Université de Rennes 1

THGR

THÉORIE DES GROUPES

Définitions élémentaires, classifications des groupes abéliens de type fini, étude des groupes diédraux, sous-groupes normaux et quotients, actions de groupes, groupe symétrie et études particulières, produit direct et semi-direct, théorèmes de Sylow, études de quelques groupes.

Auteur
Frédéric Touzet

Notes de cours
Victor Lecerf

2021–2022

Table des matières

Chapitre 1

Notions de base

1.1 Groupes

Définition 1.1.1. *Un groupe est la donnée d'un couple $(G, *)$ où est G est un ensemble, et $*$ est une loi de composition interne sur G associative, vérifiant l'existence d'un élément neutre, et telle que chaque élément de G possède un inverse dans G. $(G, *)$ est dit* ***abélien*** *lorsque la loi est commutative.*

Remarques.

- Puisque $*$ est associative, l'expression $x^n = \prod_{i=1}^{n} x$ est bien définie.
- L'élément neutre est unique. On le note 0 lorsque la loi est notée additivement (notamment lorsque le groupe est abélien), et 1 lorsque la loi est notée multiplicativement. Si le cadre est général, on notera e_G l'élément neutre d'un groupe G.
- Chaque élément de G possède un unique inverse. De la même manière qu'au point précédent, l'inverse de x peut-être notée $-x$ ou x^{-1} en fonction de la notation de la loi [1].
- Par abus de notation, on confond $(G, *)$ et G.

1.2 Morphismes de groupes

Définition 1.2.1. *Soit $(G, *)$ et $(H, \triangle)$ deux groupes. On appelle morphisme de groupes toute application $\varphi : G \longrightarrow H$ telle que :*

$$\forall x, y \in G,\ \varphi(x * y) = \varphi(x) \triangle \varphi(y).$$

φ est un isomorphisme lorsque c'est de plus une bijection. Si $(G, *) = (H, \triangle)$, on parle d'endomorphisme. Si ces deux conditions sont réunies, c'est un automorphisme.

Notations. L'ensemble des automorphisme d'un groupe G est aussi un groupe lorsqu'il est muni de la composition. On le note $\mathrm{Aut}(G)$.

1. Certains auteurs préfèrent parler de symétrique, et le note $\mathrm{Sym}(x)$.

Proposition 1.2.1. *Soit $(G, *)$ et $(H, \triangle)$ deux groupes, et un morphisme de groupes $\varphi : G \longrightarrow H$. Alors :*

(i) $\varphi(e_G) = e_H$.

(ii) Si φ est un isomorphisme, φ^{-1} en est de même.

Définition 1.2.2. *Deux groupes sont dits **isomorphes** s'il existe un isomorphisme entre ces deux groupes.*

Remarque. La notion d'isomorphisme est la pierre angulaire de la théorie des groupes. En effet, l'étude principal des groupes est de se demander quelles sont les structures possibles de groupes que l'on peut induire sur un ensemble. Savoir que deux groupes sont isomorphes, c'est dire qu'ils ont la même structure, et que les noms qu'on donne aux éléments de l'un ne sont que des étiquettes sur les éléments de l'autre.

1.3 Sous-groupes

1.3.1 Définition

Définition 1.3.1. *Soit $(G, *)$ un groupe. On appelle sous-groupe de G tout ensemble non vide $H \subset G$ telle que la restriction de la loi de G à H^2 confère à H une structure de groupe. On notera $H < G$. Un sous-groupe H est dit **propre** si $H \neq G$.*

Proposition 1.3.1. *Soit $H \subset G$. H est un sous-groupe de G si et seulement si :*

(i) $e_G \in H$.

(ii) $\forall x, y \in G,\ xy^{-1} \in H$.

1.3.2 Sous-groupes remarquables

Définition 1.3.2. *Soit G et H des groupes, et $f : G \longrightarrow H$ un morphisme de groupes. On appelle noyau de f l'ensemble*

$$\ker(f) = f^{-1}\big(\{e_H\}\big)$$

Et image l'ensemble :

$$\mathrm{Im}(f) = f(G)$$

Remarque. Ces deux ensembles sont particuliers du point de vue des structures de groupes. Ils permettent de caractériser beaucoup de phénomènes et propriétés.

Proposition 1.3.2. *Soit G_1 et G_2 des groupes, $H_1 < G_1$ et $H_2 < G_2$ des sous-groupes. Soit $\varphi : G_1 \longrightarrow G_2$ un morphisme de groupes. Alors :*

(i) $\varphi(H_1)$ est un sous-groupe de G_2.

(ii) $\varphi^{-1}(H_2)$ est un sous-groupe de G_1.

Remarque. En particulier, le noyau et l'image sont tous des sous-groupes.

1.4 Sous-groupe engendré par une partie

1.4.1 Construction

Proposition 1.4.1. *Soit G un groupe. Une intersection quelconque de sous-groupes de G est un sous-groupe de G.*

Remarque. Une union de sous-groupes n'est *quasiment jamais* un sous-groupe. En effet, si G est un groupe et H_1 et H_2 en sont des sous-groupes, alors $H_1 \cup H_2$ est un groupe *si et seulement si* l'un est inclus dans l'autre.

Définition 1.4.1. *Soit G un groupe, A une partie de G. On appelle $\langle A \rangle$ le plus petit sous-groupe de G contenant A, et*

$$\langle A \rangle = \bigcap_{H<G,\, A\subset H} H.$$

Définition 1.4.2. *Une partie A de G est dite génératrice si $\langle A \rangle = G$. Un groupe est dit de type fini s'il admet une partie génératrice finie.*

Exercice. Montrer que $(\mathbb{Q}, +)$ n'est pas de type fini.

1.4.2 Groupes de types finis remarquables

Définition 1.4.3. *Soit G un groupe. S'il existe $x \in G$ tel que $G = \langle x \rangle$, on dit que G est* ***monogène*** *et :*

$$G = \{x^n \,|\, n \in \mathbb{N}\}$$

G est alors abélien. S'il est de plus fini, il est dit ***cyclique****.*

Exemples.

— $(\mathbb{Z}, +)$ est monogène car il est engendré par 1.

— Pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est cyclique.

1.5 Ordre d'un groupe

Définition 1.5.1. *Soit G un groupe, et $x \in G$. On appelle ordre de G son cardinal noté $|G| \in \mathbb{N} \cup \{\infty\}$. On appelle ordre de x la quantité*

$$\mathrm{Ord}(x) = \big|\langle x \rangle\big|.$$

Remarque. Si $x \in G$ est d'ordre fini, $\mathrm{Ord}(x)$ est le plus petit entier n strictement positif tel que $x^n = e_G$.

1.6 Ensembles et quotients

Définition 1.6.1 (Quotient)**.** *Soit X un ensemble et $\sim$ une relation d'équivalence. On appelle quotient de X par la relation $\sim$ l'ensemble des classes d'équivalences des éléments de X par $\sim$. Cet ensemble est noté $X/\sim$.*

Remarque. Soit G est groupe, et H un sous-groupe de G. Soit la relation définie par

$$\forall x, y \in G,\ (x \sim y) \iff (y^{-1}x \in H).$$

C'est une relation d'équivalence. On note ici $G/\sim = G/H$. Nous verrons plus tard qu'il existe dans certains cas un structure naturel sur ce quotient. On note $[G : H] = |G/H|$ son cardinal (appelé *indice de H dans G)*. On peut remarquer des plus que les éléments de G/H sont de la forme gH avec $g \in G$.

Théorème 1.6.1 (Lagrange)**.** *Soit G un groupe fini, et H un sous-groupe de G. Alors,*

$$|G| = [G : H] \cdot |H|.$$

En particulier, l'ordre d'un sous-groupe de G divise $|G|$.

Démonstration. Soit $g \in G$, et $\varphi : H \longrightarrow gH, h \longmapsto gh$. C'est un bijection. Ainsi, toutes les classes d'équivalences ont même cardinal (celui de H). Puisque la relation d'équivalence partitionne G, on a exactement $|G| = [G : H] \cdot |H|$.

□

Corollaire 1.6.1. *Soit G un groupe fini, et $g \in G$. Alors, $\mathrm{Ord}(g)$ divise G. En particulier, $g^{|G|} = e_G$.*

Démonstration. Soit $g \in G$. $\langle g \rangle$ est un sous-groupe de G, donc $\mathrm{Ord}(g)$ divise $|G|$ par le théorème de Lagrange. De plus, cela signifie que $|G|$ est multiple de l'ordre de g, d'où le second résultat.

□

Chapitre 2

Groupes abéliens de type fini

2.1 Groupes monogènes, cycliques

Définition 2.1.1. *Un groupe est dit monogène s'il est généré par un seul élement. Il est dit cyclique s'il est fini*

Si $G = \langle x \rangle$, on a un morphisme surjectif

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & x^n \end{array}$$

C'est un isomorphisme lorsque G est infini. Dans le cas fini et en notant $|G| = n$

$$\begin{array}{rccc} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & x^n \end{array}$$

est aussi un isomorphisme.

Proposition 2.1.1. *Tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ ($n \in \mathbb{N}$), et est donc monogène.*

Démonstration. Soit G sous-groupe de $\mathbb{Z}$, $n = \min G \bigcap \mathbb{N}^*$. Alors tout élément x de G s'écrit par division euclidienne sous la forme $x = qn + r$ avec r compris entre 0 et $n-1$. Mais $r = x - qn \in G$. Par minimalité de n on a nécessairement $r = 0$. La réciproque est évidente.

□

Exercice. Tout sous-groupe de $\mathbb{R}$ est, soit un $n\mathbb{Z}$, soit dense dans $\mathbb{R}$.

Proposition 2.1.2. *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre d diviseur de n. De plus, pour tout $d \in \mathbb{N}$ diviseur de n, il existe $H < \mathbb{Z}/n\mathbb{Z}$ d'ordre d, et $H = \langle \overline{n/d} \rangle$.*

Démonstration. Montrons la première propriété. Soit H un sous-groupe non trivial de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $d > 1$. Soit $\overline{x} \in H$. Puisque $d\overline{x} = 0$, il existe k tel que $x = \frac{pn}{d}$. Ainsi, $H \subset \langle \overline{n/d} \rangle$. De plus, ces deux groupes sont de même ordre, donc égaux. Pour la seconde propriété, ce qui précède montre que pour tout d diviseur de n, $\langle \overline{n/d} \rangle$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et c'est l'unique sous-groupe de tel ordre.

□

Proposition 2.1.3.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \,|\, \mathrm{ord}(x) = n\}$$

Démonstration. Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors x et n sont premiers entre eux. Donc si $k\overline{x} = \overline{0}$ pour un certain $k < n$, n divise nécessairement k en vertu du théorème de Gauss, impliquant $k = 0$. Donc $\overline{x}$ est d'ordre n. Réciproquement, si $\overline{x}$ est un élément d'ordre n, alors x génère $\mathbb{Z}/n\mathbb{Z}$. Donc il existe k entier tel que $k\overline{x} = \overline{1}$. Donc x est inversible.

