UNIVERSITE KASDI MERBAH
OUARGLA
Faculte des Mathematiques et des Sciences de la Matière
Département de mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et informatique

Specialite : Mathématiques

Option : Algebre et géuometere

PAR : Souayah Zineb

Sujet

Étude des structures des groupes finis

Devant le jury:

Bahayou M.Amine	M.A.Université KASDI Merbah-Ouargla	Préssident
Boussaid Mohamed	M.A.Université KASDI Merbah-Ouargla	Rapporteur
Ben Moussa M.Tayeb	M.A.Université KASDI Merbah-Ouargla	Examinateur
Gerboussa Yacine	M.A.Université KASDI Merbah-Ouargla	Examinateur

Soutenu publiquement le: 07/10/2020

REMERCIEMENT

En premier lieu je tiens à remercier mon Dieu, notre créateur, pour m'avoir donné la force d'accomplir ce travail.

Je tiens à exprimer toute ma reconnaissance à mon directeur de mémoire, Monsieur Mohamed BOUSSAID. Je le remercie de m'avoir encadré, orienté, aidé et conseillé.

Enfin, je tiens à remercier :

Je remercie sincèrement mes professeurs et l'ensemble des enseignants du département de mathématiques.

Je remercie tous ceux qui m'ont aidé de près ou de loin, et toute ma famille pour leur soutien.

Je vous remercie tous.

DÉDICACES

Je dédie le fruit de mes années d'études à mes très chères parents paix à leur âme, qui m'ont tous donnée, et leur amour et leur sacrifices éternels. À ma deuxième mère Olia.

À mes frères : Abdo, Elhachemi et Nidhal et à mes sœurs : Imane, Hadjar, Khawla et Tartile.

À mon fiancé : Omar Ben khaddoudj.

À toutes mes amies.

À tous mes enseignants.

Table des matières

RÉSUMÉ

L'objectif de ce mémoire est de présenter les premiers résultats de la théorie des groupes qui aident à déterminer la structure des groupes finis (cas abélien, cas des groupes quelconques de petits ordres).
Dans ce travail, nous avons essayé de déterminer à isomorphisme près la structure de quelques groupes finis d'ordre donné n. Nous avons utilisé en particulier les théorèmes de Sylow pour accomplir ce travail.

ABSTRACT

The objective of this thesis is to present the first results in group theory which helps to determine the structure of finite groups (abelian case, and any groups of small orders).
In this work, we have tried to determine up to isomorphism the structure of some finite groups of a given order n. We used in particular Sylow's theorems to accomplish this work.

NOTATION

- $|G|$: ordre du groupe G.
- $[G : H]$: indice du sous groupe H de G.
- Si H est normal dans G, on note $H \lhd G$.
- $\mathsf{stab}(x)$: stabilisateur de x.
- $\mathrm{O}(x)$: orbite de x.
- $\bar{x}$: classe d'équivalence de x.

Introduction générale

La théorie des groupes forme une branche très active et prolifique des mathématiques.
Ce travail a pour but l'étude des structures de groupes finis. Il comprend quatre chapitres :

Chapitre 1.
Nous avons donné certaines notions et définitions essentielles des groupes comme : les théorèmes des isomorphisme, somme directe et produit semi-direct, les groupes cycliques et l'action d'un groupe sur une ensemble.

Chapitre 2.
Nous avons revu un théorème fondamental, sur les groupes abéliens finis, avec sa démonstration. Nous avons déterminé des décompositions en groupes finis : en groupes primaires et en groupes cycliques primaires.

Chapitre 3.
Ce chapitre est consacré aux théorèmes de Sylow qui aident à déterminer la structure d'un groupe fini donné. Nous avons donné quelques exemples et applications de ces théorèmes.

Chapitre 4.
Il est le noyau de ce travail. Nous avons étudié dans cette partie étudie la structure de groupes de petits ordres et nous avons donné quelque exemples : des groupes d'ordre 8, 12, 14 et 15 .

1

Généralités

1.1 Rappels et notions de base

Définition 1.1.1. *(groupe) Soit G un ensemble non vide et $(*)$ une loi de composition interne définie sur G : $(a,b) \mapsto a*b$. On dit que $(G,*)$ est* un groupe *si :*

1. *Pour tous x,y et z de G, $x*(y*z) = (x*y)*z$, ($*$ est associative).*
2. *G possède un élément neutre e pour cette lois : pour tout x de G, $x*e = e*x = x$.*
3. *Tout élément x de G possède un symétrique y de G : $x*y = y*x = e$.*

Exemple 1.1.1.

— $(\mathbb{R}^*,\cdot)$ *est un groupe.*

— $(\mathbb{R},+)$ *est un groupe.*

Définition 1.1.2. *(sous-groupe) soit H une partie d'un groupe G. On dit que H est* **un sous-groupe** *de G si :*

1. *$H \neq \emptyset$.*
2. *$a,b \in H \Rightarrow ab \in H$.*
3. *$a \in H \Rightarrow a^{-1} \in H$.*

Ces trois conditions sont équivalentes à l'unique axiome : $a,b \in H \Rightarrow ab^{-1} \in H$ et $H \neq \emptyset$.
En notation additive, les conditions 2) et 3) deviennent :

- *$a,b \in H \Rightarrow a+b \in H$.*
- *$a \in H \Rightarrow -a \in H$.*

Exemple 1.1.2. *L'ensemble $H = \{z \in \mathbb{C}^*,\ z^n = 1,\ n \in \mathbb{N}\}$ est un sous-groupe de $(\mathbb{C}^*,\cdot)$.*

Définition 1.1.3. *On appel* **ordre** *d'un groupe G, son cardinal.*

Proposition 1.1.1.

1. *Une partie non vide H de $\mathbb{Z}$ est un sous- groupe additif de $\mathbb{Z}$ si et seulement s'il existe un entier $n \geqslant 0$ tel que :*
$$H = n\mathbb{Z} = \{nz; z \in \mathbb{Z}\}.$$
2. *L'intersection d'une famille $(H_i)_{i\in I}$ des sous-groupes d'un groupe G est un sous-groupe de G.*
3. *Soit H un sous-groupe de G et soient x et y deux éléments de G :*
   - $Hx = H$ *si, et seulement si,* $x \in H$,
   - $Hx = Hy$ *si, et seulement si,* $xy^{-1} \in H$,
   - $xH = H$ *si, et seulement si,* $x \in H$,
   - $xH = yH$ *si, et seulement si,* $x^{-1}y \in H$.
4. *Soit H un sous-groupe de G.*
   On note pour tout $g \in G, gH = \{gh,\ h \in H\}$ et $Hg = \{hg,\ h \in H\}$. Dans le cas G est **commutatif**[1], *on a $gH = Hg$.*

Définition 1.1.4. Le centre (ou commutateur) *$Z(G)$ d'un groupe G est la partie de G formée des éléments de G qui commutent avec tout autre élément de G, soit :*
$$Z(G) = \{h \in G,\ \forall g \in G,\ gh = hg\}.$$
Un groupe G est commutatif si, et seulement si, $Z(G) = G$.

