

Groupes et géométrie

Préparation à l'agrégation interne

Académie de Guyane
2017-2018

Table des matières

1	Structure de groupe	3
1.1	Notion de groupe	3
1.2	Exemples	4
1.3	Sous-groupe	4
1.4	Morphisme de groupe	7
1.5	Produit direct de groupes	10
2	Classe modulo un sous-groupe	12
2.1	Théorème de Lagrange. Indice d'un sous groupe	12
2.2	1 ^{er} théorème d'isomorphisme	14
3	Groupes monogènes, symétriques et diédraux.	17
3.1	Groupes monogènes	17
3.2	Groupes symétriques S_n	21
3.3	Groupes diédraux	27
4	Sous-groupes normaux	29
4.1	Notion de sous-groupes normal, groupe quotient	29
4.2	Quelques propriétés	31
4.3	2 ^e et 3 ^e théorème d'isomorphisme	32
5	Action de groupe	33
5.1	Notion de groupe opérant sur un ensemble	33
5.2	Orbite. Stabilisateur	34
5.3	Exemples	35
5.4	Formule des classes	36
5.5	Points fixes d'un G-ensemble	36
6	Groupes finis	37
6.1	Théorèmes de Sylow	37
6.2	Quelques applications	37
7	Groupes linéaires et sous-groupes	38

8 Isométries et déplacements d'un espace affine euclidien 39

Chapitre 1

Structure de groupe

Introduite explicitement au début du XIX^e siècle, la notion de groupe apparaît dans les travaux d'Evariste Galois sur la résolution des équations polynômiales. Peu après, des groupes sont mis en évidence en géométrie, avec les groupes de symétrie de polygones et polyèdres réguliers notamment.

De nos jours, la notion de groupe se retrouve associé à des concepts divers comme par exemple en géométrie différentielle (groupes de Lie) ou en topologie algébrique (groupes d'homologie).

Nous accorderons dans ce document une place particulière à l'analyse de la structure des groupes finis.

1.1 Notion de groupe

Définition 1. G est un ensemble muni d'une loi de composition interne définie par $(x; y) \longrightarrow x.y$

On dit que la loi $.$ définit une structure de groupe, ou que G est un groupe relativement à cette loi si les 3 axiomes suivants sont vérifiés :

1. La loi $.$ est associative.
2. Il existe dans $(G, .)$ un élément neutre noté e .
3. Tout élément de $(G, .)$ est symétrisable.

Remarque 1.

- a) L'élément neutre e est unique.
- b) Tout élément possède un symétrique unique.

Définition 2.

G est dit abélien ou commutatif si pour tout $x, y \in G$, $x.y = y.x$

G est dit fini s'il n'a qu'un nombre fini d'élément.

Dans ce cas, le cardinal de G s'appelle l'ordre du groupe, noté $o(G)$

Remarque 2.

- a) pour tout $n, m \in \mathbb{N}$ et $x \in G$, $x^n x^m = x^m x^n = x^{n+m}$ (notation multiplicative).

- b) Attention, en général $(xy)^n \neq x^n y^n$, et on a : $(xy)^{-1} = y^{-1} x^{-1}$
 c) Dans G tout élément est simplifiable à gauche et à droite :

$$xa = ya \Rightarrow x = y$$

En particulier, cela montre que le symétrique est unique.

1.2 Exemples

1. $(\mathbb{Z}, +)$ est un groupe abélien.
2. $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient des classes d'entiers modulo n est un groupe fini abélien.
3. Si $E = \{1; 2; \dots; n\}$, l'ensemble S_n des permutations de E , muni de la composition des applications, est un groupe fini, d'ordre $n!$, appelé groupe symétrique.

Pour $n \geq 3$, S_n est non abélien.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_1 \circ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2$$

$$\tau_3 \circ \sigma_1 = \tau_1$$

4.

$$Q_8 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \right. \\ \left. \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}; \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}; \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\} \subset GL_2(\mathbb{C})$$

est un groupe pour la multiplication des matrices, d'ordre 8.

Le groupe des quaternions est non abélien.

5. Si E est un espace vectoriel sur un corps $\mathbb{K}$,
 $GL(E) = \{\text{automorphismes } \mathbb{K}\text{-linéaires de } E\}$ est un groupe pour la composition des applications linéaires.

1.3 Sous-groupe

1.3.1 Premières propriétés

Sauf mention contraire, G désigne toujours un groupe multiplicatif d'élément neutre e .

Définition 3.

Une partie non vide H de G est un **sous-groupe** de G si :

1. $(x; y) \in H \times H \Rightarrow xy \in H$
2. $x \in H \Rightarrow x^{-1} \in H$

Remarque 3.

a) Les deux conditions ci-dessus impliquent que $e \in H$

b) Un sous-groupe de G est dit **propre** s'il est distinct de G et on écrira :

- $H \leq G$ pour exprimer que H est un sous-groupe de G , et
- $H < G$ pour exprimer que H est un sous-groupe propre de G .

Proposition 1.

Soit G un groupe et $\{H_i\}_{i \in I}$ une famille de sous-groupes de G ; alors quel que soit l'ensemble non vide I , $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Attention, en général $\bigcup_{i \in I} H_i$ n'est pas un sous-groupe de G .

En effet, on vérifie, par exemple, que dans le groupe $(\mathbb{Z}, +)$, les ensembles $3\mathbb{Z} = \{3k; k \in \mathbb{Z}\}$ et $8\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$;
mais $11 = 3 + 8 \notin 3\mathbb{Z} \cup 8\mathbb{Z}$.

1.3.2 Exemples

1. Les groupes additifs $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont tels que $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$
2. Les groupes multiplicatifs $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ sont tels que $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$
3. $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$ est un sous-groupe multiplicatif de $\mathbb{C}^*$.
4. $\mathbb{U}_n = \{z_0, z_1, \dots, z_{n-1}\}$ où $z_k = e^{\frac{2i\pi}{n}k}$ est un sous-groupe fini d'ordre n de $\mathbb{U}$ donc de $\mathbb{C}^*$.
5. Si G est un groupe, l'ensemble :
 $Z(G) = \{x \in G, xa = ax, \text{ pour tout } a \in G\}$
est un sous-groupe de G appelé le *centre* de G . Il s'agit de l'ensemble des $x \in G$ qui commutent avec tout élément de G .
On remarque que $Z(G)$ est un sous-groupe propre de G si, et seulement si G n'est pas abélien.
6. Si E est un espace vectoriel de dimension $n \geq 2$, $GL(E) = GL_n(\mathbb{K})$ est un sous-groupe non abélien de $(M_n(\mathbb{K}), \times)$.
7. L'ensemble des similitudes de $\mathbb{R}^2$ est un sous-groupe de $GL_2(\mathbb{R})$.
8. L'ensemble des isométries d'un espace affine euclidien est un sous-groupe de son groupe affine.

1.3.3 Sous-groupes engendrés

Définition 4.

Soient G un groupe et S une partie non vide de G . On désigne par $\mathcal{H}_S$ l'ensemble des sous-groupes de G contenant S et on pose :

$$\langle S \rangle = \bigcap_{H \in \mathcal{H}_S} H.$$

$\langle S \rangle$ est un sous-groupe de G appelé **sous-groupe de G engendré par S** .

Remarque 4.

- a) Dans l'ensemble des sous-groupes de G ordonné par l'inclusion, $\langle S \rangle$ est le plus petit sous-groupe de G contenant S .
- b) On peut montrer que

$$\langle S \rangle = \{x_1 x_2 \dots x_n; n \in \mathbb{N}^*, x_i \in S \text{ ou } x_i^{-1} \in S, 1 \leq i \leq n\}$$

Définition 5. Soient G un groupe.

- 1. Si S une partie non vide de G telle que $\langle S \rangle = G$, on dit que S est une partie génératrice de G ou encore que S engendre G .
- 2. Si G est engendré par un élément, c'est à dire s'il existe $x \in G$ tel que $\langle x \rangle = G$, le groupe G est dit **monogène**.
- 3. Plus généralement, s'il existe une partie non vide et finie $S = \{x_1 x_2 \dots x_n\}$ de G telle que $\langle S \rangle = G$, on dit que G est de **type fini**.
Un groupe fini est de type fini, mais la réciproque est fausse.
- 4. On appellera **groupe cyclique** tout groupe monogène fini.

Exemple 1.

- 1. Reprenons le groupe symétrique $S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$.
On montre que $\sigma_1 = \sigma_2$ et $\sigma_1^3 = e$, d'où :

$$\langle \sigma_1 \rangle = \{\sigma_1, \sigma_2, e\}$$

D'autre part, $\sigma_1 \circ \tau_3 = \tau_2$ et $\tau_3 \circ \sigma_1 = \tau_1$, et par suite :

$$\langle \sigma_1, \tau_3 \rangle = \{\sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3, e\}$$

- 2. $\mathbb{Z}$ est un groupe monogène infini, engendré par 1 ou par -1.

Définition 6.

Soit x un élément d'un groupe G quelconque.

- 1. Si le sous-groupe de G engendré par x est de cardinal fini, on dit que x est d'ordre fini dans G , et le cardinal du sous-groupe $\langle x \rangle$ s'appelle l'ordre de x dans G , noté $o(x)$.
- 2. Si le sous-groupe de G engendré par x est de cardinale infini, on dit que x est d'ordre infini dans G .

Exemple 2.

1. L'élément neutre est le seul élément d'ordre 1 dans un groupe G .
2. Tout élément non nul dans $\mathbb{Z}$ est d'ordre infini.
3. Dans S_3 , les transpositions τ_1, τ_2 et τ_3 sont d'ordre 2, et les cycles σ_1 et σ_2 sont d'ordre 3.