□

Application : On rappelle que l'indicatrice d'Euler est la fonction φ qui à n associe le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$. Soit $n \in \mathbb{N}^*$. Tout élément de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre diviseur de n. On peut alors partitioner $\mathbb{Z}/n\mathbb{Z}$ en regroupant ses éléments de même ordre. D'où :

$$\sum_{d|n} \varphi(d) = n$$

Théorème 2.1.1. *Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif. Tout sous-groupe fini de $(\mathbb{K}^*, \cdot)$ est cyclique.*

Démonstration. Soit G un tel sous-groupe, et $n = |G|$. On a $\sum_{d|n} \varphi(d) = n$, donc par Lagrange, on a une partition de G :

$$\begin{cases} \forall d|n,\ A_d = \{x \in G \,|\, \mathrm{ord}(x) = d\} \\ G = \bigcup_{d|n} \end{cases}$$

Alors $|G| = \sum_{d|n} \mathrm{card}(A_d)$.

Soit d diviseur de n. Soit A_d est vide, soit il existe dans G un certain élément x d'ordre d, et $\langle x \rangle = (\mathbb{Z}/d\mathbb{Z}, +)$est un groupe de cardinal d. Ainsi, pour tous $y \in \langle x \rangle$, $y^d = 1_{\mathbb{K}}$. De par la structure de corps de $\mathbb{K}$, les y sont les racines du polynôme $X^d - 1$. $A_d \subset \langle x \rangle$ (P admet au plus d racines). De plus, $|A_d| = \varphi(d)$donc son cardinal est 0 ou $\varphi(d)$. En comparant toutes les égalités, trouvées, on trouve exactement que ce cardinal est $\varphi(d)$. En particulier A_n est non vide, donc G est cyclique.

□

2.2 Structure de groupe

Lemme 2.2.1 (chinois)**.** *Soit n et m entiers naturels non nuls, premiers entre eux. Alors :*

$$\mathbb{Z}/(nm)\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Démonstration. Cette démonstration utilise le théorème 4.2.2 que nous verrons au chapitre 4, il existe cependant des démonstrations plus élémentaires. Notons $\overline{x}$ la classe d'équivalence de x dans $\mathbb{Z}/n\mathbb{Z}$, et $\tilde{y}$ celle de y dans $\mathbb{Z}/m\mathbb{Z}$. Posons l'application :

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & x & \longmapsto & (\overline{x}, \tilde{x}) \end{array}$$

f est un morphisme d'anneau, dont le noyau est $\ker f = \{x \in \mathbb{Z} \,|\, n|x \text{ et } m|x\}$. Puisque n et m sont premiers entre eux, $\ker f = \{x \in \mathbb{Z} \,|\, (nm)|x\} = (nm)\mathbb{Z}$. Donc $\mathbb{Z}/(nm)\mathbb{Z}$ est isomorphe

à $f(\mathbb{Z})$. Ainsi $\text{Card}(f(\mathbb{Z})) = \text{Card}\mathbb{Z}/(nm)\mathbb{Z} = nm$, donc $\text{Card}(f(\mathbb{Z})) = \text{Card}\,\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. De plus, le premier étant un sous-groupe de l'autre, ils sont égaux. Donc selon le premier théorème d'isomorphisme, $\mathbb{Z}/(nm)\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

□

Corollaire 2.2.1. *Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, avec les p_i premiers deux à deux distincts, et les $\alpha_i > 0$. Alors :*

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$

Et :

$$\varphi(n) = \prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi p_i^{\alpha_i - 1}(p_i - 1)$$

Démonstration. On vérifie que $\varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i - 1}(p_i - 1)$. Il suffit de se demander combien d'entiers non nuls inférieurs ou égaux à $p_i^{\alpha_i - 1}$ sont premiers avec ce dernier.

□

Théorème 2.2.1. *Soit p premier, et $\alpha \in \mathbb{N}^*$. Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est*

- *cyclique si $p \geq 3$. Il est alors isomorphe à $(\mathbb{Z}/\varphi\left(p^\alpha\right)\mathbb{Z}, +)$.*
- *trivial si $p = 2$ et $\alpha = 1$.*
- *isomorphe à $\mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si $p = 2$ et $\alpha \geq 2$.*

2.3 Description des groupes abéliens de type fini

Dans toute cette partie, $(G, +)$ désigne un groupe abélien de type fini.

Définition 2.3.1. *Soit $\mathscr{F} = (x_1, \ldots, x_k)$ un famille génératrice de G. Cette famille est dite appelée pseudo-base si :*

$$\forall (m_1, \ldots, m_k) \in \mathbb{Z}^k,\ \left(\sum_{i=1}^{k} m_i x_i = 0\right) \Longrightarrow (\forall i \in [\![1, k]\!],\ m_i x_i = 0)$$

Et une base si :

$$\forall (m_1, \ldots, m_k) \in \mathbb{Z}^k,\ \left(\sum_{i=1}^{k} m_i x_i = 0\right) \Longrightarrow (\forall i \in [\![1, k]\!],\ m_i = 0)$$

Définition 2.3.2. *On appelle ensemble des torsions de G, noté $\text{Tor}(G)$, l'ensemble des éléments de G d'ordre fini.*

Exemple. $\mathrm{Tor}(\mathbb{Q}) = \{0_{\mathbb{Q}}\}$.

Lemme 2.3.1. *Soit $(x_1, \ldots, x_k)$ une pseudo-base (resp. une base) de G. Alors il existe des entiers positifs $n_1, \ldots, n_k, r$ (resp. un entier r strictement positif) tel que :*

$$G \cong \left(\prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}\right) \times \mathbb{Z}^r \ (\textit{resp. } G \cong \mathbb{Z}^r)$$

Démonstration. Si $(x_1, \ldots, x_k)$ est une pseudo-base on a un isomorphisme :

$$\prod_{i=1}^{k} \langle x_i \rangle \cong G$$

Induit par le morphisme $(m_1 x_1, \ldots, m_k x_k) \longmapsto \sum_{i=1}^{k} m_i x_i$. De plus, les $\langle x_i \rangle$ sont soit isomorphes à $\mathbb{Z}$, soit cycliques.

Si $(x_1, \ldots, x_k)$ est une base, on a un isomorphisme :

$$\begin{array}{ccc} \mathbb{Z}^k & \longrightarrow & G \\ (m_1, \ldots, m_k) & \longmapsto & \sum_{i=1}^{n} m_i x_i \end{array}$$

□

Théorème 2.3.1. *Tout groupe abélien de type de fini admet une pseudo-base donnée par le théorème précédent.*

$\mathrm{Tor}(G)$ est isomorphe à $\prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ via l'isomorphisme du théorème dans le cas des pseudo-bases. De plus, G est fini *si et seulement si* $\mathrm{Tor}(G) = G$, et Tor(G)=$\{0\}$ *si et seulement si* G est isomorphe à $\mathbb{Z}^r$, *si et seulement si* G admet une base (on dit dans ce cas que G est un groupe libre).

Définition 2.3.3. *L'entier r est appelé rang de G. Cet entier est bien défini car il est unique.*

Pour cela, il suffit en fait de montrer $(\mathbb{Z}^p \cong \mathbb{Z}^r) \implies (p = r)$.

Proposition 2.3.1. *Soit H un sous-groupe de G. Alors, H est un groupe abélien de type fini, et* $\mathrm{rg}(H) \leq \mathrm{rg}(G)$.

Remarque : $\mathrm{rg}(H) = \mathrm{rg}(G)$ n'implique pas nécessairement que $H = G$. Exemple : $\mathbb{Z}$ et $n\mathbb{Z}$ avec $n \geq 2$ sont tous deux de rang 1.

Démonstration. Dans le cas où G est libre, et l'ensemble des torsions est réduit à 0, donc $G \cong \mathbb{Z}^r$. Par récurrence sur r. Pour $r = 1$, l'exemple le montre. Soit $r > 1$, on suppose le résultat acquis aux rangs inférieurs. Soit $H < G$, on considère le morphisme φ de $\mathbb{Z}^r$ dans $\mathbb{Z}$ qui à un élément de $\mathbb{Z}^r$ lui associe sa dernière coordonnée. On remarque d'abord que $\ker(\varphi) = \mathbb{Z}^{r-1}$. Deux cas se présentent :

- Si $H < \ker(\varphi) = \mathbb{Z}^{r-1}$, on conclut par récurrence.

- Sinon, $\varphi(H)$ est un sous-groupe naturel de $\mathbb{Z}$, donc de la forme $\varphi(h_0)\mathbb{Z}$, pour un certain $h_0 \notin \ker\varphi$. Soit $h \in H$, on peut écrire $\varphi(h) = m_0\varphi(h_0)$ (m_0 un entier relatif). Donc $h - m_0h_0 \in \ker\varphi \bigcap H < \mathbb{Z}^{r-1}$, et est donc de la forme $m_1h_1 + \ldots + m_sh_s$ avec $s \leq r-1$. Cela montre que $(h_1, \ldots, h_s)$ est une base de H, qui est donc abélien libre de rang inférieur ou égal à r.

□

2.4 Raffinement, décomposition canonique et décomposition primaire

Dans toute cette partie, $(G, +)$ désigne un groupe abélien de type fini. On a vu que $G \cong \mathrm{Tor}(G) \times \mathbb{Z}^r$, et $\mathrm{Tor}(G) \cong \prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$. Le problème est qu'on n'a pas unicité des n_i en général (en particulier, le lemme chinois fournie de tels exemples).

Théorème 2.4.1 (Admis). *Si G est fini (donc $\mathrm{Tor}(G) = G$), alors :*

1. *Il existe $d_1, \ldots, d_s$ des entiers tels que*

$$G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$$

avec $1 < d_1|d_2|\ldots|d_s$ et $d_1 \cdots d_s = |G|$. (décomposition canonique).

2. *Il existe $p_1, \ldots p_k$ des nombres premiers, et $\alpha_1, \ldots, \alpha_k > 0$ des entiers tels que*

$$G \cong \prod_{i=1}^{s} \mathbb{Z}/n_i\mathbb{Z}$$

où $n_i = p_i^{\alpha_i}$, $\alpha_i > 0$ (décomposition primaire).

Ces décompositions sont uniques (à permutation près des facteurs dans le second cas).

Remarques. Les $d_1, \ldots, d_s$ sont appelés les facteurs invariants de G.