Définition 1.1.5. *(***le conjugué***) Soit G un groupe. Deux éléments x, y de G sont conjugués s'il existe $g \in G$ tel que :*
$$y = gxg^{-1}.$$

Proposition 1.1.2.
Deux sous-groupes H et K de G sont conjugués s'il existe $g \in G$ tel que :
$$K = gHg^{-1}.$$

1.2 Sous-groupes distingués et Groupes quotients

Théorème 1.2.1. *Pour tout sous-groupe H de G, la relation R_g définie sur G par :*
$$xR_g y \Leftrightarrow x^{-1}y \in H$$

1. G est commutatif si, et seulement si, pour tout x, y de G, $xy = yx$.

est une relation d'équivalence dont l'ensemble des classes à gauches sera noté

$$(G/H)_g = \{gH,\ g \in G\}.$$

Remarque 1.2.1. *On peut définir, de manière analogue l'ensemble :* $(H/G)_d = \{Hg,\ g \in G\}$ *des classes à droites modulo* H *à partir de la relation d'équivalence :*

$$xR_d y \Leftrightarrow xy^{-1} \in H.$$

La relation d'équivalence R_d *nous fourni une partition de* G*.*

Théorème 1.2.2. *Si* H *est un sous-groupe de* G *; alors l'ensemble des classes à gauche (resp à droite) modulo* H *deux à deux distinctes forme une partition de* G*.*

Proposition 1.2.1.
soit H *un sous-groupe de* G *;il existe une bijection de l'ensemble des classes à droite modulo* H *sur l'ensemble des classes à gauche modulo* H *et*

$$|(G/H)_g| = |(G/H)_d|\ .$$

Définition 1.2.1. *On définit l'indice de* H *dans* G*, et on note* $[G:H]$ *comme le cardinal de* G/H*, i.e*

$$(G:H) = |G/H|$$

Proposition 1.2.2.
Soient H *et* K *deux sous-groupes d'un groupe fini* G *tels que* $H \subset K$ *alors*

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

Proposition 1.2.3.
Soient H *et* K *deux sous-groupes d'un groupe fini* G *, alors*

$$|HK| = |H|.|K|/|H \cap K|$$

Définition 1.2.2. *Un sous-groupe* H *de* G *vérifiant , pour tout* $x \in G, xH = Hx$ *. On dit que alors que* H *est* **un sous-groupe distingué** *dans* G *(***ou normal***) .*

Remarque 1.2.2. *1. Dans le groupe commutatif , tous les sous-groupes sont distingués .*

2. *Soit H est un sous-groupe distingué dans G ; comme $xH = Hx$ pour tout x de G ,* $(G/H)_g = (G/H)_d$ *. Réciproquement , Si* $(G/H)_g = (G/H)_d$ *, alors :* $H \lhd G$
En résumé :

$$H \lhd G \Leftrightarrow (G/H)_g = (G/H)_d.$$

Proposition 1.2.4.

- *Tout sous-groupe d'indice 2 d'un groupe G est distingué dans G .*
- *Pour un sous groupe H d'un groupe G , les assertions suivantes sont équivalentes :*

a) H *est distingué dans* G *,*

b) $\forall x \in G; xH = Hx,$

c) $\forall x \in G; xH \subset Hx,$

d) $\forall x \in G; xHx^{-1} = H,$

e)$\forall x \in G; xHx^{-1} \subset H.$

Exemple 1.2.1. $(R^2, +)$ *est un groupe abélien*
$H = \{(x, x); x \in R\}$
$\overline{(0,0)} \in H$
$R^2/H = \{(x, y) + H; (x, y) \in R^2\}$.
$\overline{(x, y)} = (x, y) + H = \{(x, y) + (\alpha, \alpha)/\alpha \in R\}.$

Homomorphismes

Définition 1.2.3. *Soient G et G' deux groupes, $f : G \to G'$ une application. f est* un homomorphisme *du groupe dans G le groupe G' si pour tout x, y de G :*

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

Si la loi de G' est notée additivement, l'homomorphisme f doit vérifier :

$$f(xy) = f(x) + f(y).$$

Ainsi $x \to \ln x$ vue plus haut est un homomorphisme du groupe multiplicatif $\mathbb{R}_+^*$ dans le groupe additive $\mathbb{R}$.

Exemple 1.2.2. *Considérons l'application $f : \mathbb{R} \to \mathbb{R}_+^*$ définie par :*

$$f(x) = e^x,$$

est un homomorphisme du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{R}_+^*$.

Remarque 1.2.3. *L'application composée $g \circ f$ de deux homomorphismes de groupes, $f : G \to G'$ et $g : G' \to G''$ est un homomorphisme de groupes. En effet,*

$$(g \circ f)(xy) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

Définition 1.2.4. *Soit $f : G \to G'$ un homomorphisme de groupes.* $\mathrm{Im}(f) = \{f(x),\ x \in G\}$ *est appelé* l'image *de f.*

L'image de l'homomorphisme f est un sous-groupe de G' car si $y, z \in \mathrm{Im}(f)$, il existe $a, b \in G$, tels que $y = f(a)$ et $z = f(b)$. On a

$$yz^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \mathrm{Im}(f).$$

L'homomorphisme f est surjectif si, et seulement si, $\mathrm{Im}(f) = G'$.

Définition 1.2.5. *On appelle* noyau *de f le sous-ensemble de G, noté* $\ker(f)$*, défini par :*

$$x \in \ker(f) \Leftrightarrow f(x) = e',$$

(tel que e' est le neutre de G' et e est le neutre de G). C'est-à-dire :

$$\ker(f) = f^{-1}(e') = \{x \in G,\ f(x) = e'\}.$$

Le noyau de f est un sous-groupe distingué de G.
L'homomorphisme $f : G \to G'$ est injectif si, et seulement si, $\ker(f) = \{e\}$.

1.3 Groupes cycliques

Lemme 1.3.1. *Soit G un groupe et soit X un sous-ensemble de G. Alors, il existe un plus petit sous-groupe de G contenant X.*

Démonstration.

— G est un sous-groupe de G contenant X.

— Soit $(S_i)_{i \in I}$ la famille (non vide) des sous-groupes de G contenant X et soit $S = \bigcap (S_i)_{i \in I}$. C'est un sous-groupe de G contenant X. Si T est un sous-groupe de G contenant X, T est l'un des S_i et donc $S \subset T$.

□

Le plus petit sous-groupe d'un groupe G contenant une partie X est appelé *sous-groupe de G engendré par X*. On le note $< X >$ et on dit que X est un système générateur de $< X >$.