1.4 Morphisme de groupe

1.4.1 Propriétés générales

Définition 7.

Etant donnés deux groupes $(G, .)$ et $(G', *)$, un **morphisme de groupes** de G dans G' est une application $f : G \longrightarrow G'$ telle que, quels que soient x et y dans G , on ait :

$$f(x.y) = f(x) * f(y)$$

L'ensemble des morphismes d'un groupe G dans un groupe G' sera noté $\text{Hom}(G, G')$.

L'ensemble des morphismes d'un groupe G dans lui même sera noté $\text{End}(G)$.

Proposition 2. Tout $f \in \text{Hom}(G, G')$ vérifie les propriétés suivantes :

1. $f(e) = e'$
2. $f(x^{-1}) = f(x)^{-1}$, quel que soit $x \in G$
3. $f(x^n) = (f(x))^n$, quel que soit $x \in G$ et $n \in \mathbb{N}$
4. $H \leq G \Rightarrow f(H) \leq G'$
5. $H' \leq G' \Rightarrow f^{-1}(H') \leq G$, où $f^{-1}(H') = \{x \in G, f(x) \in H'\}$

Corollaire 1.

1. $f(G)$ est un sous-groupe de G'
2. $f^{-1}(e')$ est un sous-groupe de G

Définition 8. Soit $f \in \text{Hom}(G, G')$

$f(G)$ est appelé **image de f** et est noté $\text{Im} f$ $f^{-1}(e')$ est appelé **noyau de f** et est noté $\text{Ker} f$

Proposition 3. Pour $f \in \text{Hom}(G, G')$, on a :

1. f surjectif $\Leftrightarrow \text{Im} f = G'$
2. f injectif $\Leftrightarrow \text{Ker} f = \{e\}$

1.4.2 Premiers exemples

1. Soit G un groupe et H un sous-groupe de G .

$$\begin{array}{ccc} \text{L'injection canonique } i: & H & \longrightarrow G \\ & x & \longmapsto x \end{array}$$

est un morphisme *injectif* de groupes.

2. Soit $n \in \mathbb{Z}^*$.

$$\begin{array}{ccc} \text{La surjection canonique } \pi: & \mathbb{Z} & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ & x & \longmapsto \bar{x} \end{array}$$

est un morphisme *surjectif* de groupes.

3. Soit un entier $n > 1$.

$$\begin{array}{ccc} \text{L'application } \det: & GL_n(\mathbb{R}) & \longrightarrow \mathbb{R}^* \\ & A & \longmapsto \det(A) \end{array}$$

est un morphisme de groupe.

Son noyau $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}), \det(A) = 1\}$ est appelé **groupe spécial linéaire**.

1.4.3 Théorème de Cayley

Définition 9.

1. Une application f d'un groupe G dans un groupe G' est un **isomorphisme de groupes** si $f \in \text{Hom}(G, G')$ et s'il existe $g \in \text{Hom}(G', G)$ tel que :

$$g \circ f = \text{id}_G \text{ et } f \circ g = \text{id}_{G'}$$

2. S'il existe un isomorphisme entre deux groupes G et G' , on dit que G et G' sont isomorphes, et on note : $G \simeq G'$.
3. Un isomorphisme d'un groupe G sur lui même est appelé un **automorphisme** de G . L'ensemble des automorphismes de G est noté $\text{Aut}(G)$.

Proposition 4.

Pour tout groupe G , $\text{Aut}(G)$ est un sous-groupe du groupe symétrique de G (càd du groupe des bijections de G sur lui même).

Remarque 5.

a) On peut montrer que f isomorphisme $\Leftrightarrow f \in \text{Hom}(G, G')$ et f bijectif

b) Un isomorphisme étant une bijection, deux groupes isomorphes sont équipotents (càd de même cardinal).

En particulier, deux groupes finis isomorphes sont de même ordre. Attention la réciproque est fautive, comme le montre l'exemple ci-dessous.

On considère le groupe $G = \mathbb{Z}/4\mathbb{Z}$

et le groupe $G' = \{e, a, b, c, d\}$ que l'on notera V (pour Vierergruppe).

Le groupe V est défini par les égalités : $a = b = c = e$, $ab = ba = c$,

$ac = ca = b$ et $bc = cb = a$.

Dans V , tout élément non nul est d'ordre 2 et est son propre inverse.

En revanche dans $\mathbb{Z}/4\mathbb{Z}$, $\bar{1}$ et $\bar{3}$ sont d'ordre 4.

Un éventuel isomorphisme entre $\mathbb{Z}/4\mathbb{Z}$ et V enverrait par exemple $\bar{1}$ sur un élément de V d'ordre 4... qui n'existe pas.

On a mis en évidence l'existence de deux groupes finis de même ordre qui ne sont pas isomorphes. En particulier, V n'est pas cyclique, bien qu'abélien.

Exemple 3. Exemples d'isomorphismes

1. Si E est un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$,

$$GL(E) \simeq GL_n(\mathbb{K})$$

Toute base $b = \{e_1; e_2 \dots e_n\}$ de E sur $\mathbb{K}$ permet de définir un isomorphisme :

$$\begin{aligned} M_b : GL(E) &\longrightarrow GL_n(\mathbb{K}) \\ u &\longmapsto M_b(u) \end{aligned}$$

où $M_b(u)$ est la matrice de u dans la base b , c'est à dire la matrice dont les colonnes sont formées par les composantes, dans b , des vecteurs $u(e_1), u(e_2), \dots, u(e_n)$.

2. De façon générale, si $f \in \text{Hom}(G, G')$ et f injectif, alors $G \simeq \text{Im}(f)$.

3. **Automorphismes intérieurs d'un groupe G :**

$$\begin{aligned} \text{À tout } g \in G, \text{ on associe l'application : } \sigma_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

Toutes ces applications sont des automorphismes de G .

Mieux, en posant $\text{Int}(G) = \{\sigma_g; g \in G\}$,

on montre que $\text{Int}(G)$ est un sous-groupe de $\text{Aut}(G)$.

4. À tout $g \in G$, on associe l'application : $\tau_g : G \longrightarrow G$

$$x \longmapsto gx$$

Toutes ces applications sont des automorphismes de G .

Attention, l'ensemble $T(G) = \{\tau_g; g \in G\}$, est un sous ensemble (et même un sous-groupe) du groupe symétrique de G mais n'est pas un sous-groupe de $\text{Aut}(G)$.

Théorème 1. Théorème de Cayley

Tout groupe est isomorphe à un sous-groupe du groupe de ses permutations.

En particulier, tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique S_n . Précisons :

$$\begin{aligned} \text{L'application : } \tau : G &\longrightarrow T(G) \\ g &\longmapsto \tau_g \end{aligned}$$

est un isomorphisme de groupes.

1.5 Produit direct de groupes

Soient deux groupes G_1 et G_2 d'éléments unités e_1 et e_2 .

Posons $G = G_1 \times G_2 = \{(x_1; x_2); x_1 \in G_1 \text{ et } x_2 \in G_2\}$.

On vérifie facilement que l'ensemble non vide G muni de la loi de composition interne définie par : $\tau :$

$$\begin{aligned} G \times G &\longrightarrow G \\ ((x_1; x_2), (y_1; y_2)) &\longmapsto (x_1 x_2; y_1 y_2) \end{aligned}$$

est un groupe dont l'élément neutre est $(e_1; e_2)$

et quel que soit $(x_1; x_2) \in G$, $(x_1; x_2)^{-1} = (x_1^{-1}; x_2^{-1})$.

Définition 10.

Le groupe $G_1 \times G_2$ est appelé **groupe produit direct** des groupes G_1 et G_2 .

On associe au produit direct $G_1 \times G_2$ deux couples d'applications :

a) **les projections canoniques p_1 et p_2** telles que :

$$\begin{aligned} p_1 : G_1 \times G_2 &\longrightarrow G_1 \text{ et } p_2 : G_1 \times G_2 \longrightarrow G_2 \\ (x_1; x_2) &\longmapsto x_1 \qquad \qquad (x_1; x_2) \longmapsto x_2 \end{aligned}$$

b) **les injections canoniques q_1 et q_2** telles que :

$$\begin{aligned} q_1 : G_1 &\longrightarrow G_1 \times G_2 \text{ et } q_2 : G_2 \longrightarrow G_1 \times G_2 \\ x_1 &\longmapsto (x_1; e_2) \qquad \qquad x_2 \longmapsto (e_1; x_2) \end{aligned}$$

Remarque 6.

a) $G_1 \times G_2$ est abélien $\Leftrightarrow G_1$ abélien et G_2 abélien .

b) Les applications $G_1 \longrightarrow G_1 \times \{e_2\} = \text{Im } q_1$ et $G_2 \longrightarrow \{e_1\} \times G_2 = \text{Im } q_2$
 $x_1 \longmapsto (x_1; e_2) \qquad \qquad x_2 \longmapsto (e_1; x_2)$

sont des isomorphismes de groupes.

En particulier, $G_1 \times G_2$ contient au moins un sous-groupe isomorphe à G_1

et un sous-groupe isomorphe à G_2 .

c) Si G_1 et G_2 sont des groupes finis, on a :

$$o(G_1 \times G_2) = o(G_1) \times o(G_2)$$

Proposition 5. Soient deux groupes G_1 et G_2 .