Exemple. Déterminer à isomorphisme près tous les groupes abéliens finis d'ordre 360 *via* la décomposition canonique. On a $360 = 2 \cdot 180 = 2 \cdot 2 \cdot 90 = 6 \cdot 60 = 2 \cdot 6 \cdot 30 = 3 \cdot 120$. Ainsi, un groupe abélien fini d'ordre 360 est isomorphe à l'un des groupes suivants :

— $\mathbb{Z}/360\mathbb{Z}$
— $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$
— $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$
— $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$
— $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$
— $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$

Lemme 2.4.1. *Soit G un groupe abélien de type fini, et $(x_1, \ldots, x_n)$ une famille génératrice de G. Soit $(c_1, \ldots, c_k) \in \mathbb{N}^k$ une famille de PGCD 1. Alors, il existe une famille génératrice $(y_1, \ldots, y_k)$ famille génératrice telle que $y_1 = \sum_{i=1}^{k} c_ix_i$.*

Démonstration du théorème de structure. On montre en fait que tout groupe abélien de type fini possède une base. On raisonne par récurrence sur le nombre minimale de générateurs de G. Pour $k = 1$, c'est évident. Soit $k > 1$, on suppose le résultat acquis au rang $k - 1$. Parmi toutes les familles génératrices à k éléments, il en existe une notée $(x_1, \dots, x_k)$, telle que x_1 soit d'ordre minimal (possiblement infini). Supposons que $\langle x_1 \rangle \cap \langle x_2, \ \cdots, x_k \rangle \neq \{0\}$. Il existe alors une relation $\sum_{i=1}^{k} m_i x_i = 0$ avec $m_1 x_1 \neq 0$. Quitte à modifier les signes de certains x_i, on peut supposer les m_i positifs, et $m_1 < \mathrm{ord}(x)$. Soit $c_i = m_i/(\mathrm{PGCD}(m_1, \dots, m_k))$ par leur PGCD, on peut les supposer premiers entre eux. Alors, il existe une famille génératrice $(y_1, \dots, y_k)$ avec $y_1 = \sum_{i=1}^{k} c_i x_i$. Cependant :

$$dy_1 = \sum_{i=1}^{k} m_i x_i = 0$$

Et d est inférieur à m_1 donc à l'ordre de x_1. C'est absurde. Ainsi $\langle x_1 \rangle \cap \langle x_2, \ \cdots, x_k \rangle \neq \{0\}$, et donc $\langle x_1 \rangle \times \langle x_2, \ \cdots, x_k \rangle \cong G$.

□

Chapitre 3

Le groupe diédral

3.1 Introduction

On note $\mathrm{Iso}(\mathbb{R}^2) = O_2(\mathbb{R})$ le groupe des isométries linéaires sur $\mathbb{R}^2$. Le groupe diédral D_n est le sous-groupe de $\mathrm{Iso}(\mathbb{R}^2)$ défini par :

$$g \in D_n \iff g(\mathbb{U}_n) = \mathbb{U}_n$$

Où $\mathbb{U}_n$ est le groupe des racines n-ièmes de l'unité.

Remarque. Si $S, R \in \mathrm{Iso}(\mathbb{R}^2)$, où S est une symétrie et R est une rotation. Alors $S = S^{-1}$, et $SRS = R^{-1}$. De plus, R s'écrit sous la forme :

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Théorème 3.1.1. *Soit n un entier naturel. Le groupe diédral D_n est d'ordre $2n$. De plus, il est engendré par la symétrie S de conjugaison (d'ordre 2), et la rotation R d'angle $2\pi/n$ (d'ordre n). On a alors :*

$$D_n = \langle R \rangle \cup S\langle R \rangle$$

Démonstration. Soit $f \in D_n$, et $z \in \mathbb{U}_n$. Dans le cas où f est une rotation, alors il existe $k \in \mathbb{Z}$ tel que $R^k(f(z)) = z$.

□

3.2 Caractérisation de D_n $(n \geq 3)$

Théorème 3.2.1. *Soit G un groupe tel que*

i. $G = \langle r, s \rangle$ avec s d'ordre 2 et r d'ordre $n \geq 3$.

ii. $srs = r^{-1}$.

Alors G est isomorphe à D_n. Plus précisément, il existe un isomorphisme ψ envoyant r sur R, et s sur S.

Remarque. Cela permet de s'affranchir de donner un cadre rigoureux à la manipulation d'éléments des groupes diédraux, puisque peu importe la construction choisie, la structure est la même.

Démonstration. L'unicité vient du fait général que : si G_1, G_2 sont deux groupes, et que $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$ sont des familles respectivement de G_1 et G_2. Alors il existe *au plus* un morphisme de $\varphi : G_1 \longrightarrow G_2$ tel que $\varphi(a_i) = b_i$ pour tout i.

Existence : on a $\langle s\rangle = \{1, s\}$, et $\langle r\rangle = \{1, r, \cdots r^{n-1}\}$. On a exactement deux classes à droites modulo $\langle r\rangle$: $\langle r\rangle$ et $\langle r\rangle s$ (on vérifie qu'elles ne sont pas égales car $srs = r^{-1} \neq r$ car $n \geq 3$). On a $\langle r\rangle \cup \langle r\rangle s \subset G$. On montre ensuite que c'est un sous-groupe de G.

□

Exemple. Montrer que D_3 est isomorphe à $\mathfrak{S}_3$.

Corollaire 3.2.1. *Aut(D_n) est en bijection avec l'ensembles des couples de la forme (S', R') avec S' d'ordre 2 et R' d'ordre n.*

Il y a n symétrie S' d'ordre 2, et $\varphi(n)$ rotations engendrant $\langle R\rangle$.

Chapitre 4

Sous-groupes normaux

4.1 Définition

Définition 4.1.1. *Soit G un groupe, et $H < G$. H est dit normal (ou distingué) dans G si pour tous $g \in G$, $h \in H$, $ghg^{-1} \in H$. On note alors $H \triangleleft G$.*

Remarques. Il est équivalent de dire que pour tous $g \in G$, $gH = Hg$: les classes à droite coïncident avec les classes à gauche. Ou encore que H est stable par tous les automorphismes intérieurs de G.

Il est important de remarquer que $\triangleleft$ ne définit *pas* une relation d'équivalence (elle n'est pas transitive). [1]

Exemples.

- Si G est abélien, tous ses sous-groupes sont distingués dans G.
- Si φ est un morphisme entre deux groupes G et H, alors $\ker\varphi$ est distingué dans G.
- Vérifier que $\langle S\rangle = \{1, S\}$ n'est pas normal dans D_n ($n \geq 3$).

Proposition 4.1.1. *Soit H un sous-groupe de G tel que $[G : H] = 2$. Alors $H \triangleleft G$.*

Démonstration. On a deux classes à gauche : H et gH pour un certain $g \in G\backslash H$. Ainsi, $G = H \cup gH$ (union disjointe). On utilise le même argument pour les classes à droite, et on obtient que $gH = Hg$ pour tout $g \in G$.

□

Proposition 4.1.2. *Soit $\varphi : G_1 \longrightarrow G_2$ un morphisme de groupe, et $H_1 < G_1$, $H_2 < G_2$. Alors :*

i. $(H_2 \triangleleft G_2) \Longrightarrow (\varphi^{-1}(H_2) \triangleleft G_1)$.

ii. $(H_1 \triangleleft G_1) \Longrightarrow (\varphi(H_1) \triangleleft \varphi(G_1))$.

En particulier si $H_1 \triangleleft G_1$ et si φ est surjective, $\varphi(H_1) \triangleleft G_2$. Ce n'est pas le cas en général.

Définition 4.1.2. *Un groupe G est dit simple si ses seuls groupes normaux sont $\{e_G\}$ et G.*

1. On peut aller chercher des exemples du côté de chez $\mathfrak{S}_3$.

Exemple. $\mathbb{Z}/p\mathbb{Z}$ est simple *si et seulement si* p est premier.

4.2 Groupes quotients

Théorème 4.2.1. *Soit G un groupe et $H \triangleleft G$. Il existe une unique loi de groupe sur G/H telle que la projection canonique $\pi : G \longrightarrow G/H$ soit un morphisme de groupe.*

Remarque. Si π est un morphisme de groupe, H en est le noyau.

Démonstration. On veut montrer que si $(x, y), (x', y') \in G^2$ vérifient $xH = x'H$ et $yH = y'H$, alors :

$$xyH = x'y'H$$

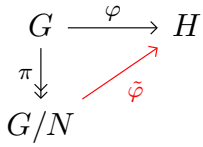
Il suffit alors de montrer que $(x'y')^{-1}xy \in H$. En effet :

$$\begin{aligned}(x'y')^{-1}xy &= y'^{-1}x'^{-1}xy \\ &= y'^{-1}\left(yy^{-1}\right)x'^{-1}xy \\ &= \underbrace{y'^{-1}y}_{\in H}\ \underbrace{\left(y^{-1}\underbrace{x'^{-1}x}_{\in H}y\right)}_{\in H \text{ car } H \text{ est dinstingué}}\end{aligned}$$

□

Théorème 4.2.2 (Propriété universelle du quotient, factorisation)**.** *Soit $\varphi : G \longrightarrow H$ un morphisme de groupe, et $N < \ker\varphi$ distingué dans G. Il existe un unique morphisme de groupe injectif $\tilde{\varphi} : G/N \longrightarrow H$ tel que $\varphi = \tilde{\varphi} \circ \pi$.*

Cela se résume par le diagramme commutatif suivant :



Démonstration. Il suffit de remarquer que les éléments d'une même classe ont même image. On définit alors $\tilde{\varphi} : G/H \longrightarrow H$ qui à une classe associe l'image d'un de ses représentants. En particulier, si $\overline{x} \in G/H$ représenté par un élément $x \in G$ et $\tilde{\varphi}(\overline{x}) = e_H$, cela signifie que x est dans la même classe que e_G puisque φ est un morphisme. D'où $\overline{x} = \overline{e}_G = e_{G/H}$. □

Théorème 4.2.3 (Premier théorème d'isomorphisme)**.** *Soit $\varphi : G \longrightarrow H$ un morphisme de groupe.*

$$G/\ker\varphi \cong \mathrm{Im}(\varphi)$$

Démonstration. Cet isomorphisme est induit par $\tilde{\varphi}$. Puisque $\mathrm{Im}(\varphi) = \mathrm{Im}(\tilde{\varphi})$, alors $\tilde{\varphi} : G/H \longrightarrow \mathrm{Im}(\varphi)$ est un isomorphisme.

□

Proposition 4.2.1. *Soit G un groupe, et $N \triangleleft G$. Soit $\pi : G \longrightarrow G/N$ la projection canonique sur G/N. Alors le mécanisme qui à un sous groupe H de G contenant N associe $\overline{H} = \pi(H)$(ou réciproquement le mécanisme qui à un sous groupe $\overline{H}$ de G/N contenant N associe $\pi^{-1}(\overline{H})$) définit une bijection entre l'ensemble des sous-groupes de G contenant N et l'ensemble des sous-groupes de G/N.*

Remarque. H est normal dans G *si et seulement si* $\overline{H}$ est normal dans G/N.