Lemme 1.3.2. *Soit X un sous-ensemble d'un groupe G. Alors $< X >$ est l'ensemble des éléments de G de la forme :*

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n},$$

où, pour tout $i = 1, ..., n$, $x_i \in X$, $\alpha_i = 1$ ou $\alpha_i = -1$.

Théorème 1.3.1. *Tout groupe fini d'ordre premier est cyclique.*

Proposition 1.3.1.

— *Soit $G =< a >$ un groupe cyclique. Alors*

$$< a >= \{a^n,\ n \in \mathbb{Z}\} \text{ et en notation additive } < a >= \{na,\ n \in \mathbb{Z}\}.$$

— *Tout groupe cyclique est commutatif puisque :*

$$a^n a^m = a^{n+m} = a^{m+n} = a^m a^n, \text{ pour tout } n, m \in \mathbb{Z}.$$

— *Tout groupe fini d'ordre premier p est abélien.*

Définition 1.3.1. *(***Groupe monogène***) Un groupe est* monogène *s'il est engendré par un seul élément. Un groupe d'ordre fini engendré par un élément est dit* cyclique.

Exemple 1.3.1. *Le groupe à six éléments $G = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ est cyclique, car $G =< \bar{1} >=< \bar{5} >$. On a les deux sous-groupes de G : $H =< \bar{2} >= \{\bar{2}, \bar{4}, \bar{0}\} =< \bar{4} >$ et $K =< \bar{3} >= \{\bar{0}, \bar{3}\}$.*

Proposition 1.3.2. *Si G est un groupe fini d'ordre p premier, alors tout élément de G (différent de l'élément neutre) engendre G.*

Exemple 1.3.2. *Si $G = \{1, a, b\}$ est d'ordre 3, alors $G =< a >=< b >$.*

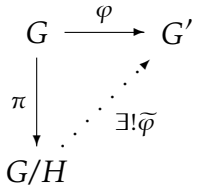
1.4 Théorèmes d'isomorphisme

Définition 1.4.1. *On appel* isomorphisme *de groupes tout homomorphisme bijectif. Lorsqu'il existe un isomorphisme $f : G \to G'$, on dit que G et G' sont deux groupes isomorphes.*
Un isomorphisme de G dans G est appelé un automorphisme *de G.*

Dans ce paragraphe, on suppose $H \lhd G$.

1.4.1 Propriété universelle du groupe quotient

Soit $\varphi : G \to G'$ un morphisme de groupes tel que $H \subset \ker(\varphi)$ et $\pi : G \to G/H$ est la projection canonique. Alors, il existe un unique $\widetilde{\varphi} : G/H \to G'$ tel que $\varphi = \tilde{\varphi} \circ \pi$:



1.4.2 Premier théorème d'isomorphisme

Avec les mêmes notations, $G/\ker(\varphi) \simeq \mathrm{Im}(\varphi)$.

1.4.3 Deuxième théorème d'isomorphisme

Soient H et K deux sous-groupes de G avec $K \lhd G$.
Alors, $(H \cap K) \lhd H$ et

$$H/(H \cap K) \simeq HK/K.$$

1.4.4 Troisième théorème d'isomorphisme

Soient K et H deux sous-groupes normaux de G tel que $K \subset H$. Alors, $(H/K) \lhd (G/K)$ et

$$G/H \simeq (G/K)/(H/K).$$

Ordre d'un élément dans un groupe

On se donne un groupe multiplicatif $(G, \cdot)$.

Définition 1.4.2. *L'ordre d'un élément x de G est l'élément $\mathrm{o}(x) \in \mathbb{N}^*$ défini par :*

$$\mathrm{o}(x) = \mathrm{card}(< x >).$$

Remarque 1.4.1. *Seul l'élément neutre 1_G est d'ordre 1 dans G. En effet, si $x = 1$ alors $< x >= \{1\}$ et si $x \neq 1$; alors $x^0 \neq x^1$ et $< x >$ a au moins deux éléments.*

Remarque 1.4.2. *Pour tout $x \in G$, on a $\mathrm{o}(x) = \mathrm{o}(x^{-1})$.*

Remarque 1.4.3. *Dans le cas où le groupe G est fini d'ordre $n \geq 1$, le théorème de Lagrange nous dit que l'ordre de tout élément de G divise l'ordre de G et en conséquence, on a $x^n = 1$, pour tout $x \in G$.*

Théorème 1.4.1. *Si $\varphi : G \to G'$ est un isomorphisme de groupes, on a*

$$o(\varphi(x)) = o(x), \text{ pour tout } x \in G.$$

Corolaire 1 :

Dire que $x \in G$ est d'ordre fini $n \geqslant 1$ équivaut à dire que $x^n = 1$ et $x^k \neq 1$ pour tout k est compris entre 1 et $n-1$ ($o(x)$ est le plus petit entier naturel non nul tel que $x^n = 1$).

Corolaire 2

Dire que $g \in G$ est d'ordre fini $n \geqslant 1$ équivaut à dire que, pour $k \in Z$; on a $g^k = 1$ si, et seulement si, k est multiple de n .

1.5 Groupe de permutations

Définition 1.5.1. *Soit X un ensemble et soit l'ensemble*

$$S(X) = \{f : X \to X, \ f \text{ bijective}\}.$$

L'ensemble $S(X)$ muni de la composition des applications $(S(X), \circ)$, est un groupe appelé groupe symétrique *ou* groupe de permutations de X.
Si X est fini et $|X| = n$, $S(X)$ est noté S_n.
Un élément de S_n est appelé une permutation.

Remarque 1.5.1. *Tout groupe G est isomorphe à un sous-groupe d'un groupe de permutations.*

1.6 Groupe diédral

Lemme 1.6.1. *Si G et G' sont deux groupes donnés satisfaisant à :*

1. $|G| = |G'| = 2n$,
2. $G =< t, s >$ *et* $G' =< t', s' >$,
3. $o(t) = o(t') = 2$ *et* $o(s) = o(s') = n$,
4. $tsts = 1$ *et* $t's't's' = 1$,

alors G et G' sont isomorphes.

Démonstration.
$H = o(s)$ est d'ordre n et $t \notin H$ .puisque $|G/H| = 2$, on a $G/H = \{H, tH\}$ et $G = H \cup tH$
$G = \{1, ss^1, ..., s^{n-1}\} \cup \{t, ts, ts^2, ..., ts^{n-1}\}$.

De même :
$G' = \{1, s', s'^2, ..., s'^{n-1}, t't's, t's'^2, ..., t's'^{n-1}\}$.
Il suffit alors de vérifier que l'application ϕ définie par
$\phi(s^k) = s'^k$ et $\phi(ts^k) = t's'^k$
est un isomorphisme de G sur G' .

□

Définition 1.6.1. *(Groupe diédral)*
Si G est un groupe vérifiant les conditions 1) , 2) , 3) et 4) du lemme , il est dit **diédral d'indice** n *. On le note D_n . Par définition ,*
$|G| = 2n$, $G =< t; s >$, $o(t) = 2, o(s) = n$ *et* $tsts = 1$.