Un groupe G est isomorphe à $G_1 \times G_2$ si, et seulement s'il contient deux sous-groupes H_1 et H_2 tels que :

1. $H_i \simeq G_i$, pour $i = 1, 2$.
2. $\forall h_1 \in H_1, \forall h_2 \in H_2, h_1 h_2 = h_2 h_1$.
3. $G = H_1 H_2$.
4. $H_1 \cap H_2 = \{e\}$, où e est l'élément neutre de G

Exemple 4. Le groupe produit direct $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est généralement appelé le groupe de Klein.

D'après la remarque a) ci-dessus, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe abélien fini d'ordre 4.

Considérons alors le Vierergruppe, $V = \{e, a, b, c\}$ avec les règles de calcul que l'on rappelle : $a = b = c = e$ et $ab = ba = c, bc = cb = a, ac = ca = b$.
 Dans V , on pose :

$$H_1 = \{e, a\} = \langle a \rangle \text{ et } H_2 = \{e, b\} = \langle b \rangle.$$

On remarque que $H_1 \simeq H_2 \simeq \mathbb{Z}/2\mathbb{Z}$

D'autre part, $ab = ba = c$, d'où $V = H_1 H_2$.

De plus, comme $H_1 \cap H_2 = \{e\}$, on a, d'après la proposition précédente :

$$V \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Chapitre 2

Classe modulo un sous-groupe

2.1 Théorème de Lagrange. Indice d'un sous groupe

2.1.1 Relation d'équivalence modulo un sous-groupe

A tout sous-groupe H d'un groupe G , on peut associer *deux relations binaires* $\mathcal{R}_H$ et ${}_H\mathcal{R}$ définies dans G par :

$$x \mathcal{R}_H y \Leftrightarrow xy^{-1} \in H \text{ et } x {}_H\mathcal{R} y \Leftrightarrow x^{-1}y \in H$$

Proposition 6. G étant un groupe :

1. Pour tout sous-groupe H de G , les relations $\mathcal{R}_H$ et ${}_H\mathcal{R}$ sont des relations d'équivalence.
2. $x \equiv y \pmod{\mathcal{R}_H} \Leftrightarrow y \in Hx$, où $Hx = \{hx; h \in H\}$
 $x \equiv y \pmod{{}_H\mathcal{R}} \Leftrightarrow y \in xH$, où $xH = \{xh; h \in H\}$

Définition 11.

1. H étant un sous-groupe d'un groupe G , les relations d'équivalence $\mathcal{R}_H$ et ${}_H\mathcal{R}$ sont appelées **relation d'équivalence à droite et à gauche de x modulo H** .
2. Pour $x \in G$, les ensembles Hx et xH sont appelés **classes à droite et classes à gauche de x modulo H** .

Remarque 7.

1. Les classes à droite (resp. à gauche) modulo H étant des classes d'équivalence, deux classes sont soit disjointes, soit égales.
Donc, si $\{x_i\}_{i \in I}$ est une famille de représentants des classes à droite (resp. à gauche) modulo H , distinctes, alors la famille $\{Hx_i\}_{i \in I}$ forme une partition de G :

$$G = \bigcup_{i \in I} Hx_i \text{ et } (Hx_i \neq Hx_j \Leftrightarrow i \neq j)$$

2. Si G est abélien, quel que soit $H \leq G$, et quel que soit $x \in G$, on a $Hx = xH$, donc $\mathcal{R}_H = {}_H\mathcal{R}$.
 Dans ce cas, deux éléments x et y de G , équivalents modulo $\mathcal{R}_H$ seront dits **équivalents modulo H** ; on écrira :
 L'ensemble quotient de G par $\mathcal{R}_H$ ($= {}_H\mathcal{R}$) sera noté $\frac{G}{H}$ et appelé quotient de G par H .
3. Si le groupe G est non abélien, en général, les classes à gauche et à droite ne coïncident pas, donc $\mathcal{R}_H \neq {}_H\mathcal{R}$.
 On note alors les ensembles quotients $\frac{G}{\mathcal{R}_H}$ et $\frac{G}{{}_H\mathcal{R}}$ respectivement $(\frac{G}{H})_d$ et $(\frac{G}{H})_g$.

Exemple 5.

1. On rappelle que le groupe S_3 est engendré par :
 $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
 Pour simplifier l'écriture, posons : $\sigma = \sigma_1$ et $\tau = \tau_3$.
 On a alors $S_3 = \{e, \tau, \sigma, \sigma^2, \tau \circ \sigma, \sigma \circ \tau\}$.
 Soit $H = \langle \tau \rangle = \{e, \tau\}$. Les classes à droite et à gauche de S_3 modulo H sont respectivement :

$$\begin{cases} H = \{e, \tau\} \\ H\sigma = \{\tau \circ \sigma\} \\ H\sigma^2 = \{\sigma^2, \tau \circ \sigma^2 = \sigma \circ \tau\} \end{cases} \quad \begin{cases} H = \{e, \tau\} \\ \sigma H = \{\sigma \circ \tau\} \\ \sigma^2 H = \{\sigma^2, \sigma^2 \circ \tau = \tau \circ \sigma\} \end{cases}$$

 $\tau \circ \sigma \neq \sigma \circ \tau \Rightarrow H\sigma \neq \sigma H$, d'où $\mathcal{R}_H \neq {}_H\mathcal{R}$.
2. Soit $H = n\mathbb{Z}$ un sous-groupe de $(\mathbb{Z}, +)$
 Le groupe $(\mathbb{Z}, +)$ étant abélien, on a $\mathcal{R}_H = {}_H\mathcal{R}$.
 L'équivalence modulo $(n\mathbb{Z})$ coïncide donc avec la congruence modulo n . Le quotient $\mathbb{Z}/n\mathbb{Z}$ est donc muni d'une structure de groupe, induite par celle de $\mathbb{Z}$.
 En fait, il en est de même pour tout quotient d'un groupe abélien par l'un quelconque de ses sous-groupes.

2.1.2 Théorème de Lagrange. Indice d'un sous groupe

Théorème 2. *Théorème de Lagrange*

Si G est un groupe fini, alors l'ordre de tout sous-groupe H de G divise l'ordre de G .

Corollaire 2.

Si G est un groupe fini, quel que soit $x \in G$, l'ordre de x divise l'ordre de G .

Théorème 3.

Pour tout sous-groupe H d'un groupe G , les ensembles $(\frac{G}{H})_d$ et $(\frac{G}{H})_g$ sont

équipotents.

Précisons : la correspondance $\theta : \begin{matrix} (\frac{G}{H})_d & \longrightarrow & (\frac{G}{H})_g \\ Hx & \longmapsto & x^{-1}H \end{matrix}$ est une bijection.

Ce théorème légitime la définition suivante :

Définition 12.

Étant donné un sous-groupe H d'un groupe G , $\text{card}((\frac{G}{H})_d) = \text{card}((\frac{G}{H})_g)$ s'appelle **l'indice de H dans G** et se note $[G : H]$.

Si $[G : H]$ est fini, on dit que H est d'indice fini dans G .

Remarque 8.

a) Si G est un groupe fini, alors pour tout sous-groupe H de G , on a :

$$o(G) = o(H) [G : H].$$

b) $[G : H]$ peut être fini sans que ni G ni H ne le soit.

Considérons par exemple $G = \mathbb{Z}$ muni de l'addition, et son sous-groupe non nul $H = n\mathbb{Z}$ qui sont des groupes de cardinal infini.

On sait que $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n , donc $[\mathbb{Z} : n\mathbb{Z}] = n$, bien que G et H soient infinis.

2.1.3 Formule des indices

Théorème 4. Formule des indices

Si H est un sous-groupe de G d'indice fini, et si K est un sous-groupe de G contenant H , alors K est d'indice fini dans G .

De plus on a la formule suivante :

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

Cette formule s'appelle la **formule des indices**.

2.2 1^{er} théorème d'isomorphisme

2.2.1 Compatibilité d'une relation d'équivalence avec une loi de composition

L'idée est qu'on aimerait que les ensembles quotients créés à partir d'une relation d'équivalence modulo un sous-groupe héritent de la loi de composition du groupe de départ.

On introduit pour cela la notion suivante :

Définition 13. Soit $\mathcal{R}$ une relation d'équivalence définie dans un ensemble $(E, \cdot)$. On dit que :

1. $\mathcal{R}$ est compatible à droite (resp. à gauche) avec la loi $\cdot$ si, quels que soient $x, y, a \in E$,

$$x\mathcal{R}y \Rightarrow x.a\mathcal{R}y.a$$

$$(resp. x\mathcal{R}y) \Rightarrow a.x\mathcal{R}a.y$$

2. $\mathcal{R}$ est **compatible avec la loi** . si, quels que soient $x, x', y, y' \in E$,

$$(x\mathcal{R}y \text{ et } x'\mathcal{R}y') \Rightarrow x.x'\mathcal{R}y.y'$$

La proposition suivante nous rapproche de notre but :

Proposition 7.

Une relation d'équivalence $\mathcal{R}$ définie dans un ensemble $(E, .)$ est compatible avec la loi si, et seulement si elle est compatible à droite et à gauche avec cette loi.

2.2.2 Deux cas très utiles

La proposition suivante va nous permettre de conclure.

Proposition 8.

Pour tout sous-groupe H d'un groupe G , la relation d'équivalence $\mathcal{R}_H$ (resp. ${}_H\mathcal{R}$) est compatible à droite (resp. à gauche) avec la loi de composition de G .

Cas où le groupe G est abélien

Pour tout sous-groupe H de G on a vu qu'on a alors $\mathcal{R}_H = {}_H\mathcal{R}$.

Cette relation d'équivalence est, d'après les deux dernières propositions, compatible avec la loi de composition de G .