Proposition 4.2.2. *Soit $\varphi : G_1 \longrightarrow G_2$ un isomorphisme de groupe. Soit $H_1 \triangleleft G_1$, et $H_2 = \varphi(H_1)$ (donc distringué dans G_2). Il existe un isomorphisme $\overline{\varphi}$ tel que :*

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ {\scriptstyle \pi_1}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \pi_2} \\ G_1/H_1 & \xrightarrow[\overline{\varphi}]{} & G_2/H_2 \end{array}$$

Démonstration. Appliquer le théorème de factorisation.

□

Proposition 4.2.3. *Soient G_1, G_2 des groupes, et $H_1 \triangleleft G_1$, $H_2 \triangleleft G_2$ des sous-groupes distingués. Alors $H_1 \times H_2$ est distingué dans $G_1 \times G_2$. De plus, on a l'isomorphisme :*

$$\begin{array}{ccc} G_1/H_1 \times G_2/H_2 & \longrightarrow & (G_1 \times G_2)/(H_1 \times H_2) \\ (x_1 \mod H_1, x_2 \mod H_2) & \longmapsto & (x_1, x_2) \mod H_1 \times H_2 \end{array}$$

Remarque. Le rang d'un groupe abélien de type fini est unique. En effet, $G \cong \mathrm{Tor}(G) \times \mathbb{Z}^r$. Donc :

$$G/\mathrm{Tor}(G) \cong \mathbb{Z}^r$$

Il suffit alors de montrer que $\mathbb{Z}^r \cong \mathbb{Z}^s$ nécessite l'égalité $r = s$. On a :

$$\mathbb{Z}^r/2\mathbb{Z}^r \cong \mathbb{Z}^s/2\mathbb{Z}^s$$

Donc :

$$(\mathbb{Z}/2\mathbb{Z})^r \cong (\mathbb{Z}/2\mathbb{Z})^s$$

D'où $2^r = 2^s$.

Théorème 4.2.4 (Second théorème d'isomorphisme)**.**

4.3 Exemples fondamentaux

4.3.1 Centre d'un groupe

Définition 4.3.1. *Soit G un groupe. On appelle centre de G le sous-groupe abélien distingué dans G :*

$$\mathcal{Z}(G) = \{x \in G \,|\, \forall y \in G,\, xy = yx\}$$

Remarques.

- On peut encore définir le centre de G par $\mathcal{Z}(G) = \ker(\mathrm{Int}(G))$, où $\mathrm{Int}(G)$ est le sous-groupe des automorphismes intérieurs de G.
- $\mathcal{Z}(G)$ est aussi un sous-groupe caractéristique de G : il est invariant par tous les automorphismes de G.

Exercices.

- Déterminer le centre du groupe diédral d'ordre $n \in \mathbb{N}^*$ (traiter le cas n pair ou impair).
- Soit G un groupe. Montrer que $\mathrm{Int}(G) \triangleleft \mathrm{Aut}(G)$. Le quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$ est appelé groupe des automorphismes extérieurs.

4.3.2 Groupe dérivé

Définition 4.3.2. *Soit G un groupe, et $x, y \in G$. On appelle commutateur de x et y la quantité $[x, y] = xyx^{-1}y^{-1}$.*

Remarque. x et y commutent *si et seulement si* $[x, y] = e_G$.

Définition 4.3.3. *Soit G un groupe. On appelle groupe dérivé de G le sous-groupe de G engendré par les commutateurs, noté $D(G)$. Il est distingué dans G.*

- G est abélien *si et seulement si* $D(G) = e_G$ *si et seulement si* $\mathcal{Z}(G) = G$.
- $D(G)$ est aussi un sous-groupe caractéristique de G.

Proposition 4.3.1. *Soit G un groupe, H un groupe abélien, et $\varphi : G \longrightarrow H$ un morphisme. Alors :*

i. $G^{ab} = G/D(G)$ est abélien.

ii. Il existe un unique morphisme $\overline{\varphi} : G^{ab} \longrightarrow H$ tel que $\varphi = \overline{\varphi} \circ \pi$ (où $\pi : G \longrightarrow G^{ab}$ est la projection canonique).

Remarque. G^{ab} est appelé *abélianisé* de G. C'est le plus grand quotient abélien de G.

Chapitre 5

Actions de groupes

5.1 Vocabulaire et notations

Définition 5.1.1. *Soit X un ensemble, et G un groupe. Une action de G sur X est la donnée d'une application :*

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

Remarques.

- De manière équivalente, une action de groupe est la donnée d'un morphisme $\rho : G \longrightarrow \mathfrak{S}_X$. En reprenant la notation de la définition, $g \cdot x = \rho(g)(x)$.
- On dit que G *opère* sur X, et l'on note $G \curvearrowright X$.

Exemple. $\mathfrak{S}_n$ opère sur $[\![1, n]\!]$ *via* l'identité.

Définition 5.1.2 (Orbite, stabilisateur)**.** *Soit G un groupe opérant sur un ensemble X. Soit $x \in X$. On appelle orbite de x l'ensemble :*

$$G \cdot x = \{g \cdot x \,|\, g \in G\}$$

On appelle stabilisateur de x l'ensemble :

$$G_x = \{g \in G \,|\, g \cdot x = x\}$$

Proposition 5.1.1. *Soit G un groupe opérant sur l'ensemble X.*

i. $\forall g \in G$, $G_{g \cdot x} = g G_x g^{-1}$

ii. Soit $x \in X$. L'application $\alpha : G/G_x \longrightarrow G \cdot x$, $gG_x \longmapsto g \cdot x$ est bien définie, et est une bijection.

iii. Soit $\mathcal{R}$ la relation définie sur X par $x \mathcal{R} y \iff \exists g \in G,\, y = g \cdot x \iff y \in G \cdot x$. C'est une relation d'équivalence, et les orbites partitionnent alors X.

Démonstration. (i) Soit $h \in G$. On a les équivalences suivantes :

$$h \cdot (g \cdot x) = g \cdot x \iff (g^{-1}hg) \cdot x = x \iff g^{-1}hg \in G_x \iff h \in g G_x g^{-1}$$

(ii) Soient $g, h \in G$. Alors $gG_x = hG_x$ *si et seulement si* il existe $g' \in G_x$, tel que $h = gg'$. Dans ce cas, $h \cdot x = (gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x$. Montrons seulement que α est injective (la surjectivité est évidente). Soient $h, g \in G$ tels que $h \cdot x = g \cdot x$. Alors $h^{-1}g \in G_x$, *i.e* que $hG_x = gG_x$.

(iii) Exercice.

□

Définition 5.1.3. *On dit que G opère transitivement (ou que l'action de G est transitive) si X est une orbite,* i.e *:*

$$\forall x, y \in X,\ \exists g \in G,\ y = g \cdot x$$

On dit que G opère fidèlement si $\rho : G \longrightarrow \mathfrak{S}_X$ est injectif.

Exemple. D_n opère transitivement sur $[\![1, n]\!]$.

5.2 Exemples

5.2.1 Action naturelle d'un groupe sur lui-même

Soit G un groupe. Alors G opère sur lui même via le morphisme définit par $\rho(g) : x \longmapsto gx$. On a alors pour tous $x \in G$: $G_x = \{e_G\}$ et $G \cdot x = G$. On en déduit que G opère fidèlement et transitivement sur lui-même. Or, on sait que

$$\ker(\rho) = \bigcap_{x \in G} G_x.$$

On en déduit $G \cong \rho(G) < \mathfrak{S}(G)$. Il existe un sous-groupe de $\mathfrak{S}(G)$ isomorphe à G.

Théorème 5.2.1 (Théorème de Cayley)**.** *Soit G un groupe d'ordre $n \in \mathbb{N}^*$. Alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

5.2.2 Action par conjugaison

Soit G. un groupe. G agit sur lui-même via le morphisme ρ définit par $\rho(g) : x \longmapsto gxg^{-1}$. Pour $x \in G$, l'orbite de x est exactement sa classe de conjugaison, et son stabilisateur est exactement le centralisateur de x dans G.

5.2.3 Actions sur les classes à gauche

Soit $H < G$. Alors $G/H = \{xH \,|\, x \in G\}$. On a une action par translation à gauche :

$$\forall g, x \in G,\ g \cdot (xH) = (gx)H$$

C'est une action transitive, et $G_H = H$. Plus généralement, $G_{gH} = gHg^{-1}$.

5.2.4 Actions sur les sous-groupes

G opère sur X, l'ensemble des sous-groupes de G, par conjugaison, $g \cdot H = gHg^{-1}$.

5.3 Équations aux classes

Théorème 5.3.1. *Soit G un groupe opérant sur un ensemble X. Les orbites sous cette action partitionnent X. De plus, $|G\cdot x| = |G/G_x| = [G : G_x]$. Soit $(x_1, \cdots, x_m)$ un système de représentants des orbites. On a alors :*

$$|X| = \sum_{i=1}^{m} |G \cdot x_i| = \sum_{i=1}^{m} [G : G_{x_i}]$$

Si de plus, on met d'une part les orbites de plus d'un élément, on a :

$$|X| = \left|X^G\right| + \sum_{\substack{i=1 \\ G_{x_i} \neq G}}^{m} [G : G_{x_i}]$$

Avec $\left|X^G\right| = \{x \in X \,|\, \forall g \in G,\, g \cdot x = x\}$

Remarque. Dans le cas où G est un groupe fini, G opère sur lui même ($X = G$) par conjugaison, et on a donc $\left|X^G\right| = \mathcal{Z}(G)$, et $C_G(x)$ (le centralisateur de x).

Définition 5.3.1. *Soit G un groupe, et p un nombre premier. On dit que G est un p-groupe s'il existe $n \in \mathbb{N}^*$ tel que $|G| = p^n$.*

Corollaire 5.3.1. *Si G est un p-groupe opérant sur un ensemble X, alors :*

$$\left|X^G\right| = |X| \mod p$$

Démonstration. Si H est un sous-groupe stricte de G alors $[G : H] = p^r$ pour un certain $r \in [\![0, n-1]\!]$, d'où le résultat.

□

Dans le cas particulier où G agit sur lui-même *via* la conjugaison, on obtient le corollaire suivant :

Corollaire 5.3.2. *Si G est un p-groupe, alors $|\mathcal{Z}(G)| = |G| \mod p$, et donc $|\mathcal{Z}(G)| = p^r$ pour un certain $r \in [\![1, n]\!]$.*

On peut alors utiliser les résultats sur les actions de groupes pour s'intéresser à des résultats de classification. Par exemple, un p-groupe n'est jamais simple puisque $|\mathcal{Z}(G)| \triangleleft G$. Nous allons montrer un second résultat, on montre pour cela un lemme.