Exemple 1.6.1. *S_3 est un groupe d'ordre 6 ; τ_1 est d'ordre 2 , σ_1 est d'ordre 3 et et $\tau_1\sigma_1\tau_1\sigma_1 = 1$ .Comme τ_1 et σ_1 engendrent S_3 .*

$$S_3 \simeq D_3$$

Théorème 1.6.1. *Soient $P > 2$ un entier premier et G est un groupe d'ordre $2p$; G est cyclique ou diédral .*

1.7 Somme directe et produit semi-directe de groupes

Définition 1.7.1. *(***Somme directe***) Soit G un groupe commutatif noté additivement. soient $H_1, H_2, ..., H_n$ des sous-groupes de G . on dit que G est* **somme directe** *des sous-groupes H_i si tout élément $x \in G$ s'écrit , de façon unique*

$$x = h_1 + h_2 + ... + h_n \text{ , avec } h_i \in H_i \text{ .}$$

On écrit alors $G = H_1 \oplus H_2 \oplus ... \oplus H_n$.

Exemple 1.7.1. *Tout les éléments $z \in \mathbb{C}$ s'écrit de façon unique , $z = a + ib$ avec $a, b \in \mathbb{R}$.*

Lemme 1.7.1. *Soient $H_1, H_2....H_n$ des sous-groupes d'un groupe G . Le groupe G est leur somme directe , si et seulement si*

a) $G = H_1 + H_2 + ... + H_n$,

b) $\forall j \in [1,n]; H_j \cap (\Sigma_{i \neq j} H_i) = 0.$

Exemple 1.7.2.

1. $Z/6Z = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.
   $H = \{\bar{0}, \bar{3}\}$ *et* $K = \{\bar{0}, \bar{2}, \bar{4}\}$
   $Z/6Z = H \oplus K$ *et* $H \cap K = \{0\}$.
   Alors $Z/6Z \simeq H \times K \simeq Z/2Z \times Z/3Z$.
2. *Dans* $G = (R^3, +)$
   Soient $H = \{(x, y, 0)/x, y \in R\}$ *et* $K = \{(0, y, z)/y, z \in R\}$.
   $R^3 = H + K$ *et* $H \cap K = \{(0, y, 0)\} \neq \{(0, 0, 0)\}$ *,dans ce cas* G *n'est pas somme directe .*

Exemple 1.7.3.

Soient $a, b \in \mathbb{Z}^*$ *; il est clair que* $a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$.

D'après le théorème de Bezout , l'égalité a lieu si et seulement si a et b sont premiers entre eux - le montrer - .

La somme $a\mathbb{Z} + b\mathbb{Z}$ *n'est jamais directe car*

$ab \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow a\mathbb{Z} \cap b\mathbb{Z} \neq 0$.

Comme les seuls sous-groupes de $\mathbb{Z}$ *sont les* $n\mathbb{Z}$ *,* $\mathbb{Z}$ *n'est jamais somme directe de deux ses sous-groupes propres .*

Définition 1.7.2. *(***Produit semi-directe***)*

Soient G_1 *et* G_2 *deux sous-groupe d'un groupe* G*. Le groupe* G *est produit semi-direct de* G_1 *par* G_2 *si et seulement si* $G_1 \cap G_2 = \{e\}, G = G_1 G_2$ *et* G_1 *distingué dans* G*.*

1.8 Action d'un groupe sur un ensemble

Définition 1.8.1. *Soit* G *un groupe et* E *un ensemble. On dit que* G *opère sur l'ensemble* E *s'il existe une lois de composition externe* $(.)$ *telle que*

$$\begin{array}{ccc} G \times E & \to & E \\ (a, x) & \mapsto & a \cdot x \end{array}$$

Qui vérifie :

1. $e \cdot x = x$, *pour tout* $x \in E$. *(*e *est le neutre de* G*).*
2. $(ab) \cdot x = a \cdot (b \cdot x)$, *pour tous* $a, b \in G$, *pour tout* $x \in E$.

Exemple 1.8.1. *Le groupe multiplicatif* $\mathbb{R}^*$ *opère sur* $\mathbb{R}^2$

$$\begin{array}{ccc} \mathbb{R}^* \times \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (\lambda, (a, b)) & \mapsto & (\lambda a, \lambda b). \end{array}$$

Remarque 1.8.1. *Soit* G *un groupe qui opère sur un ensemble* E. *On a les définitions :*

— $\{g \in G,\ g \cdot x = x\}$ *est un sous-groupe de* G *appelé* stabilisateur *de* x.

— *L'ensemble* $\{g \cdot x,\ g \in G\}$ *est appelé* **orbite** *de* x *dans* E.

2

Structure des groupes abéliens finis

2.1 Théorème de structure

Définition 2.1.1. *Si G est un groupe abélien fini, son groupe dual est $\hat{G}$, ensemble des morphismes de groupes de G dans $\mathbb{C}^*$, muni de la multiplication. Les éléments de $\hat{G}$ sont appelés caractères linéaires.*

Définition 2.1.2. *L'exposant d'un groupe fini G est le plus petit N tel que $\forall g \in G$, $g^N = e$.*

Lemme 2.1.1. *L'exposant N de G est égal à $\mathrm{ppcm}_{g\in G}\mathrm{o}(g)$. De plus, il existe un élément d'ordre N dans G.*

Théorème 2.1.1. *(Théorème de structure) Si G est un groupe abélien fini, et N_1 est l'exposant de G, il existe $N_2|...|N_r$ tels que*

$$G \simeq \mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_r\mathbb{Z}.$$

Démonstration. Remarquons tout d'abord qu'en vertu du lemme précédent, G et $\hat{\mathrm{G}}$ ont même exposant.

En effet si $\forall X \in \hat{\mathrm{G}}$, $X^M = 1$, alors $\forall g \in G, \forall X \in \hat{\mathrm{G}}$, $X(g^M) = 1$ d'où $g^M = 1$ donc l'exposant de G divise M . Symétriquement, on obtient que m divise l'exposant de G ce qui conclut.

Montrons le théorème de structure par récurrence sur $|G|$. Il est évident pour $|G| = 1$, on suppose donc $|G| \geqslant 2$ Notons N_1 l'exposant de G et prenons $X_1 \in \hat{\mathrm{G}}$ d'ordre N_1. Son image $X_1(G)$ est donc un sous-groupe du groupe U_{N_1} des racines N_1-èmes de l'unité, donc de la forme U_l où $l|N_1$. Comme X_1 est d'ordre N_1, on a $l = N_1$. En particulier, on peut se donner $x_1 \in G$ tel que $X_1(x_1) = \exp(\frac{2i\pi}{N_1})$. L'ordre de x_1 est N_1 et donc $H = gp(x_1)$ est un sous-groupe cyclique d'ordre N_1 de G.

