w) = \pm 1.$$

EXEMPLE. — $w = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$. On a :

$$\varepsilon(w) = \frac{(w(1) - w(2))(w(1) - w(3))(w(2) - w(3))}{(1 - 2)(1 - 3)(2 - 3)} = \frac{(2 - 3)(2 - 1)(3 - 1)}{(1 - 2)(1 - 3)(2 - 3)} = 1.$$

LEMME 4.3. —

On a :

1. $\varepsilon : S_n \rightarrow \{\pm 1\}$ est un morphisme de groupes ;
2. $\varepsilon(ij) = -1$ pour tout $i \neq j$.

DÉMONSTRATION 4.6 (Théorème). —

Si

$$w = \tau_1 \tau_2 \dots \tau_r = \tau'_1 \tau'_2 \dots \tau'_{r'}$$

alors par le lemme :

$$\varepsilon(w) = (-1)^r = (-1)^{r'}.$$

DÉMONSTRATION 4.7 (Lemme). —

Soit $E = \{(i, j) \mid 1 \leq i < j \leq n\}$. On pose :

$$f_w : \begin{cases} E \rightarrow E \\ \begin{pmatrix} i & j \end{pmatrix} \mapsto \begin{pmatrix} w(i) & w(j) \end{pmatrix} \text{ si } w(i) < w(j) . \\ \begin{pmatrix} i & j \end{pmatrix} \mapsto \begin{pmatrix} w(j) & w(i) \end{pmatrix} \text{ si } w(i) > w(j) \end{cases}$$

f est une bijection car elle est injective et l'ensemble de départ et d'arrivée ont le même cardinal qui est fini.

Donc on a :

$$\varepsilon(w) = \frac{\prod_{1 \leq i < j \leq n} (w(i) - w(j))}{\prod_{(i,j) \in E} (w(i) - w(j))}$$

$$\varepsilon(w) = \pm 1.$$

Pour vérifier que ε est un morphisme, on calcul $\varepsilon(wv)$:

$$\varepsilon(wv) = \prod_{(i,j) \in E} \frac{wv(i) - wv(j)}{i - j}$$

$$\varepsilon(wv) = \prod_{(i,j) \in E} \frac{wv(i) - wv(j)}{v(i) - v(j)} \prod_{(i,j) \in E} \frac{v(i) - v(j)}{i - j}$$

$$\varepsilon(wv) = \prod_{(i,j) \in E} \frac{wv(i) - wv(j)}{v(i) - v(j)} \varepsilon(v).$$

On calcule :

$$\varepsilon(w) \stackrel{?}{=} \prod_{(i,j) \in E} \frac{wv(i) - wv(j)}{v(i) - v(j)}$$

$$\varepsilon(w) = \prod_{(i,j) \in E_1} \frac{wv(i) - wv(j)}{v(i) - v(j)} \prod_{(i,j) \in E_2} \frac{wv(i) - wv(j)}{v(i) - v(j)}$$

Où $E_1 = \{(i, j) \in E \mid v(i) < v(j)\}$ et $E_2 = \{(i, j) \in E \mid v(j) < v(i)\}$; $E = E_1 \amalg E_2$.

$$\varepsilon(w) = \prod_{(i,j) \in E_2} \frac{wv(j) - wv(i)}{v(j) - v(i)} \prod_{(i,j) \in E_1} \frac{wv(i) - wv(j)}{v(i) - v(j)}$$

$$\varepsilon(w) = \prod_{i < j ; v^{-1}(j) < v^{-1}(i)} \frac{w(i) - w(j)}{i - j} \prod_{i < j ; v^{-1}(i) < v^{-1}(j)} \frac{w(i) - w(j)}{i - j}$$

$$\varepsilon(w) = \prod_{i < j} \frac{w(i) - w(j)}{i - j}$$