Par suite, l'ensemble quotient de G par $\mathcal{R}_H$ ($= {}_H\mathcal{R}$), noté $\frac{G}{H}$, est muni de la loi de composition quotient de celle de G telle que :

quels que soient $\bar{x}$ et $\bar{y}$ dans $\frac{G}{H}$:

$$\bar{x}\bar{y} = \overline{xy}$$

Cas où le sous-groupe H de G est le noyau d'un morphisme de groupes.

On considère deux groupes quelconques G et G' et $f \in \text{Hom}(G, G')$.

Posons $H = \text{Ker} f$ et considérons les relations $\mathcal{R}_H$ et ${}_H\mathcal{R}$.

Dans G on a :

$$\begin{aligned} x\mathcal{R}_Hy &\Leftrightarrow xy^{-1} \in \text{Ker} f \\ &\Leftrightarrow f(xy^{-1}) = e', \text{ élément unité de } G' \\ &\Leftrightarrow f(x)f(y)^{-1} = e' \\ &\Leftrightarrow f(x) = f(y) \end{aligned}$$

On vérifie de même que $x_H\mathcal{R}y \Leftrightarrow f(x) = f(y)$, d'où $\mathcal{R}_H = {}_H\mathcal{R}$.

Posons alors $\frac{G}{H} = (\frac{G}{H})_d = \frac{G}{H}_g$.

Plus précisément, on a dans notre cas $H = \text{Ker} f$, donc on notera notre quotient $\frac{G}{\text{Ker} f}$, et en s'appuyant, comme dans le cas abélien, sur les propositions précédentes, on obtient cette proposition d'où découlera le 1^{er} théorème d'isomorphisme :

Proposition 9. *Pour tout morphisme f d'un groupe G dans un groupe G' :*

1. *L'ensemble quotient $\frac{G}{\text{Ker}f}$ est un groupe par rapport à la loi de composition quotient, définie par $\bar{x}\bar{y} = \overline{xy}$, quels que soient $\bar{y}$ dans $\frac{G}{\text{Ker}f}$.*

2. *L'application canonique $\pi : G \longrightarrow \frac{G}{\text{Ker}f}$*

$$x \longmapsto \bar{x}$$

est un morphisme de groupe surjectif.

Théorème 5. *1^{er} théorème d'isomorphisme*

Pour tout morphisme f d'un groupe G dans un groupe G' , on a :

$$\frac{G}{\text{Ker}f} \simeq \text{Im}f$$

Chapitre 3

Groupes monogènes, symétriques et diédraux.

Les familles de groupes étudiées dans ce chapitre représentent des types fondamentaux de structures de groupes, qui serviront de références dans la description d'autres groupes.

3.1 Groupes monogènes

3.1.1 Caractérisation des groupes monogènes

On rappelle qu'un groupe G est monogène s'il existe un élément l'engendrant.

Un tel élément x est un *générateur* de G , et si le groupe est multiplicatif, on écrit :

$$G = \langle x \rangle = \{x^k, k \in \mathbb{Z}\}.$$

Nous avons déjà vu qu'il existe des groupes monogènes infinis, comme $(\mathbb{Z}, +)$ et des groupes monogènes finis, que l'on dit cyclique, comme $\mathbb{Z}/n\mathbb{Z}$.

Ce sont en fait, à isomorphisme prêt, les seuls.

Théorème 6.

Si G est un groupe monogène, alors G vérifie l'une des conditions suivantes :

1. $G \simeq \mathbb{Z}$, dans ce cas G est monogène infini, ou
2. il existe un entier $n > 0$ tel que $G \simeq \mathbb{Z}/n\mathbb{Z}$, et dans ce cas G est cyclique d'ordre n .

Remarque 9.

1. Deux groupes monogènes infinis sont isomorphes.
- Deux groupes cycliques de même ordre n sont isomorphes.

2. Si G est un groupe fini d'ordre n , et x un élément de G d'ordre m , alors :

- a) $\langle x \rangle \simeq \mathbb{Z}/m\mathbb{Z}$
- b) $(k \in \mathbb{Z} \text{ et } x^k = e) \Leftrightarrow k \in m\mathbb{Z}$
- c) m est le plus petit entier strictement positif tel que $x^m = e$
- d) $x^n = e$

Exemple 6.

Pour tout entier $n > 0$, le groupe multiplicatif $\mathbb{U}_n$ des racines de l'unité dans $\mathbb{C}$, est cyclique d'ordre n .

En effet, on a déjà vu que $\mathbb{U}_n = \{z_k\}_{0 \leq k \leq n-1}$ où $z_k = \cos \frac{2ik\pi}{n} + i \sin \frac{2ik\pi}{n}$, est un groupe fini d'ordre n . Il nous reste à déterminer un élément d'ordre n .

Mais pour tout $0 \leq k \leq n-1$, $z_1^k = z_k$ (c'est la formule de Moivre), et n est le plus petit k entier tel que $z_1^k = e$.

On en déduit que $\mathbb{U}_n = \langle z_1 \rangle$ est cyclique d'ordre n .

Proposition 10.

Tout groupe fini d'ordre premier p est cyclique.

3.1.2 Sous-groupes d'un groupe monogène

Théorème 7.

- a) Tout sous-groupe non trivial d'un groupe monogène infini, est monogène infini.
- b) Tout sous-groupe d'un groupe cyclique, est cyclique.

Proposition 11.

Soit $n \in \mathbb{N}$, et considérons le morphisme canonique $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

Pour tout sous-groupe K de $\mathbb{Z}/n\mathbb{Z}$, il existe un unique diviseur k de n tel que $\pi(k) = \bar{k}$ engendre K . De plus, $o(K) = \frac{n}{k}$.

Corollaire 3. n est un entier strictement positif

Le nombre de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est égal au nombre de diviseurs de n dans $\mathbb{N}^*$.

Exemple 7.

Les diviseurs de 6 dans $\mathbb{N}^*$ sont 1, 2, 3 et 6. $\mathbb{Z}/6\mathbb{Z}$ possède donc 4 sous-groupes distincts.

$$\langle \bar{1} \rangle = \mathbb{Z}/6\mathbb{Z} \quad \langle \bar{2} \rangle = \{\bar{0}; \bar{2}; \bar{4}\} \quad \langle \bar{3} \rangle = \{\bar{0}; \bar{3}\} \quad \langle \bar{6} \rangle = \{\bar{0}\}$$

On a bien, par exemple, $\langle \bar{2} \rangle$ qui est d'ordre $\frac{6}{2} = 3$.

De plus, les sous-groupes $\langle \bar{4} \rangle$ et $\langle \bar{5} \rangle$ coïncident nécessairement avec l'un des sous-groupes ci-dessus.

En effet : $\langle \bar{4} \rangle = \langle \bar{2} \rangle$, et $\langle \bar{5} \rangle = \langle \bar{1} \rangle = \mathbb{Z}/6\mathbb{Z}$

Ce résultat sera justifié et généralisé dans la sous-partie suivante.

On déduit de l'étude des sous groupes de $\mathbb{Z}/n\mathbb{Z}$ le théorème suivant, relatif aux groupes cycliques quelconques, notés multiplicativement.

Théorème 8. $G = \langle x \rangle$ est un groupe cyclique d'ordre n

Pour tout diviseur d de n , il existe un et un seul sous-groupe de G d'ordre d . Celui-ci est engendré par x^k , où $k = \frac{n}{d}$.

Remarque 10.

Nous venons de voir que pour un groupe cyclique G d'ordre n , il existe une bijection entre les diviseurs de n et les sous-groupes (cycliques !) de G .

Mais attention, si G est un groupe fini quelconque d'ordre n , et si $d \in \mathbb{N}^*$ divise n , alors :

a) Il n'existe en général pas de sous-groupe de G d'ordre d .

Le groupe alterné A_4 par exemple ne possède pas de sous-groupe d'ordre 6.

b) S'il existe un sous-groupe de G d'ordre d , il n'est pas nécessairement unique. Penser par exemple au groupe de Klein qui possède deux sous-groupes d'ordre 2.

c) Tous les sous-groupes de G peuvent être cycliques sans que G ne le soit. Penser par exemple au groupes Q_8 des quaternions, non cyclique et même non abélien.

3.1.3 Générateurs d'un groupe monogène

On rappelle que dans $\mathbb{Z}$, deux éléments sont dits **premiers entre eux** si leurs seuls diviseurs communs sont 1 et -1,

c'est à dire si leur PGCD vaut 1. On notera (a, b) le PGCD de a et b .

Le résultat suivant est supposé connu :

Théorème 9. *Théorème de Bézout*

Deux entiers non nuls a et b sont premiers entre eux dans $\mathbb{Z}$ si, et seulement si il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = 1$$

Théorème 10. Soit un groupe monogène $G = \langle x \rangle$ (noté multiplicativement)

1. Si G est monogène infini, alors les seuls générateurs de G sont x et x^{-1}

2. Si G est cyclique d'ordre $n > 1$, alors les générateurs de G sont les x^k tels que k et n sont premiers entre eux dans $\mathbb{Z}$.

Remarque 11. Si G est un groupe cyclique d'ordre n , il suffit en fait de considérer les entiers k premiers avec n tels que $0 \leq k \leq n-1$, pour obtenir tous les générateurs x^k de G .

En effet, soit $k \in \mathbb{Z}$ tel que $(k, n) = 1$. Par division euclidienne, il existe s et k' des entiers tels que $k = sn + k'$ et $1 \leq k' \leq n-1$.