Montrons que$G \simeq H \times ker(X_1)$.

On a $X_1(H) = X_1(G)$ donc $X_{1|H}$ est injectif pour des raisons de cardinal. En d'autres termes, $H \cap Ker(X_1) = \{e\}$. De plus, si $g \in G$, il existe $h \in H$ tel que $X_1(g) = X_1(h)$ donc $gh^{-1} \in Ker(X_1)$ ce

qui assure que $G = HKer(X_1)$. Donc $G \simeq H \times Ker(X_1)$.
Enfin, il est clair que l'exposant N_2 de $ker(X_1)$ divise celui de G et par hypothèse de récurrence $ker(X_1) \simeq Z/N_2Z...Z/N_rZ$ donc comme $H \simeq Z/N_1Z$, on a le résultat par récurrence. □

Exemple 2.1.1. *Le groupe abélien de type* $(2;2;3;5;8;9)$ *est le groupe abélien d'ordre* 4320 *dont la décomposition canonique est* $Z/2Z \times Z/6Z \times Z/360Z$. *Sa composante* 2*-primaire est* $Z/2Z \times Z/2Z \times Z/8Z$.

Exemple 2.1.2. *Les groupes* $G_1 = Z/36Z \oplus Z/45Z \oplus Z/60Z$ *et* $G_2 = Z/5Z \oplus Z/108Z \oplus Z/180Z$ *sont-ils isomorphes ? Calculons leurs types. Celui de* G_1 *est* $(2;2;3;4;5;5;9;9)$, *tandis que celui de* G_1 *est* $(4;4;5;5;9;27)$. *Puisque les deux types sont différentes, ces deux types sont différents. Leurs représentations canoniques sont* $G_1 \simeq Z/6Z \oplus Z/90Z \oplus Z/180Z$ *et* $G_2 \simeq Z/180Z \oplus Z = 540Z$.

2.2 Décomposition en groupes commutatifs finis

Définition 2.2.1. *Soit* p *un entier premier divisant l'ordre d'un groupe* G. *L'ensemble* G_p *des éléments de* G *est une puissance de* p *est un sous-groupe de* G *appelé* p-composante *de* G *tel que :*

$$G_p = \{x^p,\ x \in G\}.$$

2.2.1 Décomposition en groupes primaires

Théorème 2.2.1. *Tout groupe commutatif fini* G *est somme directe de groupes* p*-primaires où* p *parcourt l'ensemble* D *des diviseurs premiers de l'ordre de* G *:*

$$G = \oplus_{p \in D} G_p.$$

Ce théorème est un théorème d'existence des décompositions primaires en ce sens que si G est un groupe fini d'ordre $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, il permet d'affirmer que

$$G = G_{p_1} \oplus G_{p_2} \oplus ... \oplus G_{p_k}\ .$$

On peut ainsi brutalement écrire , (avant de déterminer , dans chaque cas précis , les G_p) :
$Z/8Z = G_2$,
$Z/4Z \times Z/6Z = H_2 \oplus H_3$,
$Z/30Z = K_2 \oplus K_3 \oplus K_5$,
$Z/48Z = L_2 \oplus L_3$.

Exemple 2.2.1. *Dans* $Z/6Z$

$x+6Z \in H_2 \Leftrightarrow \exists k \in N; 2^k(x+6Z) = 6Z \Leftrightarrow x \in 3Z$

$H_2 = 3Z/6Z$ *(isomorphe à* $Z/2Z$ *) .*

De même $H_3 = 2Z/6Z$ *(isomorphe à* $Z/3Z$*) .*

par conséquent :

$Z/6Z = (3Z/6Z) \oplus (2Z/6Z)$.

2.2.2 Décomposition en groupes cycliques primaires

Théorème 2.2.2. *Tout groupe cyclique* G *d'ordre* $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ *(isomorphe à* Z/nZ*) est somme directe des groupes*

$$G_{p_i} \simeq Z/p_i^{\alpha_i} Z.$$

Exemple 2.2.2. $Z/24Z = L_2 \oplus L_3$ *avec*

$L_2 = 3Z/24Z \simeq Z/8Z$ *et* $L_3 = 8Z/24Z \simeq Z/3Z$.

De même ,

$Z/90Z = G_2 \oplus G_3 \oplus G_5$

où $G_2 \simeq Z/2Z, G_3 \simeq Z/9Z, G_5 \simeq Z/5Z$.

3

Théorèmes de Sylow

Définition 3.0.1. *(p-**groupe**) Soit $p > 0$ un entier premier . On dit que G est* **un p-groupe** *(ou un groupe p-primaire) si et seulement si $|G|$ est puissance de p .*

Exemple 3.0.1. • *$Z/4Z$ est un 2-groupe d'ordre 4 car les périodes de ses éléments sont $2, 3$ ou 6 .*
• *le groupe de Klein $(Z/2Z) \times (Z/2Z)$ est 2-groupe d'ordre 4 .*

Théorème 3.0.1. *(**de Cauchy**). Soit G un groupe fini d'ordre n et $p > 0$ un diviseur premier de n . le groupe G possède un élément d'ordre p .*

Théorème 3.0.2. *(**Burnside**) . Tout p-groupe fini G non réduit à un élément possède un center non réduit à un élément , et $|Z(G)| \geqslant P$.*
(On dit souvent qu'un p-groupe non trivial est de centre non trivial).

Définition 3.0.2. *(p-**sous-groupe de Sylow**) Soit $p > 0$ un entier premier . Un sous-groupe H de G est un* **p-sous-groupe de Sylow** *de G si H est maximal dans l'ensemble des p-sous-groupes de G , ordonné par inclusion.*

Lemme 3.0.1. *Soit G un groupe fini , tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow.*

Théorèmes de Sylow

Soit G un groupe d'ordre $p^n m$, où p est un nombre premier, n est un entier naturel et p ne divise pas m, . Alors :

Théorème 3.0.3. *(***Premier théorème de Sylow***) Il existe un p-Sylow de G d'ordre p^n .*

Théorème 3.0.4. *(***Deuxième théorème de Sylow***) .Tous les p-Sylow de G sont conjugués entre eux, c'est-à-dire que si H et K sont deux p-Sylow de G, alors il existe un élément g dans G vérifiant $gHg^{-1} = K$.*

Théorème 3.0.5. *(***Troisième théorème de Sylow***) Soit n_p le nombre de p-Sylow de G.*

- *n_p divise m.*
- *$n_p \equiv 1 mod.$*

Définition 3.0.3. *Si S est un p-Sylow de G, alors*

$$S \lhd G \Leftrightarrow S \text{ est l'unique } p\text{-Sylow de } G \Leftrightarrow n_p \equiv 1$$

3.1 Applications et propriétés

Proposition 3.1.1. *Soient $p_1;...;p_r$ les diviseurs premiers de l'ordre d'un groupe fini G. Pour tout entier $i2 \in \{1...r\}$, fixons un p_i-Sylow H_i . Les sous-groupes $H_1;...;H_r$ engendrent alors le groupe G.*

Proposition 3.1.2. *Tout groupe abélien fini G est isomorphe au produit direct de ses sous-groupes de Sylow.*

Démonstration. les sous-groupes de Sylow H_i sont distingués et l'application :
$H_1 \times ...H_r \to G$
$(h_1,...,h_r) \mapsto h_1h_2...h_r$
est un homomorphisme surjectif, donc injectif (car les ordres coïncident).