Lemme 5.3.1. *Soit G un groupe tel que $G/\mathcal{Z}(G)$ soit monogène. Alors G est abélien.*

Démonstration. On considère la projection canonique $\pi : G \longrightarrow G/\mathcal{Z}(G)$. Soit $z \in G$ tel que $\pi(z)$ engendre $G/\mathcal{Z}(G)$. On a alors :

$$G/\mathcal{Z}(G) = \{z^m \mathcal{Z}(G) \,|\, m \in \mathbb{Z}\}$$

Soient $x, y \in G$, il existe m_1 et m_2 des entiers relatifs, et $u, v \in \mathcal{Z}(G)$ tels que $x = z^{m_1}u$ et $y = z^{m_2}v$. En utilisant les propriétés de chaque élément mis en jeu, on trouve que $[x, y] = 1$. D'où G est abélien.

□

Proposition 5.3.1. *Soit G un groupe d'ordre p^2 pour un certain nombre premier p. Alors G est abélien. On peut alors classifier les groupes d'ordres p^2 à isomorphisme près. Soit G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, soit il est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Si $\mathcal{Z}(G)$ est d'ordre p^2, alors G est égale à son centre et donc commutatif. Si $|\mathcal{Z}(G)|$ est d'ordre p, alors $|G/\mathcal{Z}(G)|$ est d'ordre p premier (soit un élément de G est d'ordre 1, soit il est d'ordre p). Donc $G/\mathcal{Z}(G)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On conclut alors par le lemme, et le théorème de classification des groupes abéliens d'ordre fini.

□

Théorème 5.3.2 (Cauchy)**.** *Soit G un groupe fini, et p un diviseur premier de $|G|$. Il existe dans G un élément d'ordre p.*

Corollaire 5.3.3. *Soit G un groupe d'ordre $2p$ pour $p \geq 3$ un nombre premier. G est alors isomorphe à $\mathbb{Z}/2p\mathbb{Z}$, ou à D_p*

Démonstration. Selon le théorème de Cauchy, il existe $x \in G$ un élément d'ordre 2, et $y \in G$ un élément d'ordre p. $G/\langle y\rangle$ est d'ordre 2, $\langle y\rangle$ est donc distingué (et même isomorphe à $\mathbb{Z}/p\mathbb{Z}$). On sait par ailleurs que $x \notin \langle y\rangle$ car 2 et p sont premiers entre eux. Cela signifie que $G = \langle y\rangle \sqcup x\langle y\rangle$. En particulier, $G = \langle x, y\rangle$. De plus xy^-1 est une puissance de y puisque $\langle y\rangle$ est distingué dans G. On a alors deux cas :

1. Si $xyx^{-1} = y$, alors x et y commutent, donc G est abélien puisque ce sont les générateurs de G. On a nécessairement $G \cong \mathbb{Z}/2\mathbb{Z} \times \times\mathbb{Z}/p\mathbb{Z} =\cong \mathbb{Z}/2p\mathbb{Z}$ grâce à la décomposition canonique, puis au théorème chinois.
2. Si $xyx^{-1} = y^j$ avec $j \notin p\mathbb{Z}$. Alors $(xyx^{-1})^j = y^{j^2}$, donc $xy^jx^{-1} = x(xyx^{-1})x^{-1} = y$ car x est d'ordre 2. On en déduit que $j^2 = 1 \mod p$, donc $j = \pm 1 \mod p$, et donc que $\overline{j}^2 - \overline{1} = \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, cette équation a deux solutions : 1 et -1. La première solution est exclue par nos étude de cas, donc $j = -1$. Donc G suit la caractérisation de D_p.

□

Chapitre 6

Le groupe symétrique

On rappelle que pour $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ est le groupe des permutations de $[\![1, n]\!]$, muni de la composition. C'est un groupe d'ordre $n!$. On peut noter une permutation de la manière suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

6.1 Signature d'une permutation

Définition 6.1.1 (Signature)**.** *Soit $\sigma \in \mathfrak{S}_n$. On appelle signature de σ la quantité :*

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

$\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$ est un morphisme de groupe surjectif.

Montrons que la signature est bien à valeur dans $-1, 1$, et que c'est un morphisme. Soit $\sigma \in \mathfrak{S}_n$, on a :

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

Pour $i, j \in [\![1, n]\!]$ avec $i < j$, on pose $\sigma(i) = k$ et $\sigma(j) = l$. Il apparait alors une fois et une seule fois dans les indices au dénominateur, soit un terme $l - k$ si $k < l$, soit un terme $k - l$ si $l < k$. En réarrangeant les termes, on peut alors transformer le produit en un produit de 1 et de -1.

Soit maintenant $\sigma, \tau \in \mathfrak{S}_n$. On a :

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

Soit i, j deux entiers entre 1 et n. Puisque

$$\frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}$$

Et qu'on a toujours $\tau(i) < \tau(j)$ ou $\tau(j) < \tau(i)$, alors par un changement de variable :

$$\frac{\varepsilon(\sigma\tau)}{\varepsilon(\tau)} = \prod_{1 \leq k < l \leq n} \frac{\sigma(l) - \sigma(k)}{l - k}$$

Qui vaut exactement $\varepsilon(\sigma)$.

Remarques.

— On appelle $\mathfrak{A}_n$ le noyau de ε, un sous-groupe distingué dans $\mathfrak{S}_n$.

— En fait, la signature est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\{-1, 1\}$.

6.2 Décomposition en produit de cycle

Définition 6.2.1. *Soit $\sigma \in S_n$. On note* $\mathrm{Fix}(\sigma)$ *l'ensemble des points fixes de σ, et on appelle $supp(\sigma) = \mathfrak{S}_n \setminus \mathrm{Fix}(\sigma)$ le support de σ.*

Ces deux ensembles sont stables par σ.

Définition 6.2.2. *Un k-cycle est une permutation σ de de support $\{a_1, \dots, a_k\}$ de cardinal k, avec $\sigma(a_i) = a_{i+1}$ (si $1 \leq i \leq k-1$), et $\sigma(a_k) = a_1$. On note alors $\sigma = (a_1\, a_2\, \dots\, a_k)$.*

Remarques. Soit $\sigma \in \mathfrak{S}_n$.

(i) Si σ est un k-cycle, alors σ est d'ordre k.

(ii) Si σ est une transposition, elle est de signature -1.

(iii) $\sigma(a_1\, a_2\, \dots\, a_k)\sigma^{-1} = (\sigma(a_1)\, \sigma(a_2)\, \dots\, \sigma(a_k))$

(iv) $(a_1\, a_2\, \dots\, a_k) = (a_1\, a_2)(a_2 a_3) \cdots (a_{k-2}\, a_{k-1})(a_{k-1}\, a_k)$.

(v) En déduire que $\varepsilon(a_1\, a_2\, \dots\, a_k) = (-1)^{k-1}$.

Lemme 6.2.1. *Soient $\sigma, \tau \in S_n$ de supports disjoints. Alors $\sigma\tau = \tau\sigma$, et $supp(\sigma\tau) = supp(\sigma) \sqcup supp(\tau)$.*

Théorème 6.2.1 (Décomposition en produit de cycles)**.** *Toute permutation σ non triviale de $\mathfrak{S}_n$ s'écrit comme un produit de cycles de longueurs supérieures à 2, de supports deux à deux disjoints. Si on note $l_1, \dots, l_m$ les longueurs des cycles dans la décomposition, alors* $\mathrm{Ord}(\sigma) = \mathrm{ppcm}(l_1, \dots, l_m)$

Démonstration. Notons $l = \mathrm{ppcm}(l_1, \dots, l_m)$. On a clairement $\sigma^l = \mathrm{id}_{[\![1,n]\!]}$,

□

Corollaire 6.2.1. *On a les résultats suivants :*

(i) Les cycles génèrent $\mathfrak{S}_n$.

(ii) Les transpositions génèrent $\mathfrak{S}_n$.

(iii) Les 3-cycles génèrent $\mathfrak{A}_n$.

Considérons l'action suivante : soit $\sigma \in S_n$, $G = \langle\sigma\rangle$, et $X = [\![1, n]\!]$. On fait opérer G sur X avec $\sigma \cdot i = \sigma(i)$. Pour $1 \leq j \leq n$, on note $K_j = |G \cdot j|$. On a alors :

$$G \cdot j = \{j, \sigma(j), \dots, \sigma^{K_j - 1}(j)\}$$

L'action de σ sur $G \cdot j$ coïncidient avec celle du cycle $c_j = \big(j, \sigma(j), \dots, \sigma^{K_j-1}(j)\big)$. Notons que $supp(c_j) = G \cdot j$. De plus :

$$c_j = c_{j'} \iff j' \in G \cdot j$$

Dans le cas contraire, $supp(c_j)$ et $supp(c'_j)$ sont disjoints. Soient $j_1, \dots, j_m$ des représentants des orbites. On obtient que $\sigma = c_{j_1} \cdots c_{j_m}$. De plus :

$$|G \cdot j| = 1 \iff c_j = \mathrm{id}_{[\![1,n]\!]}$$

On peut supposer par ailleurs que C_{j_m} est de longueur supérieure à 2. Réciproquement, si $\sigma = c_1 \cdots c_{m'}$, on vérifie que les $supp(c_i)$ sont les orbites de longueurs supérieures à 2.

Théorème 6.2.2. *Soient $\sigma_1, \sigma_2 \in \mathfrak{S}_n$. σ_1 et σ_2 sont conjuguées dans $\mathfrak{S}_n$ si et seulement si pour tout $k \in \mathbb{N}^*$, σ_1 et σ_2 admettent le même nombre de k-cycles dans leurs décompositions.*

Démonstration. $\boxed{\Longrightarrow}$ On rappelle que si $c = (a_1 \cdots a_k)$, alors $\sigma c \sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k))$ pour $\sigma \in \mathfrak{S}_n$. Deux cycles conjugués ont donc même support et même longueur. Notons $\sigma_1 = c_1 \cdots c_m$, et $l(c_i)$ la longueur du cycle c_i, avec les c_i à supports deux à deux disjoints. Alors pour toute permutation $\sigma \in \mathfrak{S}_n$, et $i \in [\![1, m]\!]$. Puisque les longueurs des cycles et les supports des permutations sont invariants par conjugaison, on en conclut que les supports sont encore disjoints. Puisque les cycles sont tous de mêmes longueurs, il y a donc autant de longueur donnée qu'avant la conjugaison.

$\boxed{\Longleftarrow}$ On écrit $\sigma_1 = c_1 \cdots c_m$ et $\sigma_2 = d_1 \cdots d_m$, avec $l(c_i) = l(d_i)$ et $supp(c_i) = supp(d_i)$ pour tout indice i. Il existe donc pour chaque i un τ_i tel que $d_i = \tau_i c_i \tau^{-1}$. Les τ_i sont à supports disjoints puisqu'ils ont même supports que les c_i et les d_i. On pose alors $\sigma = \tau_1 \cdots \tau_m$, qui convient.

□

Corollaire 6.2.2. *Le nombre de classe de conjugaison dans $\mathfrak{S}_n$ est donné par $p(n)$, le nombre de partitions de n.*

Remarque. On peut alors reformuler le théorème précédent : σ_1 et σ_2 sont conjuguées dans $\mathfrak{S}_n$ *si et seulement si* $\langle \sigma_1 \rangle$ et $\langle \sigma_2 \rangle$ ont même nombres d'orbites de longueur k pour tout $k \in [\![1, n]\!]$.