On a alors $x^k = x^{sn}x^{k'} = x^{k'}$, car $x^{ns} = (x^n)^s = e^s = e$.

et $(k', n) = 1$ car tout diviseur de k' et n divise aussi k .

Définition 14. *Fonction d'Euler*

Pour $n \in \mathbb{N}^*$, posons $E_n = \{k \in \mathbb{N}; 1 \leq k \leq n-1 \text{ et } (k, n) = 1\}$

On appelle **fonction d'Euler** l'application $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ telle que :

$$\varphi(1) = 1 \text{ et } \varphi(n) = \text{card}(E(n)), \text{ quel que soit } n > 0.$$

On peut alors reformuler le théorème précédent :

Proposition 12.

Un groupe cyclique d'ordre n possède exactement $\varphi(n)$ générateurs, où φ est la fonction d'Euler.

Remarque 12.

On ne sait a priori pas calculer $\varphi(n)$ (on va le voir dans la section suivante), mais on sait que si p est un nombre premier, $\varphi(p) = p - 1$

Proposition 13. Caractérisation des générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$

Pour un entier $n > 1$, les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les éléments inversibles (pour la multiplication) de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Leur ensemble forme un groupe multiplicatif, abélien, d'ordre $\varphi(n)$ et noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

On étudiera en détail, en exercices, le groupe des inversibles (qui sont les générateurs) d'un groupe cyclique.

Remarque 13.

Dans l'anneau $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier, l'ensemble des inversibles est donc de cardinal $\varphi(p) = p - 1$, tout élément non nul est donc inversible. Cela montre que les anneaux $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier sont des corps !

3.1.4 Calcul de $\phi(n)$

Rappelons au préalable quelques résultats d'arithmétique sur $\mathbb{Z}$:

Si m et n sont deux entiers dont $d > 0$ est le PGCD et $l > 0$ le PPCM.

On a :

1. $dl = mn$,
donc en particulier, $(m, n) = 1 \Leftrightarrow mn$ est le PPCM de m et n .
2. $m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}$

Ayant déjà remarqué qu'un produit direct de groupes cycliques n'est pas nécessairement cyclique (groupe de Klein par exemple), on peut maintenant donner le résultat précis suivant :

Théorème 11. m et n sont deux entiers strictement positifs

Les anneaux (donc en particulier les groupes additifs) $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes si, et seulement si m et n sont premiers entre eux.

Ce théorème se généralise au cas d'un nombre fini d'entiers $m_1, m_2, \dots, m_k$.

Corollaire 4. *Théorème chinois*

Soient $m_1, m_2, \dots, m_k$ ($k \geq 2$) des entiers positifs non nuls.

Alors les anneaux :

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/m_1m_2\dots m_k\mathbb{Z}$$

sont isomorphes si, et seulement si les m_i sont deux à deux premiers entre eux.

On peut alors énoncer le théorème permettant le calcul de $\varphi(n)$, pour $n > 1$. Celui-ci est basé sur deux lemmes que nous démontrerons en exercices.

Théorème 12. *Soit $n > 1$ un entier.*

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition en facteurs premiers de n , alors :

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

3.2 Groupes symétriques S_n

3.2.1 Notion de σ -orbite

On rappelle que le groupe S_n est le groupe des permutations (càd des bijections sur lui même) de l'ensemble $\{1, 2, \dots, n\}$, muni de la composition des applications. Il peut être considéré plus généralement comme le groupe des permutations d'un ensemble quelconque à n éléments. Le groupe S_n est fini, de cardinal $n!$.

Définition 15. *Soit $\sigma \in S_n$.*

*Le **support de σ** est l'ensemble $\text{supp}(\sigma) = \{i \in \{1, 2, \dots, n\}, \sigma(i) \neq i\}$*

Remarque 14.

1. Dans S_n , $\sigma = e \Leftrightarrow \text{supp}(\sigma) = \emptyset$ 2. Si $\sigma \in S_n$ et $\sigma \neq e$, la restriction de σ à $\text{supp}(\sigma)$ est une permutation de l'ensemble $\text{supp}(\sigma)$. 3. $\text{supp}(\sigma) = \text{supp}(\sigma^{-1})$ et $\text{supp}(\sigma^k) \subseteq \text{supp}(\sigma), \forall k \in \mathbb{Z}$

Proposition 14.

Deux permutations à supports disjoints commutent dans S_n .

A toute permutation $\sigma \in S_n$, on peut associer une relation binaire $\mathcal{R}_\sigma$ définie sur $\{1, 2, \dots, n\}$ par :

$$i\mathcal{R}_\sigma k \Leftrightarrow \exists r \in \mathbb{Z}, \sigma^r(i) = k.$$

On montre $\mathcal{R}_\sigma$ est une relation d'équivalence dans $\{1, 2, \dots, n\}$ et que la classe d'équivalence d'un élément $i \in \{1, 2, \dots, n\}$ est :

$$\Omega_\sigma(i) = \{\sigma^r(i), r \in \mathbb{Z}\}$$

Définition 16. Soit $\sigma \in S_n$ et $i \in \{1, 2, \dots, n\}$.
 $\Omega_\sigma(i)$ s'appelle la σ -orbite de i

Remarque 15.

1. Soit $\sigma \neq e \in S_n$ tel que $o(\sigma) = p$
alors $\langle \sigma \rangle = \{\sigma^r, r \in \mathbb{Z}\} = \{e, \sigma, \dots, \sigma^{p-1}\}$.
De plus $1 \leq |\Omega_\sigma(i)| \leq p$ pour tout $i \in \{1, 2, \dots, n\}$,
avec $|\Omega_\sigma(i)| = 1 \Leftrightarrow i \notin \text{supp}(\sigma)$ (dans ce cas l'orbite est dite ponctuelle).
2. Si $\{i_1, i_2, \dots, i_q\}$ est une famille de représentants des σ -orbites distinctes de $\{1, 2, \dots, n\}$, alors les $\{\Omega_\sigma(i_l)_{1 \leq l \leq q}\}$ forment une partition de $\{1, 2, \dots, n\}$.
En particulier : $n = \sum_{1 \leq q \leq t} |\Omega_\sigma(i_q)|$

Exemple 8.

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ on a :
 $\Omega_\sigma(1) = \{1, 5, 3\}$, $\Omega_\sigma(2) = \{2\}$, $\Omega_\sigma(4) = \{4, 6\}$

3.2.2 Cycles, transpositions

Considérons la permutation :

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}$$

Le support de γ est $\{2, 4, 5, 6\}$ et on a : $\gamma(2) = 4$, $\gamma(4) = 6$, $\gamma(6) = 5$ et $\gamma(5) = 2$.

Dans le groupe S_6 , γ est un cycle de longueur 4 et est noté $(2, 4, 6, 5)$

Définition 17.

1. Une permutation $\gamma \in S_n$ est un **cycle de longueur r** ($1 \leq r \leq n$) (ou **r -cycle**) s'il existe un ensemble ordonné de r entiers distincts dans $\{1, 2, \dots, n\} : j_1, j_2, \dots, j_r$ tels que :

$$\gamma(j_1) = j_2, \gamma(j_2) = j_3, \dots, \gamma(j_{r-1}) = j_r \text{ et } \gamma(j_r) = j_1$$

$$\text{et } \gamma(j_k) = j_k \quad \forall k \in \{1, 2, \dots, n\} \setminus \{j_1, j_2, \dots, j_r\}$$

Un tel cycle sera noté $(j_1, j_2, \dots, j_r)$.

L'ensemble $\{j_1, j_2, \dots, j_r\}$ est le support de γ .

2. Un cycle de **longueur 2** dans S_n est appelé **transposition**.
Il s'agit donc d'une permutation qui, dans $\{1, 2, \dots, n\}$, échange deux éléments et laisse invariants tous les autres (lorsque $n \geq 3$).
3. Dans S_n , le **cycle de longueur n** , $\gamma_1 = (1, 2, \dots, n) = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & 1 \end{pmatrix}$
est appelé **permutation circulaire** des entiers $1, 2, \dots, n$.

Remarque 16.

1. Un cycle $(j_1, j_2, \dots, j_r)$ peut être noté $(j_k, j_{k+1}, \dots, j_r, j_1, j_2, \dots, j_{k-1})$, pour tout $(1 \leq k \leq r)$.
2. Un exemple : avec les notations du chapitre 1., les permutations τ_1, τ_2, τ_3 dans S_3 sont des transpositions, et les permutations $\sigma_1, \sigma_2, \sigma_3$ sont des 3-cycles.
3. Pour $n \geq 2$, le nombre de transpositions dans S_n est égal au nombre de façon de choisir deux éléments distincts dans $\{1, 2, \dots, n\}$. Il y en a donc $\binom{n}{2} = \frac{n(n-1)}{2}$.
4. Un cycle de longueur n n'est pas nécessairement la permutation circulaire. Considérer par exemple, dans S_4 :

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1, 3, 4, 2) \neq (1, 2, 3, 4)$$

Proposition 15. Dans S_n , un r -cycle est un élément d'ordre r .

Corollaire 5. Si $\tau \in S_n$ est une transposition, alors $\tau^2 = e$, donc $\tau^{-1} = \tau$.

Remarque 17.

1. Dans S_n , l'inverse d'un r -cycle est un r -cycle. En effet, si $\gamma = (j_1, j_2, \dots, j_r)$, alors :

$$\gamma^{-1} = \gamma^{r-1} = (j_r, j_{r-1}, \dots, j_2, j_1)$$

2. Attention, en général, pour $2 \leq p \leq r-2$, γ^p n'est pas un cycle. Il suffit par exemple de considérer, dans S_4 , la permutation circulaire γ_1 qui vérifie $\gamma_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ qui n'est pas un cycle...
3. La remarque précédente montre en particulier qu'un produit de cycles n'est pas nécessairement un cycle.