□

Théorème 3.1.1. *(***Argument de Frattini***)) Soit H un sous-groupe distingué d'un groupe fini G. Fixons un sous-groupe de Sylow S de H et indiquons par$N = N_G(S)$ son normalisateur*[1] *dans G.*
On a alors l'identité
$G = HN$.

1. $N_G(S)$ est l'ensemble des éléments $g \in G$ vérifient $gSg^{-1} = x$

4

Structure des groupes de petit ordre

4.1 Groupes d'ordre $n \leq 15$

Il s'agit dans ce thème , de déterminer les groupes finis d'ordre $n \leqslant 15$. compte tenu de ce que nous avons démontré dans les notions précédant , il nous reste seulement à étudier les cas $n = 8, n = 12, n = 14, n = 15$.

En effet

a) Si p est premier , tout groupe d'ordre p est cyclique isomorphe à Z/pZ ; ce qui résout les cas $n = 2, 3, 5, 7, 11$ et 13 .

b) Tout groupe d'ordre p^2 est commutatif , de type (p, p) (isomorphe à $Z/pZ \times Z/pZ$) ou de type p^2 (cyclique , isomorphe à Z/p^2Z) ; cela résout les cas $n = 4$ (groupe de Klein et groupe cyclique) et $n = 9$.

c) Pour le cas $n = 6$, le théorème (1.7.1) montre qu'un groupe d'ordre 6 est cyclique ou isomorphe à S_3 remarquons qu'on trouve pour $n = 6$ le premier groupe non commutatif .

4.1.1 Groupe d'ordre 8

soit G un groupe commutatif d'ordre 8 ; il est isomorphe à l'un des groupes suivant :

$Z/8Z; Z/4Z \times Z/2Z; Z/2Z \times Z/2Z \times Z/2Z$.

Supposons maintenant G non commutatif et d'ordre 8 . Le groupe G n'a pas d'élément d'ordre 8 , sinon $G \simeq Z/8Z$. Il possède un élément d'ordre 4 , sinon tous ses éléments seraient d'ordre 1 ou 2. Pour tout $x \in G, x^2 = 1$, et par suite , si $a, b \in G$, on a $(ab)^2 = 1$ Il vient

$$ba = a^2(ab)b^2 = a(abab)b = ab,$$

qui prouve que G est commutatif et , ce qui est absurde .

Soit donc $a \in G$ un élément d'ordre 4 et $H =< a >$. Puisque $|(G/H)_g| = \dfrac{|G|}{|H|} = 2$, il existe $b \in G$ tel que $G = H \cup Hb$ avec $b \notin H$.

En outre ,étant d'indice 2 , ce sous-groupe H est distingué dans G . On constate que $b^2 \in H$, sinon $b^2 \in Hb$ et $b \in H$, absurde .

puisque $b^2 \in H$, il y a quatre cas possibles que nous allons examiner successivement :

$$b^2 = 1, b^2 = a, b^2 = a^2, b^2 = a^3.$$

• Si $a = b^2$ on a $a \in < b >$, donc $H \subset < b >$ et $G = H \cup Hb =< b >$; c'est absurde , puisque G n'est pas cyclique .

• Si $b^3 = b^2$, alors $(a^3)^3 = a = (b^2)^3 = b^6$, donc $a \in < b >$; c'est absurde d'après ce que nous avons vu dans le cas précédent .

• Si $b^2 = a^2$, puisque $H \lhd G$, on a $b^{-1}ab \in H$. comme $b^{-1}ab$ est conjugué de a , qui est d'ordre 4 , $b^{-1}ab$ est aussi un élément de H d'ordre 4 . Deux cas sont possibles :

1er cas . Si l'élément $b^{-1}ab$ est l'élément a , on voit que $ab = ba$. Soient alors $x, y \in G$,

$$x = a^i b^j \text{ avec } i \geqslant 0 \text{ et } 0 \leqslant j \leqslant 1 \ ,$$
$$y = a^h b^k \text{ avec } h \geqslant 0 \text{ et } 0 \leqslant k \leqslant 1 \ .$$

Alors $xy = (a^i b^j).(a^h b^k) = a^i a^h b^j b^k = a^h a^i b^k b^j = (a^h b^k).(a^i b^j) = yx$.

Le groupe G serait commutatif : absurde .

2ème cas . Si l'élément $b^{-1}ab$ est l'élément a^3 , alors $ab = ba^3$ et

$$G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\} \ .$$

On peut construire la table de ce groupe en utilisant les relations vérifiées dans G ,

$a^4 = 1, ab = ba^3, b^2 = a^2$, et en remarquant que $a^3b = ba$ puisque

$a^3b = a^2(ba^3) = b^2(ba^3) = b^3a^3 = ba^5 = ba.$

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^3b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2

Ce groupe est appelé **le groupe des quaternions** ; on le note Q_2 .

• Si $b^2 = 1$, puisque $H \lhd G$, l'élément $b^{-1}ab$ de H est d'ordre 4; donc $bab^{-1} = a$ ou $bab^{-1} = a^3$ .comme dans le cas précédent , $bab^{-1} = a$ est impossible; donc $bab^{-1} = a^3$ et $ba = a^3b$. Alors $baba = baa^3b = b^2 = 1$ .Cela prouve que G est le groupe diédral D_4 . Il n'est pas isomorphe à Q_2 car dans Q_2 , il n'y a qu'un seul élément d'ordre 2 , alors qu'il y en a 5 dans G .
Finalement on trouve , à l'ordre 8 , trois groupes commutatifs :

$$Z/8Z\,;\ Z/4Z \times Z/2Z \text{ et } Z/2Z \times Z/2Z \times Z/2Z,$$

et deux groupes non commutatifs :

$$Q_2 \text{ et } D_4\ .$$

On peut construire la table du groupe D_4 en utilisant les relations , $a^4 = 1, b^2 = 1$ et $abab = 1$.

Table de D_4.

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

4.1.2 Groupe d'ordre 15

Soit G un groupe d'ordre 15. D'après les théorème de Sylow, les nombres s_3 et s_5 de 3-sous-groupes et de 5-sous-groupes de Sylow vérifient :

$s_3 = 1 + 3k$ et $s_3|15$ donc $k = 0$,

$s_5 = 1 + 5h$ et $s_5|15$ donc $h = 0$.