Lien entre partitions et groupes abéliens finis. Soit $n = \prod_{i=1}^m p_i^{\alpha_i}$ un entier écrit dans décomposition en facteurs premiers. Soit G un groupe abélien d'ordre n, on applique la décomposition canonique à la décomposition primaire :

$$G \cong \prod_{i=1}^{m} \left(\prod_{j=1}^{l_i} \mathbb{Z}/p^{m_{i,j}}\mathbb{Z} \right)$$

Où $\sum_{j=1}^{l_i} m_{i,j} = \alpha_i$, et les m_i, j sont rangés dans l'ordre croissant suivant j. Le nombre de classes d'isomorphismes d'un groupe abélien d'ordre $n = \prod_{i=1}^m p(\alpha_i)$.

6.3 Le groupe alterné

6.3.1 Résultats généraux

On rappelle que $\mathfrak{A}_n = \ker \varepsilon$. C'est donc un sous-groupe distingué de $\mathfrak{S}_n$. La signature étant un morphisme surjectif lorsque $n \geq 2$, on a $|\mathfrak{A}_n| = n!/2$ pour $n \geq 2$ (selon le théorème de Lagrange).

Proposition 6.3.1. *$\mathfrak{A}_n$ est engendré par les 3-cycles. De plus, pour $n \geq 5$, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

Démonstration. Le premier résultat a déjà été démontré. Pour σ_1, σ_2 des 3-cycles, on sait qu'il existe $\sigma \in \mathfrak{S}_n$ telles que $\sigma_2 = \sigma\sigma_1\sigma^{-1}$. Si $\sigma \in \mathfrak{A}_n$ le résultat est démontré. Sinon, on écrit $\sigma_1 = (a\,b\,c)$. Il existe alors une transposition $\tau = (a_1\,a_2)$ telle que $\{a_1, a_2\} \cap \{a, b, c\} = \varnothing$ (c'est possible car $n \geq 5$). Alors $\tau\sigma_1\tau^{-1} = \sigma$. D'où :

$$\sigma_2 = \underbrace{(\sigma\tau)}_{\in\mathfrak{A}_n}\sigma_1(\sigma\tau)^{-1}$$

□

6.3.2 Centre et groupe diédral

Proposition 6.3.2. *Soit $n \in \mathbb{N}^*$. On a :*

(i) $\mathcal{Z}(\mathfrak{S}_n) = \{\mathrm{id}_{[\![1,n]\!]}\}$ *si* $n \geq 3$.
(ii) $\mathcal{Z}(\mathfrak{A}_n) = \{\mathrm{id}_{[\![1,n]\!]}\}$ *si* $n \geq 4$.
(iii) $D(\mathfrak{S}_n) = \mathfrak{A}_n$ *si* $n \geq 1$.
(iv) $D(\mathfrak{A}_n) = \mathfrak{A}_n$ *si* $n \geq 5$.

Remarques.

— Si $n = 1$, $\mathfrak{S}_1 = \mathfrak{A}_1 = \{\mathrm{id}_{\{1\}}\}$.
— Si $n = 2$, $\mathfrak{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$.
— Si $n = 3$, $\mathfrak{A}_3 = \langle(1\,2\,3)\rangle \cong \mathbb{Z}/3\mathbb{Z}$, donc $\mathcal{Z}(\mathfrak{A}_3) = \mathfrak{A}_3$.

Démonstration. (i) Soit $n \geq 3$. Soit σ une permutation différente de l'identité, et soit $i \in [\![1, n]\!]$ tel que $\sigma(i) \neq i$. Soit $j \in [\![1, n]\!]\backslash\{i, \sigma(i)\}$. Soit $\tau = (\sigma(i)\,j)$. Alors $\sigma(\tau(i)) = \sigma(i)$ et $\tau(\sigma(i)) = j$. Ainsi, σ et τ ne commutent.

(ii) Soit $n \geq 4$. Avec la même quantification et en supposant $\sigma \in \mathfrak{A}_n$, on pose cette fois $\tau = (\sigma(i)\,j\,k)$, où $j, k \notin \{i, \sigma(i)\}$. Encore une fois, σ et τ ne commutent pas.

(iii) Soit $n \geq 1$. $D(\mathfrak{S}_n)$ est un sous-groupe de $\mathfrak{A}_n$ car pour toutes permutations σ et τ, on a $\epsilon([\sigma, \tau]) = [\epsilon(\sigma), \epsilon(\tau)] = 1$. On suppose $n \geq 3$ (on a traité les autres cas dans la remarque). Soit $c = (a\,b\,c)$ un trois cycle. On a alors $c^2 = (a\,c\,b)$, donc c et c^2 sont conjugués par un $\sigma \in \mathfrak{S}_n$, donc $c = [\sigma, c]$, et alors $c \in D(\mathfrak{S}_n)$. Pour $n \neq 5$, on peut prendre $\sigma \in \mathfrak{A}_n$, on a alors $c \in D(\mathfrak{A}_n)$. Le résultat est démontré car les 3-cycles engendrent $\mathfrak{A}_n$.

□

6.3.3 Calcul de $D(\mathfrak{A}_4)$

Soit $V_4 = \{\mathrm{id}_{[\![1,4]\!]}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. On vérifie aisément que c'est un sous-groupe de $\mathfrak{S}_4$, et que c'est un sous-ensemble de $\mathfrak{A}_4$. Remarquons par ailleurs que V_4 est constitué des involutions de $\mathfrak{A}_4$. Cela signifie donc que V_4 est un groupe commutatif (il l'était de toute manière puisque qu'il est de cardinal 4). Selon la classification des groupes d'ordre 4, il est isormorphe au groupe de Klein d'ordre 4, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. V_4 contient deux classes de conjugaison, et est donc distingué dans $\mathfrak{S}_4$. De plus :

Proposition 6.3.3. *V_4 est caractéristique dans $\mathfrak{A}_4$.*

Démonstration. Soit $\varphi \in \mathrm{Aut}(\mathfrak{A}_4)$. Les éléments de V_4 sont exactement les éléments $s \in \mathfrak{A}_4$ vérifiant $s^2 = \mathrm{id}_{[\![1,4]\!]}$. Or, pour tout $s \in V_4$, $\varphi(s)^2 = \varphi(s^2) = \mathrm{id}_{[\![1,4]\!]}$, donc $\varphi(V_4) \subset V_4$.

□

On peut désormais déduire le groupe dérivé de $\mathfrak{A}_4$.

Théorème 6.3.1. *Le groupe dérivé de $\mathfrak{A}_4$ est V_4.*

Démonstration. Le groupe quotient $\mathfrak{A}_4/V_4$ est d'ordre 3, donc nécessairement commutatif. Il est donc contenu dans l'abélianisé de $\mathfrak{A}_4$. Donc $D(\mathfrak{A}_4) < V_4$. Enfin, pour déduire l'égalité, on remarque par exemple que :

$$(1\,2)(3\,4) = [(1\,2\,3), (1\,2\,4)]$$

□

6.4 Simplicité

Définition 6.4.1. *Soit G un groupe. G est dit simple si ses seuls sous-groupes distingués sont triviaux ($\{e_G\}$ et G).*

Théorème 6.4.1 (Galois)**.** *Soit $n \geq 5$. $\mathfrak{A}_n$ est simple.*

Démonstration. Montrons d'abord le résultat suivant : si a et b sont deux éléments de $\mathfrak{A}_5$ d'ordre 5 alors b est conjugué dans $\mathfrak{A}_5$ à a ou à a^2. Notons $a = (a_1\, a_2 \ldots a_5)$ et $b = (b_1\, b_2 \ldots b_5)$, on a alors $a^2 = (a_1\, a_3\, a_5\, a_2\, a_4)$. Soit $\sigma = (a_2\, a_3\, a_5\, a_4)$ le 4-cycle conjuguant a et a^2. Si on suppose que a et b ne sont pas conjugués dans $\mathfrak{A}_n$, alors ils sont conjugués par un permutation τ de signature -1. On a alors $a^2 = \sigma a \sigma^{-1}$ et $a = \tau b \tau^{-1}$, donc $\sigma\tau$ est une permutation de signature 1 conjuguant a^2 et b. Montrons maintenant le résultat principal.

- Pour $n = 5$. $\mathfrak{A}_5$ est un groupe d'ordre 60, en particulier il contient :
  - — L'élément neutre.
  - — 15 éléments d'ordre 2 (les éléments d'ordre 2 sont des produits de deux transpositions disjointes : cela revient à choisir 2 éléments parmi 5, puis 2 parmi 3, soit 30 possibilités que l'on divise par 2 pour s'affranchir de l'ordre de multplication).
  - — 20 éléments 3-cycles.
  - — 24 éléments d'ordre 5 (pour choisir un 5-cycles, il suffit de choisir l'image de 1, puis l'image de $\sigma(1)$, ... , ce qui donne 4! possibilités (puisqu'on ne peut pas envoyer 1 sur lui-même).

  Ce qui nous donne bien un total de 60 éléments. On sait que les 3-cycles sont conjugués dans $\mathfrak{A}_n$, il en est de même pour les produits de deux transpositions (la démonstration est la même que pour les 3-cycles et consiste à exhiber la conjugaison). Soit maintenant H un sous-groupe distingué dans $\mathfrak{A}_5$, qu'on suppose non-trivial. Si H contient un élément d'ordre 2 (*resp.* 3), il les contient tous par ce qui précède (car H est stable par conjugaison dans $\mathfrak{A}_n$). Si H contient un élément a d'ordre 5, il contient aussi a^2, mais tout autre élément de $\mathfrak{A}_5$ d'ordre 5 est conjugué à a ou a^2 dans $\mathfrak{A}_5$, donc H contient tous les autres éléments de $\mathfrak{A}_5$ d'ordre 5.

Or, H ne peut pas contenir qu'un seul de ces trois types d'éléments (en effet $16 = 15 + 1$, $21 = 20 + 1$, et $25 = 24 + 1$ ne divisent pas 60). Donc H est au minimum d'ordre $36 = 20 + 15 + 1$, il est donc d'ordre 60 et $H = \mathfrak{A}_5$.