Proposition 16.

Dans S_n ($n \geq 2$), une permutation $\gamma \neq e$ est un cycle si, et seulement si, dans la décomposition de $1, 2, \dots, n$ en γ -orbites, il n'existe qu'une seule γ -orbite non ponctuelle ; le cardinal de celle-ci est alors égal à la longueur du cycle.

3.2.3 Décompositions d'une permutation

Dans S_n , deux cycles sont dits **disjoints** si leurs supports sont disjoints. D'après la Proposition 14, deux cycles disjoints commutent.

Théorème 13. Toute permutation $\sigma \neq e \in S_n$ s'écrit sous la forme :

$$\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s$$

où $s \in \mathbb{N}^*$, et $\gamma_1, \gamma_2, \dots, \gamma_s$ sont des cycles disjoints, tous différents de e . Cette décomposition est unique, à l'ordre des facteurs près.

Remarque 18.

1. La décomposition, unique, d'une permutation obtenue au théorème précédent sera appelée **décomposition canonique de σ en cycles**.
2. On peut reformuler le théorème précédent : S_n est engendré par l'ensemble de ses cycles.

Exemple 9. On reprend l'exemple précédent : les σ -orbites non ponctuelles sont $\Omega_\sigma(1) = \{1, 5, 3\}$ et $\Omega_\sigma(4) = \{4, 6\}$.

Donc $\sigma = \gamma_1 \circ \gamma_2$ où $\gamma_1 = (1, 5, 3)$ et $\gamma_2 = (4, 6)$.

On écrira : $\sigma = (1, 5, 3)(4, 6)$

Proposition 17.

Soit $\sigma \in S_n$ ($n \geq 2$).

Si $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s$ est la décomposition canonique de σ , alors l'ordre de σ dans S_n est égal au PPCM des longueurs des cycles γ_q ($1 \leq q \leq s$).

Théorème 14.

Toute permutation $\sigma \in S_n$ ($n \geq 2$) se décompose, de manière non unique, en produit de transpositions (non permutables en général).

Remarque 19.

1. La preuve du théorème s'appuie sur le fait que tout cycle peut s'écrire comme produit de transpositions.
Il suffit en effet de remarquer que pour tout $j_1, j_2, \dots, j_r \in \{1, 2, \dots, n\}$,
 $(j_1 j_2 \dots j_r) = (j_1, j_2)(j_2, j_3) \dots (j_{r-1}, j_r)$.
2. Attention cependant, la décomposition d'une permutation en produit de transpositions n'est pas unique.
Il suffit par exemple de remarquer que, $(j, k) \in S_n$ étant une transposition quelconque, on a $(j, k) = (1, j)(1, k)(1, j)$.
3. De plus, dans une décomposition de permutation en un produit de transpositions, deux de ces permutations, si elles ne sont pas disjointes, ne sont pas permutables.
En effet, si $i \neq j \neq k \in \{1, 2, \dots, n\}$, $(j, k)(k, l) \neq (k, l)(j, k)$.
4. On peut démontrer ce théorème sans passer par la décomposition en cycles.
5. Pour $n \geq 2$, le groupe S_n est engendré par l'ensemble de ses transpositions. Il existe en fait des familles plus restreintes de générateurs, voir ci-dessous.

Exemple 10.

On reprend toujours le même exemple dont la décomposition canonique est : $\sigma = (1, 5, 3)(4, 6)$.

D'après la remarque 1. , on a $\sigma = (1, 5)(5, 3)(4, 6)$.

Mais d'après la remarque 2. , on peut écrire $(5, 3) = (1, 5)(1, 3)(1, 5)$,
et donc $\sigma = (1, 3)(1, 5)(4, 6)$.

Cela fournit deux décompositions de σ en produit de transpositions.

Proposition 18. *Familles de générateurs de S_n*

1. Pour $n \geq 2$, le groupe S_n est engendré par l'ensemble des $(n-1)$ transpositions de la forme $(1, i)$, avec $2 \leq i \leq n$.
2. Pour $n \geq 2$, le groupe S_n est engendré par l'ensemble des $(n-1)$ transpositions de la forme $(i, i+1)$, avec $2 \leq i \leq n$.

3.2.4 Signature d'une permutation

Définition 18. Soit $\sigma \in S_n$, ($n \geq 1$).

Si t est le nombre de σ -orbites distinctes dans $\{1, 2, \dots, n\}$, alors on pose :

$$\varepsilon(\sigma) = (-1)^{n-t}$$

La quantité $\varepsilon(\sigma)$ est appelée **signature de la permutation σ** .

Remarque 20.

1. Si $\sigma = e$, alors $t = n$, donc $\varepsilon(e) = 1$.
2. Si τ , est une transposition, alors $t = n - 1$, donc $\varepsilon(\tau) = -1$.
3. Si γ , est un cycle de longueur r , alors $t = n - r + 1$, donc $\varepsilon(\gamma) = (-1)^{r-1}$.

Théorème 15. Soit $\sigma \in S_n$, ($n \geq 1$).

Si σ est le produit de k transpositions, alors :

$$\varepsilon(\sigma) = (-1)^k$$

De plus, si $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k = \tau'_1 \circ \tau'_2 \circ \dots \circ \tau'_l$ sont deux décompositions de σ en produit de transpositions, alors les entiers k et l sont de même parité.

La démonstration est basée sur le lemme suivant :

Lemme 1. Soit $\sigma \in S_n$, ($n \geq 1$).

Quelle que soit la transposition $\tau \in S_n$, on a :

$$\varepsilon(\sigma \circ \tau) = -\varepsilon(\sigma)$$

Théorème 16. Pour un entier $n \geq 2$, l'application :

$$\begin{array}{ccc} \varepsilon : S_n & \longrightarrow & \{-1; 1\} \\ \sigma & \longmapsto & \varepsilon(\sigma) \end{array}$$

est un morphisme de groupes surjectif.

Ici l'ensemble $\{-1; 1\}$ est vu comme sous-groupe de $(\mathbb{Q}^*, \times)$

Définition 19. Une permutation $\sigma \in S_n$ est dite **paire** si $\varepsilon(\sigma) = 1$ et **impaire** si $\varepsilon(\sigma) = -1$

Remarque 21.

1. Toute transposition est une permutation impaire.
2. Une permutation est paire (resp. impaire) si, et seulement si elle est produit d'un nombre pair (resp. impair) de transpositions.
3. Quel que soit $\sigma \in S_n$, le fait que $\varepsilon(\sigma^{-1}) = (\varepsilon(\sigma))^{-1}$ implique que σ et σ^{-1} sont de même parité.
4. Il existe une définition un peu plus classique de la signature par la formule :

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

Cependant, toutes les définitions possibles de la signature d'une permutation sont équivalentes dans la mesure où on peut montrer qu'il n'existe qu'un seul morphisme surjectif de S_n dans $(\{-1; 1\}; \times)$ tel que $\varepsilon(\tau) = -1$ pour toute transposition τ .

Exemple 11.

1. On reprend la permutation $\sigma \in S_6$ considérée plus haut.
 - Il y a 3 σ -orbites distinctes, donc $\varepsilon(\sigma) = (-1)^{6-3} = -1$.
 La permutation σ est impaire.
 - La décomposition canonique de σ est $\sigma = (1, 5, 3)(4, 6)$, donc $\varepsilon(\sigma) = (-1)^{3-1} \times (-1) = -1$.
 On retrouve que σ est une permutation impaire.
 - Une décomposition de σ en produit de transpositions est $\sigma = (1, 5)(1, 3)(1, 5)$, donc $\varepsilon(\sigma) = (-1)^3 = -1$.
 On retrouve encore que σ est une permutation impaire.

$$2. \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 6 & 8 & 1 & 7 & 3 \end{pmatrix} \in S_8$$

Les σ -orbites sont :

$$\Omega_\sigma(1) = \{1, 4, 6\} ; \Omega_\sigma(2) = \{2\} ; \Omega_\sigma(3) = \{3, 5, 8\} ; \Omega_\sigma(7) = \{7\}$$

Il y a 4 σ -orbites, donc $\varepsilon(\sigma) = (-1)^{8-4} = (-1)^4 = 1$.
 σ est une permutation paire.

3.2.5 Groupe alterné

Etant donné un groupe symétrique S_n , on désigne par $\mathcal{A}_n$ l'ensemble des permutations paires de S_n :

$$\mathcal{A}_n = \{\sigma \in S_n, \varepsilon(\sigma) = 1\}$$

$\mathcal{A}_1 = S_1 = \{e\}$, et pour $n \geq 2$, $\mathcal{A}_n$ est le noyau du morphisme ε .

Cela montre que $\mathcal{A}_n$ est un sous-groupe de S_n .

De plus :

$$(\mathcal{A}_n = \text{Ker } \varepsilon \text{ et } \varepsilon \text{ surjectif}) \Rightarrow \frac{S_n}{\mathcal{A}_n} \simeq \{-1; 1\}$$

Ainsi,

Proposition 19.

Pour tout $(n \geq 2)$, l'ensemble $\mathcal{A}_n$ des permutations paires de S_n forme un sous-groupe de S_n d'ordre $\frac{n!}{2}$.

On l'appelle le groupe alterné de degré n .

Remarque 22.