Le groupe G possède alors un unique 3-sous-groupe H , d'ordre 3 , et un unique 5-sous-groupe K , d'ordre 5 ; ils sont cycliques . Par suite

$H = \{1, a, a^2\}$; $K = \{1, b, b^2, b^3, b^4\}$

et $H \cap K = \{1\}$. Considérons le produit ab ; il est d'ordre 1 ,3, 5 ou 15 .

• Si ab est d'ordre 1 : $ab = 1 \Rightarrow a = b^{-1} \in H \cap K = \{1\}$ - absurde .

• Si ab est d'ordre 3 , et puisque H est l'unique sous-groupe d'ordre 3 de G , $< ab >= H$, donc $ab = a^i$,avec $0 \leqslant i \leqslant 2$. On en déduit que $b = a^{i-1}$ et donc appartient à H , ce qui est impossible .

• Si ab est d'ordre 5 , $< ab >= K$ et $ab = b^i$, d'où $a \in K$ - absurde .

Finalement ab est d'ordre 15 et $G \simeq Z/15Z$.

4.1.3 Groupe d'ordre 12

Comme $12 = 2^2.3$, nous somme dans une situation plus complexe que les précédentes . D'après les théorèmes de Sylow , les nombres s_2 et s_3 de 2-sous-groupes et 3-sous-groupes respectivement , sont tels que :

$s_2 = 1 + 2k$ et $s_2|12$, donc $s_2 = 1$ ou $s_2 = 3$,

$s_3 = 1 + 3h$ et $s_3|12$, donc $s_3 = 1$ ou $s_3 = 4$.

Il y a donc quatre cas à examiner .

1er cas . $s_2 = s_3 = 1$. Soit F l'unique 2-sous-groupe de Sylow et T l'unique 3-sous-groupe de Sylow de G .

Alors $F \lhd G$ et $T \lhd G$; en outre , $F \cap T = \{e\}$.

De plus , $|F|.|T| = 12$. On a donc ,$G \simeq F \times T$.

Le groupe G est alors commutatif , isomorphe à l'un des deux groupes suivants

$$Z/2Z \times Z/2Z \times Z/3Z \simeq Z/2Z \times Z/6Z \quad (\text{type } (2,2,3))$$
$$Z/4Z \times Z/3Z \simeq Z/12Z \quad (\text{type } (2^2 , 3)) .$$

Nous allons , préalablement aux autres cas , monter que dans toutes hypothèses (2ème , 3ème , et 4ème cas) , G est non commutatif .

Soit F un 2-sous-groupe de Sylow ; il est d'ordre 2 ou 4 , et T un 3-sous-groupe de Sylow ; il est d'ordre 3 , donc cyclique .

On a $F \cap T = \{1\}$ .Par suit $|FT| = \dfrac{|F||T|}{|F \cap T|} = |F||T| = |G|$.

Donc $G = FT$.

Comme $s_2 \neq 1$ ou $s_3 \neq 1$, G n'est pas commutatif .

Lemme 4.1.1. *Il existe $f \in F$ et $t \in T$ tel que $ft \neq tf$.*

Démonstration. Tout élément $g \in G$ s'écrit ft . Par suite , si le lemme était faux les éléments de F commuteraient avec ceux de T , et G seraient commutatif . □

2ème cas . $s_2 = 1$ et $s_3 = 4$. Soit alors L'unique 2-sous-groupe de Sylow de G , il est distingué dans G , et soit T 3-sous-groupe de Sylow de G . On sait que $T = \{1, b, b^2\} \simeq Z/3Z$.

Deux sous-cas sont à envisager :

(a) $F \simeq Z/4Z, F = \{1, a, a^2, a^3\}$ avec $a^4 = 1$.

Puisque $F \lhd G$, $b^{-1}ab \in F$.

• Si $b^{-1}aba$, alors $ba = ab$; cela entraîne que les éléments de F commutent avec ceux de G ; cela contredit le lemme précédent et est impossible .

• Puisque a est d'ordre 4 , il en est de même de $b^{-1}ab$; donc $b^{-1}ab \neq a^2, b^{-1}ab \neq 1$ et nécessairement , $b^{-1}ab = a^3$, soit $ab = ba^3$ .Par suite $G =< ba >$.

En effet , $(ba)^2 = b(ab)a = b^2a^4 = b^2$ implique $(ba)^3 = b^2ba = a$, donc $a \in < ba >, b = (ba)a^{-1} \in < ba >$ et finalement $G =< ba >$. Cela est absurde car G n'est pas commutatif .

(b) Le groupe F est isomorphe au groupe de Klein . On peut écrire

$K = \{1, x, y, z\} \simeq Z/2Z \times Z/2Z$.

Comme ci-dessus , si $f \in F \lhd G, b^{-1} f b \in F$.

Mais d'après le lemme , il existe $x \in F$ et $c \in T$ tels que $c^{-1}xc \neq x$. Comme $c^{-1}yc \in F$, trois sous-sous-cas du sous-cas (b) sont possibles :

*) $c^{-1}xc = 1$, d'où $xc = c$ et $x = 1$, ce qui est absurde .

*) L'élément $c^{-1}xc$ est l'élément y . Posons $z = xy$. On en tire $x = cyc^{-1}$.

$c^{-1}yc \neq x$, sinon $c^{-1}yc = cyc^{-1}$ et $y = c^2yc^{-2}$; comme $c^2 = c^{-1}$ et $c^{-2} = c$, on aurait $y = c^{-1}yc = x$, ce qui n'est pas .

De même $c^{-1}yc \neq x, c^{-1}yc \neq y$ et $c^{-1}yc \neq 1$.

Il faut alors que $c^{-1}ycxy = z$ et on a

$c^{-1}(xy)c = (c^{-1}xc)(c^{-1}yc) = yxy = y^2x = x$.

Résumons les règles de calcul ainsi obtenues :

$$xy = cy; yc = cxy; xyc = cx; x^2 = y^2 = 1; c^3 = 1; xy = yx.$$

Mais $1, c$ et c^2 ont des classes distinctes modulo F dans G , donc les éléments de G sont

$$1, c, c^2, x, y, xy, cx, cy, cxy, c^2x, c^2y, c^2xy.$$

On peut maintenant donner la table de G.

Nous allons changer le nom des éléments de G afin de permettre une comparaison plus facile des table :

$$G = \{1, c, c^2, a, b, ab, ca, cb, cab, c^2a, c^2b, c^2ab\}.$$

Table .