- Soit $n > 5$. On pose $E = [\![1, n]\!]$. Soit $H \triangleleft \mathfrak{A}_n$, et $H \neq \{\mathrm{id}_E\}$. Soit $\sigma \in H$, $\sigma \neq \mathrm{id}_E$. On souhaite en fait se ramener au cas $n = 5$. Soit $\tau \in \mathfrak{A}_n$, et $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$. Si l'on écrit $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$, alors on voit que $\rho \in H$. Mais en écrivant $\rho = \tau(\sigma\tau^{-1}\sigma^{-1})$, on voit que si τ a des points fixes, alors ρ aussi. Plus précisément : $\sigma \neq \mathrm{id}_E$, donc il existe $a \in E$ un point non fixe. On note $b = \sigma(a) \neq a$. Soit $c \in E\backslash\{a, b, \sigma(b)\}$. Soit alors le 3-cycle $\tau = (a\,c\,b)$, on a $\tau^{-1} = (a\,b\,c)$, et soit $\rho = [\tau, \sigma] = (a\,c\,b)(\sigma(a)\,\sigma(b)\,\sigma(c))$. Soit $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$. Puisque $b = \sigma(a)$, on a $\mathrm{Card} F \leq 5$. Enfin, ρ n'est pas l'identité car $\rho(b) = \tau\sigma(b) \neq b$, car $c = \tau^{-1}(b) \neq \sigma(b)$. De plus, on a $\rho(F) = F$ et $\rho_{F\backslash E} = \mathrm{id}_{F\backslash E}$. Quitte à rajouter des éléments, on peut supposer $\mathrm{Card} F = 5$. On va maintenant considérer $\mathfrak{A}(F)$. $\mathfrak{A}(F)$ est clairement isomorphe à $\mathfrak{A}_5$, et se plonge dans $\mathfrak{A}_n$ par l'application :

$$\begin{array}{ccc} \mathfrak{A}_5 & \longrightarrow & \mathfrak{A}_n \\ u & \longmapsto & \overline{u} = \left\{ \begin{array}{rcl} \overline{u}_{|_F} & = & u \\ \overline{u}_{|_{E\backslash F}} & = & \mathrm{id}_{E\backslash F} \end{array} \right. \end{array}$$

Posons $H_0 = \{u \in \mathfrak{A}(F) \,|\, \overline{u} \in H\} = H \cap \mathfrak{A}(F)$. H_0 est clairement distingué dans $\mathfrak{A}(F)$. On sait de plus que $\rho_{|_F} \in H_0$ et $\rho_{|_F} \neq \mathrm{id}_F$. Puisque $\mathfrak{A}(F) \cong \mathfrak{A}_5$ est simple, on voit que $H_0 = \mathfrak{A}(F)$. Soit alors u un 3-cycle de $\mathfrak{A}(F)$. Alors $\overline{u} \in H$ et est un 3-cycle aussi. Or, les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$ et l'engendrent. Puisque H contient un 3-cycle et que c'est un sous-groupe distingué, il va contenir tous les 3-cycles. Donc H contient $\mathfrak{A}_n$. D'où $H = \mathfrak{A}_n$.

□

Corollaire 6.4.1. *Soit $n \geq 5$, et $H \triangleleft \mathfrak{S}_n$. Alors $H \in \big\{\{\mathrm{id}_{[\![1,n]\!]}\}, \mathfrak{A}_n, \mathfrak{S}_n\big\}$.*

Démonstration. Soit $H \triangleleft \mathfrak{S}_n$. Alors $H \cap \mathfrak{A}_n \triangleleft \mathfrak{A}_n$.

- Si $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, alors soit $H = \mathfrak{A}_n$, soit H est un sous-groupe de $\mathfrak{S}_n$ contenant strictement $\mathfrak{A}_n$. Cela signifie que $|H| > n!/2$. En passant aux indices, on a donc que H est d'indice 1 dans $\mathfrak{S}_n$, donc égal à $\mathfrak{S}_n$.
- Si $H \cap \mathfrak{A}_n = \{\mathrm{id}_{[\![1,n]\!]}\}$, alors on a $\ker(\varepsilon_{|_H}) = H \cap \mathfrak{A}_n = \{\mathrm{id}_{[\![1,n]\!]}\}$. Ainsi, $\varepsilon_{|_H}$ s'injecte dans $\{\pm 1\}$. Cela signifie que $|H| \in \{1, 2\}$. Supposons que $H = \{\mathrm{id}_{[\![1,n]\!]}, \sigma\}$, et soit $\tau \in \mathfrak{S}_n$. On sait que $\tau\sigma\tau^{-1} \in H$, et que $\tau\sigma\tau^{-1} \neq \mathrm{id}_{[\![1,n]\!]}$ (sinon on aurait $\sigma = \mathrm{id}_{[\![1,n]\!]}$). Donc $\tau\sigma\tau^{-1} = \sigma$. Cela signifie que σ est central, mais le centre de $\mathfrak{S}_n$ est trivial (cf. 6.3.2), d'où $\sigma = \mathrm{id}_{[\![1,n]\!]}$.

□

Chapitre 7

Produit semi-direct

L'objectif de ce chapitre sera, étant donné un groupe G et N un sous-groupe distingué de G, d'essayer de reconstituer G à partir de la donnée de N et le quotient G/N. En fait, on va chercher des suites exactes.

Définition 7.0.1 (Suite exacte)**.** *Soient N, G, Q des groupes. Une suite exacte est une suite de groupes et de morphismes de groupes de la forme :*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

Où i est un morphisme injectif, p un morphisme surjectif, et $\mathrm{Im}(i) = \ker(p)$. On dit que G est une extension de N par Q.

Les 1 représentent le groupe trivial, qui est l'objet nul dans la catégorie des groupes.

7.1 Produit direct

Proposition 7.1.1. *Soient G_1 et G_2 des groupes. La loi :*

$$\begin{array}{rcl} (N \times Q)^2 & \longrightarrow & N \times Q \\ \big((n,q),(n',q')\big) & \longmapsto & (nn', qq') \end{array}$$

induit une structure de groupe sur $N \times Q$.

Remarque. On peut définir la projection sur Q par $p(n,q) = q$ pour tout $(n,q) \in N \times Q$. On note $\overline{N}$ le noyau de cette projection. $\overline{N}$ est isomorphe à N, et est distingué dans $N \times H$ (comme noyau d'un morphisme). Si l'on pose $i : N \longrightarrow N \times Q$, $n \longmapsto (n, e_Q)$. On a alors la suite exacte :

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} Q \longrightarrow 1$$

Puisque les rôles de N et de Q sont symétriques on obtient une autre suite exacte. On peut aussi noter $\overline{Q}$ le noyau de la projection sur N. Encore une fois, $\overline{Q}$ est un sous-groupe distingué de $N \times Q$, isomorphe à Q.

Proposition 7.1.2 (Caractérisation du produit direct)**.** *Soit G un groupe, et N et Q des groupes distingués dans G tels que $N \cap Q = \{e\}$ et $NQ = G$. Alors l'application :*

$$\begin{array}{rccc} f: & N \times Q & \longrightarrow & G \\ & (n,q) & \longmapsto & nq \end{array}$$

est un isomorphisme.

Démonstration. Montrons d'abord que f est un morphisme. Soit $(n,q) \in N \times Q$, on a $[n,q] = nqn^{-1}q^{-1} \in N \cap Q$ car N et Q sont distingués dans G, donc n et q commutent. Soient $(n_1,q_1),(n_2,q_2) \in N \times Q$. Alors :

$$\begin{aligned} f((n_1,q_1)(n_2,q_2)) &= f(n_1n_2, q_1q_2) \\ &= n_1n_2q_1q_2 \\ &= n_1q_1n_2q_2 \\ &= f(n_1,q_1)f(n_2,q_2) \end{aligned}$$

Soit $(n,q) \in \ker f$. Alors $n = q^{-1}$, donc $n,q \in N \cap Q = \{e\}$. Enfin $\mathrm{Im}(f) = NQ = G$, donc f est un isomorphisme.

□

Remarque. Dans le cas où les groupes sont finis, on peut remplacer la dernière condition par $|G| = |N||H|$.

7.2 Produit semi-direct

Définition 7.2.1. *Soit Q et N deux groupes, et une action $\alpha : Q \longrightarrow \mathrm{Aut}(N)$. On définit la loi $*_\alpha$ sur $N \times Q$ par :*

$$\forall (n_1,q_1),(n_2,q_2) \in N \times Q,\ (n_1,q_1) *_\alpha (n_2,q_2) = (n_1(q_1 \cdot n_2), q_1q_2)$$

Où $q \cdot n = \alpha(q)(n)$. Le couple $(N \times Q, *_\alpha)$ est noté $N \rtimes_\alpha Q$ appelé produit semi-direct de N et Q.

Exemples.

— Si $\alpha : Q \longrightarrow \mathrm{Aut}(N)$ est le morphisme trivial, alors $N \rtimes_\alpha Q = N \times Q$, le produit semi-direct pour l'action triviale par automorphisme est le produit direct.

Si $Q = \mathrm{Aut}(N)$, et α est le morphisme trivial, alors on appelle le produit semi-direct de N et Q par α est appelé produit semi-direct canonique, noté $N \rtimes \mathrm{Aut}(N)$.

Proposition 7.2.1. *Le produit semi-direct $N \rtimes_\alpha Q$ est un groupe.*

Démonstration. L'associativité est calculatoire, le neutre est (e_N, e_Q), et l'inverse d'un élément $(n,q) \in N \times Q$ est $(q^{-1} \cdot n^{-1}, q^{-1})$. On vérifie ce dernier point :

$$\begin{aligned} (n,q) *_\alpha (q^{-1} \cdot n^{-1}, q^{-1}) &= (n(q \cdot (q^{-1} \cdot n^{-1})), qq^{-1}) \\ &= (n\alpha(q)(\alpha(q^{-1})(n^{-1})), e_Q) \\ &= (n\alpha(q)(\alpha(q)^{-1}(n^{-1})), e_Q) \\ &= (nn^{-1}, e_Q) = (e_N, e_Q) \end{aligned}$$

□

Remarques.

— Pour $q \in Q$, l'inverse de (e_N, q) est (e_N, q^{-1}).

— Comme pour le produit direct, on retrouve un résultat analogue à la seconde assertion de la proposition 7.1.1.

— $\forall (n,q) \in N \rtimes_\alpha Q$, $(e_N, q)(n, e_Q)(e_N, q)^{-1} = (q \cdot n, e_Q)$. Cette remarque montre que l'action de Q sur N correspond à l'action de conjugaison lorsque ces derniers sont vus comme des sous-groupes de $N \rtimes Q$.

On retrouve une propriété analogue à la proposition 7.1.2, pour montrer qu'un groupe est produit semi-direct de deux sous-groupes pour l'action de conjugaison.

Proposition 7.2.2. *Soient N et Q des sous-groupes d'un groupe G, avec N distingué dans G. On suppose $N \cap Q = \{e_G\}$ et $NQ = G$. Soit de plus :*

$$\begin{array}{rccc} \alpha : & Q & \longrightarrow & \mathrm{Aut}(N) \\ & q & \longmapsto & (q \cdot n = n \longmapsto nqn^{-1}) \end{array}$$

Alors l'application :

$$\begin{array}{rccc} f : & N \rtimes_\alpha Q & \longrightarrow & G \\ & (n, q) & \longmapsto & nq \end{array}$$

est un isomorphisme de groupe.