Pour $(n \geq 2)$, les deux classes de S_n modulo $\mathcal{A}_n$ sont

$\mathcal{A}_n$ et $\tau\mathcal{A}_n = \{\tau \circ \sigma, \sigma \in \mathcal{A}_n\}$ où τ est une transposition quelconque de S_n .

Attention, $\tau\mathcal{A}_n = \mathcal{A}_n\tau$ est l'ensemble des permutation impaires de S_n et ce n'est PAS un sous-groupe de S_n .

3.3 Groupes diédraux

On considère le plan affine euclidien (c'est à dire muni du produit scalaire standard) $\mathcal{P}$. On rappelle que :

- Une isométrie du plan est une application f de $\mathcal{P}$ qui conserve le produit scalaire, et donc les distances :

$$\forall x, y \in \mathcal{P}, \langle f(x), f(y) \rangle = \langle x, y \rangle$$

- L'ensemble des isométries du plan forme un sous-groupe de $S_{\mathcal{P}}$ (groupe symétrique de $\mathcal{P}$) noté $Is(2)$.

Pour $n \geq 2$, on considère un polygone régulier à n sommets dans le plan $\mathcal{P}$. Sans perte de généralités, on considèrera le polygone régulier à n sommets centré en $O(0;0)$ dont $A(1;0)$ est un sommet, noté P_n .

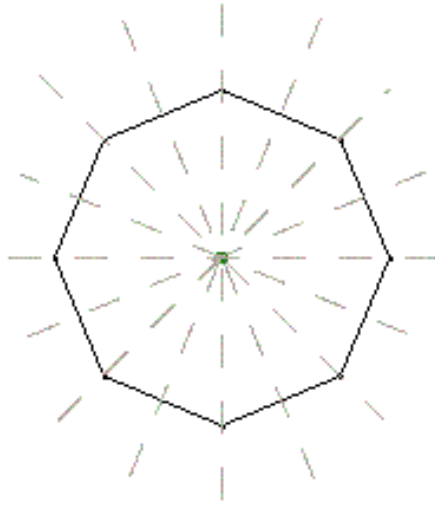
Définition 20.

Le groupe diédral $\mathbb{D}_n, (n \geq 2)$ est le groupe des isométries du plan euclidien qui préserve le polygone régulier P_n , c'est à dire qui préserve globalement l'ensemble de ses sommets.

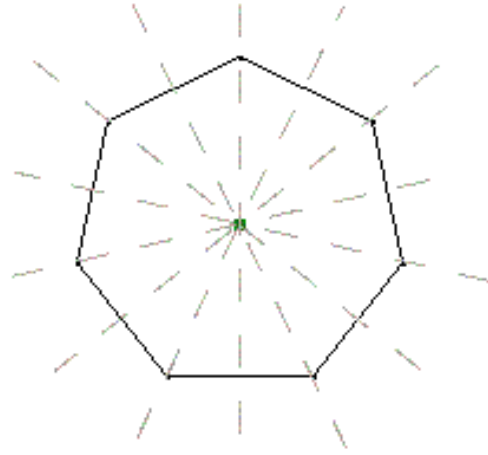
Proposition 20.

Pour tout $n \geq 2$, le groupe diédral $\mathbb{D}_n$ est fini d'ordre $2n$.

Il est composé de n rotations et n symétries.



Groupe diédral : cas n pair



Groupe diédral : cas n impair

Voici quelques résultats classiques importants, que l'on se propose de démontrer en exercices.

Proposition 21.

1. En notant r la rotation d'angle $\frac{2\pi}{n}$, et s la symétrie d'axe (Ox) , on a : Le groupe $\mathbb{D}_n$ est engendré par r et s . Plus précisément :

$$\mathbb{D}_n = \{id, r, r^2, \dots, r^{n-1}, s, r \circ s, \dots, r^{n-1} \circ s\} = \{id, r, r^2, \dots, r^{n-1}, s, s \circ r, \dots, s \circ r^{n-1}\}$$

2. L'ensemble des n rotations de $\mathbb{D}_n$ forme un sous-groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Proposition 22.

Pour $n = 2$, $\mathbb{D}_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est abélien.

Pour $n \geq 3$, $\mathbb{D}_n$ est non abélien.

Remarque 23.

Les groupes $\mathbb{D}_4$ et Q_8 sont tous deux non abéliens d'ordre 8. Ce sont d'ailleurs les seuls.

Mais ils ne sont pas isomorphes. En effet $\mathbb{D}_4$ possède 5 éléments d'ordre 2 alors que Q_8 n'en possède qu'un seul.

Chapitre 4

Sous-groupes normaux

On a vu au chapitre 2 que, G étant un groupe, les seules relations d'équivalence $\mathcal{R}$ faisant hériter l'ensemble quotient de la structure de groupe de G , sont celles qui sont compatibles avec la loi de G .

Et, on rappelle qu'une relation d'équivalence sur G est compatible avec la loi de G si, et seulement si elle est compatible à droite, et à gauche avec cette loi.

De plus, si $\mathcal{R}$ est une telle relation d'équivalence, il existe un sous-groupe H de G tel que $\mathcal{R} = \mathcal{R}_H =_H \mathcal{R}$.

Or, on a vu que si G est un groupe non abélien et H un sous-groupe quelconque, on a en général $\mathcal{R}_H \neq_H \mathcal{R}$.

En dehors des deux cas importants où soit G est abélien, soit H est le noyau d'un morphisme, il est donc important de savoir reconnaître les sous-groupes H tels que $\mathcal{R}_H =_H \mathcal{R}$.

4.1 Notion de sous-groupes normal, groupe quotient

Définition 21.

Dans un groupe G , un sous-groupe H est dit **normal** ou **distingué** si

$\mathcal{R}_H =_H \mathcal{R}$.

Dit autrement, cela signifie que, pour tout $x \in G$, $xHx^{-1} = H$.

On notera alors $H \triangleleft G$.

Remarque 24.

G étant un groupe,

1. Le groupe trivial $\{e\}$ et le groupe G sont des sous-groupes distingués.
2. Dans un groupe abélien, tout sous-groupe est distingué.
3. Si $H \triangleleft G$, on écrit : $x \equiv y \pmod{H}$ c'est à dire " x équivalent à y module H " au lieu de $x\mathcal{R}_Hy$ (ou $x_H\mathcal{R}y$).

L'ensemble quotient $(\frac{G}{H})_d = (\frac{G}{H})_g$ est un groupe noté $\frac{G}{H}$: le groupe quotient de G par le groupe normal H .

4. H est un sous-groupe distingué de G si, et seulement si, H est stable par tout automorphisme intérieur de G .
5. On a rappelé que le noyau d'un morphisme de groupes est un sous-groupe distingué. Réciproquement, tout sous-groupe distingué H dans un groupe G est le noyau de la surjection canonique : $\pi : G \longrightarrow \frac{G}{H}$

$$x \longmapsto \bar{x}$$

Théorème 17. Dans un groupe G , on a $H \triangleleft G$ si, et seulement si, il existe un groupe G' et un morphisme $f : G \longrightarrow G'$ tel que $H = \text{Ker } f$.

Exemple 12.

Voici quelques exemples importants de sous-groupes distingués.

1. $\mathbb{Z}$ étant commutatif, les sous-groupes $n\mathbb{Z}$ sont distingués, pour tout $n \in \mathbb{Z} : n\mathbb{Z} \triangleleft \mathbb{Z}$.
2. Le sous-groupe $\text{Int}(G)$ des automorphismes intérieurs d'un groupe G est distingué dans $\text{Aut}(G) : \text{Int}(G) \triangleleft \text{Aut}(G)$.
3. Pour tout $n \geq 2$, le groupe alterné A_n , comme noyau du "morphisme signature", est un sous-groupe distingué du groupe symétrique $S_n : A_n \triangleleft S_n$.
4. Si E est un espace vectoriel de dimension finie sur un corps commutatif K , le groupe spécial linéaire $SL(E)$, comme noyau du "morphisme déterminant", est distingué dans le groupe linéaire $GL(E) : SL(E) \triangleleft GL(E)$.
5. Dans le groupe diédral $\mathcal{D}_n$, le sous-groupe des rotations est distingué : $\Gamma_n \triangleleft \mathcal{D}_n$.
6. Dans un espace vectoriel euclidien E de dimension finie, le groupe des isométries positives est distingué dans le groupe orthogonal : $O^+(E) \triangleleft O(E)$.
7. Si G est un groupe, son centre $Z(G) = \{g \in G, gh = hg \forall h \in G\}$ est distingué : $Z(G) \triangleleft G$.

Définition 22. Un groupe G est dit simple s'il ne possède pas de sous-groupes distingués non triviaux.

Nous verrons en exercices d'importants exemples de (familles de) groupes simples.

4.2 Quelques propriétés

4.2.1 Morphismes et sous-groupes normaux

Proposition 23.

Soit G un groupe et $\{H_i\}_{i \in I}$ une famille de sous-groupes de G , alors :

$$(H_i \triangleleft G, \forall i \in I) \Rightarrow \bigcap_{i \in I} H_i \triangleleft G$$

Proposition 24.

Soit deux groupes G et G' et $f \in \text{Hom}(G, G')$, alors :

- a) $H \triangleleft G \Rightarrow f(H) \triangleleft f(G)$. De plus si f est surjectif, $f(H) \triangleleft G'$
- b) $H' \triangleleft G' \Rightarrow f^{-1}(H') \triangleleft G$

Proposition 25.