Démonstration. L'application f est bijective selon la démonstration de la proposition 7.1.2. De plus :

□

Chapitre 8

Théorèmes de Sylow

8.1 Introduction

L'objectif de ce cours sera d'essayer de classifier des groupes d'ordres supérieurs à 11. Nous connaissons déjà quelques résultats. En l'occurrence, si G est un groupe d'ordre p premier, alors G est cyclique isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Si G d'ordre p^2, alors G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$. Si G est d'ordre $2p$ (avec $p \geq 3$ premier), alors soit G est isomorphe à D_p, soit il est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$. On dispose aussi du théorème de structure des groupes abéliens de type fini (décomposition canonique ou primaire). On peut alors classifier quelques ordres :

— Ordre 2. $\mathbb{Z}/2\mathbb{Z}$.

— Ordre 3. $\mathbb{Z}/3\mathbb{Z}$.

— Ordre 4. $\mathbb{Z}/4\mathbb{Z}$, ou $(\mathbb{Z}/2\mathbb{Z})^2$.

— Ordre 5. $\mathbb{Z}/5\mathbb{Z}$.

— Ordre 6. $\mathbb{Z}/6\mathbb{Z}$, ou D_3.

— Ordre 8. $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (cas abéliens), D_4, ou Q_8 (voir TD).

— Ordre 9. $\mathbb{Z}/9\mathbb{Z}$, ou $(\mathbb{Z}/3\mathbb{Z})^2$.

— Ordre 10. $\mathbb{Z}/10\mathbb{Z}$, ou D_5.

— Ordre 11. $\mathbb{Z}/11\mathbb{Z}$.

— Ordre 12. On arrive enfin à un stade où nos théorèmes ne suffisent plus.

8.2 Un propriété des p-groupes

Soit G un p-groupe, d'ordre p^r ($r > 0$). On rappelle que le centre d'un p-groupe est non-trivial. En conséquence :

Corollaire 8.2.1. *Si $r > 1$, G n'est pas simple.*

Démonstration. Il est toujours vrai que $\mathcal{Z}(G) \triangleleft G$.

□

Proposition 8.2.1. *Soit G un p-groupe d'ordre p^r. Pour tout $s \in [\![0, r]\!]$, il existe un sous-groupe H de G d'ordre p^s. De plus, $H \triangleleft G$ si $s = r - 1$.*

8.3 Théorèmes de Sylow

Définition 8.3.1. *Soit G un groupe fini d'ordre $p^r m$ avec p un nombre premier, r un entier de $\mathbb{N}^*$, m tel que p ne divise pas m. On appelle p-Sylow de G un sous-groupe de G d'ordre p^r. On note $\mathrm{Syl}_p(G)$ l'ensemble des p-Sylow de G, et $s_p(G)$ le cardinal de cet ensemble.*

Théorème 8.3.1 (Sylow I)**.** *Si G est un groupe fini d'ordre $p^r m$, quantifié comme précédemment. Alors, $s_p(G) \geq 1$.*

Exemple. Vérifions ce théorème par exemple sur $G = \mathrm{GL}_n(\mathbb{F}_p)$, avec p un nombre premier. Le cardinal de G est en fait le nombre de bases de $(\mathbb{F}_p)^n$ (en tant que $\mathbb{F}_p$-espace vectoriel). On trouve alors que :

$$|G| = p^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (p^i - 1)$$

Il suffit de remarquer que l'ensemble des matrices triangulaires supérieurs dont les coefficients diagonaux valent 1, est un p-Sylow.

Lemme 8.3.1. *Soit G un groupe fini d'ordre $|G| = p^r m$ avec $p \nmid m$, et soit H un sous-groupe de G. Soit S un p-Sylow de G. Il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Démonstration. On fait opérer G sur G/S par translation à gauche. Soit $aS \in G/S$, le stabilisateur de aS est exactement aSa^{-1}. H opère de même sur G/S par restriction. Le stabilisateur de aS par cette restriction est alors $aSa^{-1} \cap H$. Les $aSa^{-1} \cap H$ sont des p-sous-groupes [1] de H. Il nous suffit alors de montrer que parmi ces groupes, l'un d'entre eux est un p-Sylow de H, ce qui revient à chercher $a \in G$ tel que $|H/(aSa^{-1} \cap H)| \wedge p = 1$. Or, $|H/(aSa^{-1} \cap H)| = \omega(aS)$ (avec $\omega(aS)$ l'orbite de aS). Supposons par l'absurde que toutes ces orbites soient de cardinal divisibles par p. L'équation aux classes indiquerait qu'il en serait de même pour G/S (puisque c'est l'union disjointes de ces orbites). Cela est absurde puisque S est un p-Sylow [2]

□

On démontre maintenant le premier théorème de Sylow.

Démonstration. On note $n = |G|$. Le théorème de Cayley nous permet alors de plonger G dans $\mathfrak{S}_n$. On plonge ensuite $\mathfrak{S}_n$ dans $\mathrm{GL}_n(\mathbb{F}_p)$: si $(e_1, \ldots, e_n)$ désigne la base canonique de $(\mathbb{F}_p)^n$, alors u_σ est défini par $u_\sigma(e_i) = u(e_{\sigma(i)})$ pour tout $i \in [\![1, n]\!]$. Or, l'exemple précédent nous a montré que $\mathrm{GL}_n(\mathbb{F}_p)$ possède un p-Sylow. On a donc réécrit G comme un sous-groupe d'un groupe possédant un p-Sylow. Le lemme précédent nous assure alors que G possède de même un p-Sylow.

□

Corollaire 8.3.1 (Hors-programme)**.** *Si G est un groupe fini d'ordre $p^r m$ tel que $p \nmid m$, alors G contient des sous-groupes d'ordres p^i, pour tout $i \in [\![0, r]\!]$.*

1. Puisque aSa^{-1} est l'image de S par l'automorphisme intérieur $x \longmapsto axa^{-1}$, c'est un groupe dont le cardinal divise celui de S par le premier théorème d'isomorphisme.
2. On aurait $p \mid |G/S| = m$.

Théorème 8.3.2 (Sylow II). *(i) Les p-Sylow de G sont conjugués : si P et Q sont des p-Sylow de G, il existe $g \in G$ tel que $P = gQg^{-1}$.*

(ii) $\mathrm{sp}(G) \equiv 1 \mod p$ *et* $s_p(G)$ *divise* m.

(iii) Tout p-sous-groupe de G est contenu dans un p-Sylow.

Corollaire 8.3.2. *Soit* $P \in \mathrm{Syl}_p(G)$. *Alors :*

$$P \triangleleft G \iff s_p(G) = 1$$

Un p-Sylow de G est distingué si et seulement si c'est l'unique p-Sylow de G.

Démonstration. — On va démontrer (i) et (iii) simultanément. Soit H un p-sous-groupe de G, et S un p-Sylow de G. Le lemme 8.3.1 nous assure qu'il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais H étant un sous-groupe, on a nécessairement $H = aSa^{-1} \cap H$. Ainsi, H est contenu dans le p-Sylow [3] aSa^{-1}. Si H est de plus un p-Sylow, alors $H = aSa^{-1}$.

— Montrons maintenant le point (ii). Soit X l'ensemble des p-Sylow de G, sur lequel on fait opérer G par conjugaison. Si S est un p-Sylow, alors on peut restreindre l'action de G à S, et S opère alors sur X. Le corollaire 5.3.1 nous assure alors que $|X| \equiv |X^S| \mod p$. Montrons alors que $|X^S| = 1$. Si $s \in S$, on a bien sûr $sSs^{-1} = S$, donc $S \in X^S$. Soit T un p-Sylow, supposé normalisé par S, *i.e* :

$$\forall s \in S,\ sTs^{-1} = T.$$

C'est-à-dire dans X^S. Soit alors $N = \mathrm{Vect}(S \cup T)$. N contient S et T, et ce sont des p-Sylow de N. Mais puisque S normalise T, on sait que $T \triangleleft N$, donc $S = T$.

□

Remarque. On peut faire opérer G sur $\mathrm{Syl}_p(G)$ par conjugaison : $g \cdot P = gPg^{-1}$. On rappelle que $N_G(P)$ (normalisateur de P dans G) est le stabilisateur par cette action. Selon le premier point du théorème 8.3.2, cette action est transitive, ainsi :

$$|G| = s_p(G) \cdot |N_G(P)|$$

De plus, deux des p-Sylow de G sont conjugués dans G.

8.4 Exemples et applications : critère de non simplicité

8.4.1 Groupe d'ordre 99

Soit G un groupe fini d'ordre $99 = 3^2 \cdot 11$. Alors $s_p(G)$ divise 11, et $\mathrm{sp}(G) \equiv 1 \mod 3$. Cela signifie donc que $\mathrm{sp}(G)$ vaut exactement 1. G n'a donc qu'un seul 3-Sylow (d'ordre 9), qui est donc distingué dans G. Cela démontre que G n'est pas un groupe simple.

8.4.2 Groupe d'ordre 12

Soit G un groupe fini d'ordre $12 = 2^2 \cdot 3$. Son 2-Sylow sont d'ordre 4 (il n'y en a qu'un), et les 3-Sylow d'ordre 3. On a $s_3(G) \mid 4$, et $s_3(G) \equiv 1 \mod 3$. Donc $s_3(G) \in \{1, 4\}$. On distingue deux cas.

3. C'est un p-Sylow car isomorphe à S.

— $s_3(G) = 1$. Soit N l'unique 3-Sylow, et Q un 2-Sylow. On sait que $N \triangleleft G$ car N est l'unique 3-Sylow. De plus, on a $|N| \wedge |Q| = 3 \wedge 4 = 1$, donc $N \cap Q = \{e_G\}$, et enfin $|N| \cdot |Q| = |G|$. On en déduit que G est le produit semi-direct $G \cong N \rtimes Q$ (pour l'action de conjugaison de Q sur N).

— $s_3(G) = 4$. On note $\mathrm{Syl}_3(G) = \{Q_1, Q_2, Q_3, Q_4\}$. Puisque les Q_i sont d'ordre 3, on a $Q_i \cap Q_j = \{e_G\}$ dès lors que $i \neq j$. Soit

$$A = \left(\bigcup_{i=1}^{4} Q_i \right) \setminus \{e_G\}$$

A contient huit éléments d'ordre 3. Les $12 - 8 = 4$ éléments restants forment l'unique 2-Sylow. Comme précédemment, $G = N \rtimes Q$ (où N est l'unique 2-Sylow, et Q un 3-Sylow).

8.4.3 Description des p-Sylow de $\mathfrak{S}_n$ pour $n \in \{3, 4, 5\}$

Bibliographie

[1] Frédéric Touzet, *Cours de théorie des groupes* (THGR), 2020.
`https://perso.univ-rennes1.fr/frederic.touzet/`

[2] Daniel Perrin, *Cours d'algèbre*, 1996.

[3] James S. Milne, *Group Theory* (`v3.16`), 2020.
`www.jmilne.org/math/`