Soit deux groupes H et K deux sous-groupes d'un groupe G , alors :

- a) $H \triangleleft G \Rightarrow H \cap K \triangleleft K$
- b) $H \triangleleft G \Rightarrow HK$ sous-groupe de G et $H \triangleleft HK$

4.2.2 Classes de conjugaison, normalisateurs

Soit G un groupe. À tout élément $g \in G$, on peut associer l'automorphisme intérieur de G , $x \mapsto y = gxg^{-1}$

Nous dirons alors que y est conjugué à x par g .

On rappelle que la relation " y est un conjugué de x " est une relation d'équivalence sur G .

Définition 23.

Les classes selon cette relation d'équivalence sont appelées classes de conjugaison dans G . Deux éléments de G faisant partie de la même classe de conjugaison sont dits conjugués.

Définition 24.

Soit G un groupe, $x \in G$, et A une partie de G .

- a) Le centralisateur de x dans G , noté $C_G(x)$ est l'ensemble des éléments de G qui commutent avec x .

Autrement dit c'est l'ensemble des éléments de G stables par la conjugaison par x .

- b) Le centralisateur de A dans G est l'ensemble des éléments de G qui commutent avec tous les éléments de A .

Remarque 25.

- a) $C_G(x)$, comme ensemble des points fixes de l'automorphisme "conjugaison par x ", est un sous-groupe de G .

- b) $C_G(A)$ est l'intersection des centralisateurs des éléments de A .

C'est donc également un sous-groupe de G .

c) $C_G(G)$, le centralisateur, dans G , de G lui même, n'est rien d'autre que le centre de G , que l'on a noté $Z(G)$.

Définition 25.

Considérons un groupe G et H un de ses sous-groupes.

L'ensemble formé par les éléments g de G tels que $gHg^{-1} = H$ est appelé le normalisateur de H dans G et on le note $N_G(H)$.

$N_G(H)$ est un sous-groupe de G , c'est l'ensemble des éléments de G laissant H globalement stable par conjugaison.

Remarque 26.

a) Il est clair que $N_G(H)$ contient H . On peut en fait montrer que c'est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

b) $N_G(H)$ contient $C_G(H)$ et donc à fortiori contient $Z(G)$.

Théorème 18.

Soit G un groupe et H un sous-groupe de G .

Le centralisateur $C_G(H)$ de H dans G est un sous-groupe distingué du normalisateur $N_G(H)$ de H dans G et le quotient $N_G(H)/C_G(H)$ est isomorphe à un sous-groupe de $\text{Aut}(H)$.

4.3 2^e et 3^e théorème d'isomorphisme

Théorème 19. 2^e théorème d'isomorphisme

Soit G un groupe, H un sous-groupe distingué de G

et K un sous-groupe de G . Alors :

- *L'ensemble $HK = \{hk, k \in K, h \in H\}$ est un sous-groupe de G .*
- *Le groupe quotient HK/H est isomorphe au groupe quotient $K/(K \cap H)$.*

Théorème 20. 3^e théorème d'isomorphisme

Soit G un groupe, H et K deux sous-groupes distingués de G tels que $K \subset H$.

Alors le groupe quotient H/K s'identifie à un sous-groupe distingué du groupe quotient G/K .

De plus, on a $G/H \simeq (G/K)/(H/K)$.

Chapitre 5

Action de groupe

5.1 Notion de groupe opérant sur un ensemble

Définition 26. Soit $(G, *)$ un groupe et X un ensemble. Une action (ou opération) de G sur X est une application :

$$\begin{aligned}\psi : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g.x\end{aligned}$$

telle que :

a) $\forall x \in X, e.x = x$

b) $\forall g, g' \in G$ et $x \in X, g.(g'.x) = (g * g').x$

On dit alors que G opère (à gauche) sur X .

Proposition 26.

À toute action de G sur X est associée un morphisme de groupe :

$$\begin{aligned}\rho : G &\longrightarrow \text{Bij}(X) \\ g &\longmapsto \rho_g : x \mapsto g.x = \psi(g, x)\end{aligned}$$

Réciproquement, un morphisme de groupe $\rho : G \longrightarrow \text{Bij}(X)$ définit une action du groupe G sur X par :

$$\begin{aligned}\psi : G \times X &\longrightarrow X \\ (g, x) &\longmapsto \rho(g)(x)\end{aligned}$$

Un tel morphisme $\rho : G \longrightarrow \text{Bij}(X)$ s'appelle une représentation du groupe G sur l'ensemble X .

Remarque 27.

Notons que si G agit sur X , alors G agit sur l'ensemble des applications de X dans un ensemble Y par $g.f = f \circ \psi(g^{-1})$,

et il agit sur l'ensemble des applications de Y vers X par $g.f = \psi(g) \circ f$.

5.2 Orbite. Stabilisateur

Dans toute cette partie on considère un groupe $(G, *)$, un ensemble X et une action $\psi : G \times X \longrightarrow X$ de G sur X .

Définition 27.

On appelle orbite de $x \in X$ sous l'action de G l'ensemble :

$$\text{Orb}(x) = \psi(G \times \{x\}) = \{g.x, g \in G\} \subset X.$$

Proposition 27.

Les orbites forment une partition de l'ensemble X .

Elles sont les classes d'équivalence de la relation :

$$x \sim x' \leftrightarrow \exists g \in G, x' = g.x$$

Exemple 13.

Si $X = \mathbb{R}^2$ sur lequel on fait agir naturellement son groupe orthogonal $G = O_2(\mathbb{R})$, les orbites sont les cercles centrés en l'origine.

Définition 28.

On dit que :

1. G opère transitivement sur X si :

$$\forall x, x' \in X, \exists g \in G, x' = g.x$$

Dit autrement cela signifie qu'il n'y a qu'une seule orbite sous l'action de G .

2. G opère fidèlement sur X si :

$$(\forall x \in X, g.x = x) \Rightarrow g = e$$

Dit autrement cela signifie que le morphisme ρ est injectif.

Exemple 14.

Si $(G, *)$ est un groupe, X un ensemble et $\psi : G \times X \longrightarrow X$ une action :

- a) G agit transitivement sur chacune des orbites.
- b) $G/\text{Ker}(\rho)$ agit fidèlement sur X .

Définition 29.

On appelle stabilisateur de $x \in X$ sous l'action de G l'ensemble :

$$\text{Stab}(x) = \{g \in G, g.x = x\} \subset G.$$

Proposition 28.

1. Pour tout $x \in X$, $\text{Stab}(x)$ est un sous-groupe de G .

2. Si x et x' appartiennent à la même orbite, alors $Stab(x)$ et $Stab(x')$ sont conjugués dans G .

Plus précisément :

$$\forall (g, x) \in (G \times X), Stab(g.x) = g * Stab(x) * g^{-1} = i_g(Stab(x))$$

3. $Ker(\rho) = \bigcap_{x \in X} Stab(x)$

5.3 Exemples

1. Commençons par quelques "actions naturelles" :
 - a) Si X est un ensemble, le groupe $G = Bij(X)$ agit évidemment sur X .
 - b) Le groupe $GL_n(k)$ agit sur k^n où k est un corps.
 - c) Le groupe $O_n(k)$ agit sur la sphère de dimension n (ensemble des vecteurs unitaires de k^n).

Dans ces trois cas, le morphisme ρ de la Proposition est le morphisme identité.

2. Tout groupe G agit sur lui même (c'est à dire que $X = G$) de différentes manières, dont voici 3 exemples :

- a) Action par translation à gauche :

$$\begin{aligned} \psi_g : G \times G &\longrightarrow G \\ (g, x) &\longmapsto g.x = g * x \end{aligned}$$

Attention, $(g, x) \longmapsto x * g$ n'est PAS une action à gauche.

- b) Action par translation à droite :

$$\begin{aligned} \psi_d : G \times G &\longrightarrow G \\ (g, x) &\longmapsto g.x = x * g^{-1} \end{aligned}$$

Pour ces deux exemples on a :

$Orb(x) = G$ donc les actions par translation à gauche et à droite de G sur lui même sont transitives.

En fait elles sont même simplement transitives, c'est à dire que :

$$\forall x, x' \in X, \exists ! g \in G, x' = g.x.$$

$Stab(x) = \{e\}$, $\forall x \in X$, donc leur intersection est également réduite à l'élément neutre, et ces deux actions sont fidèles.

On en déduit... le théorème de Cayley !

- c) Action par automorphismes intérieurs (ou par conjugaison) :

$$\begin{aligned} \psi : G \times G &\longrightarrow G \\ (g, x) &\longmapsto g.x = g * x * g^{-1} \end{aligned}$$

Ici, $\forall g \in G, \rho(g) = i_g$.

Les orbites sont exactement les classes de conjugaison.

Cette action n'est pas transitive car on a par exemple $\text{Orb}(e) = \{e\}$.

Si G est commutatif, on a même $\text{Orb}(x) = \{x\}, \forall x \in X$.

Pour tout $x \in G$,

$$\text{Stab}(x) = \{g \in G, g * x * g^{-1} = x\} = \{g \in G, g * x = x * g\}$$

Dit autrement, le stabilisateur d'un élément $x \in G$ est formé de l'ensemble des éléments du groupe qui commutent avec l'élément x , c'est à dire $\text{Stab}(x) = C_G(x)$, que l'on a appelé... le centralisateur de x !

Ainsi, $Z(G) = \bigcap_{x \in G} \text{Stab}(x)$ et l'action est fidèle si, et seulement si $Z(G) = \{e\}$.

5.4 Formule des classes

5.5 Points fixes d'un G-ensemble

Chapitre 6

Groupes finis

6.1 Théorèmes de Sylow

6.2 Quelques applications

Chapitre 7

Groupes linéaires et sous-groupes

Chapitre 8

Isométries et déplacements d'un espace affine euclidien