	1	c	c^2	a	b	ab	ca	cb	cab	c^2a	c^2b	c^2ab
1	1	c	c^2	a	b	ab	ca	cb	cab	c^2a	c^2b	c^2ab
c	c	c^2	1	ca	cb	cab	c^2a	c^2b	c^2ab	a	b	ab
c^2	c^2	1	c	c^2a	c^2b	c^2ab	a	c	ab	ca	cb	cab
a	a	ac	ac^2	1	ab	b	cab	c	ca	c^2b	c^2a	c^2
b	b	cab	c^2a	ab	1	a	cb	ca	c	c^2	c^2ab	c^2b
ab	ab	ca	c^2b	b	a	1	c	cab	cb	c^2ab	c^2	c^2a
ca	ca	c^2b	ab	c	cab	cb	c^2ab	c^2	c^2a	b	a	1
cb	cb	c^2ab	a	cab	c	ca	c^2b	c^2a	c	1	ab	b
cab	cab	c^2a	b	cb	ca	c	c^2	c^2ab	c^2b	ab	1	a
c^2a	c^2a	b	cab	c	c^2ab	c^2b	ab	1	a	cb	ca	c
c^2b	c^2b	ab	ca	c^2ab	c^2	c^2a	b	a	1	c	cab	cb
c^2ab	c^2ab	a	cb	c^2b	c^2a	c^2	1	ab	b	cab	c	ca

3ème cas . $s_2 = 3$ et $s_3 = 1$. Comme toujours $T = \{1, c, c^2\} \simeq Z/2Z$,est distingué dans G . Soit F l'un des 2-sous-groupes de Sylow : deux sous-cas sont à distinguer :

(1) $F = \{1, a, a^2, a^3\} \simeq Z/4Z$. Alors la distinction de T implique que $a^{-1}ca \in T$.

Comme G est non abélien et que a et c sont des générateurs de F et T , donc , comme $\{a, c\}$ est un système générateur du groupe non commutatif G , $a^{-1}ca \neq c$.

Puisque $a^{-1}ca \neq 1$, on a $a^{-1}ca = c^2$, soit $ca = ac^2$. Ainsi $c^2a = ca^2 = ac^4ac$ et on obtient les équations :

$$ca = ac^2, c^2a = ac, c^3 = 1, a^4 = 1. G = \{1, a, a^2, a^3, c, c^2, ac, a^2c, a^3c, ac^2, a^2c^2, a^3c^2\}.$$

table de Q_3 :

	1	a	a^2	a^3	c	c^2	ac	a^2c	a^3c	ac^2	a^2c^2	a^3c^3
1	1	a	a^2	a^3	c	c^2	ac	a^2c	a^3c	ac^2	a^2c^2	a^3c^3
a	a	a^2	a^3	1	ac	ac^2	a^2c	a^3c	c	a^2c^2	a^3c^2	c^2
a^2	a^2	a^3	1	a	a^2c	a^2c^2	a^3c	c	ac	a^3c^2	c^2	ac^2
a^3	a^3	1	a	a^2	a^3c	a^3c^2	c	ac	a^2c	c^2	ac^2	a^2c^2
c	c	ac^2	a^2c	a^3c^2	c^2	1	a	a^2c^2	a^3	ac	a^2	a^3c
c^2	c^2	ac	a^2c^2	a^3c	1	c	ac^2	a^2	a^3c^2	a	a^2c	a^3
ac	ac	a^2c^2	a^3c	c^2	ac^2	a	a^2	a^3c^2	1	a^2c	a^3	c
a^2c	a^2c	a^3c^2	c	ac^2	a^2c^2	a^2	a^3	c^2	a	a^3c	1	ac
a^3c	a^3c	c^2	ac	a^2c^2	a^3c^2	a^3	1	ac^2	a^2	c	a	a^2c
ac^2	ac^2	a^2c	a^3c^2	c	a	ac	a^2c^2	a^3	c^2	a^2	a^3c	1
a^2c^2	a^2c^2	a^3c	c^2	ac	a^2	a^2c	a^3c^2	1	ac^2	a^3	c	a
a^3c^2	a^3c^2	c	ac^2	a^2c	a^3	a^3c	c^2	a	a^2c^2	1	ac	a^2

(2) $F = \{1, x, y, z\} \simeq Z/2Z \times Z/2Z$. Puisque $T \lhd G$, on a , pour tout f de F , $f^{-1}cf \in T$. Mais il existe $f \in F, f^{-1}cf \neq c$. Supposons $x^{-1}cx = c^2$. On voit qu'alors $cx = xc^2$. On remarque que $c^2x = xc$ car

$$c^2x = c(cx) = c(xc^2) = (cx)c^2 = xc^2c^2 = xc.$$

Vérifiez que :

$S = \{1, c, c^2, x, cx, c^2x\}$ est , d'une part un sous-groupe , dans lequel , d'autre part , il est vrai que

$$c^{-1} = c^2; (c^2)^{-1} = c; x^{-1} = x; (cx)^{-1} = cx; (c^2x)^{-1} = c^2x.$$

Le sous-groupe S est donc d'ordre 6 , dès qu'on a constaté que tous ces éléments sont distincts .

Puisque $xc = c^2x \neq cx$, S est non abélien , donc isomorphe à D_3 . Mais $|(G/S)_g| = 2$ et $S \lhd G$.

L'élément $y^{-1}cy \in S$, et comme il est d'ordre 3 , on a $y^{-1}cy = c$ ou c^2 .

Montrons qu'il existe $h \in F, h \notin S$ tels que $h^{-1}ch = c$.

$\star$ Si $y^{-1}cy = c$, alors $h = y$.

$\star$ Si $y^{-1}cy = c^2$, alors $h = xy$.

Or on sait que $x^{-1}cx = c^2$, donc

$$(xy)^{-1}c(xy) = y^{-1}(x^{-1}cx)y = y^{-1}c^2y = y^{-1}cy.y^{-1}cy = c^4 = c$$

.

En prenant $h = y$ ou $h = xy$, on a $h \in F - S$ tel que $h^{-1}ch = c$.

Soit $H =< c >\simeq Z/2Z$.

Il est clair que $S \cap H = \{1\}$.

Les éléments de H et S commutent , $|S||H| = |G|$,

Donc $G \simeq S \times H$ et $G \simeq D_3 \times Z/2Z \simeq D_6$.

4ème cas . $s_2 = 3$ et $s_3 = 4$. Il y a 4 sous-groupes d'ordre 3 ; comme 2 à 2 , leur intersection est $\{1\}$, il y a donc 8 éléments d'ordre 3 ; soit K leur ensemble (qui n'est pas un sous-groupe , l'élément neutre n'y figurant pas) .

Les 2-sous-groupes de Sylow sont d'ordre 4 .Leur intersection avec un 3-sous-groupe de Sylow est $\{1\}$. Donc si H est un 2-sous-groupe , $H \cap K = \phi$ et $|H \cup K| = 12$.

Par suit G serait égal à $H \cup K$ et ce groupe G aurait un seul 2-sous-groupe de Sylow , contrairement à l'hypothèse .

4.1.4 Groupe d'ordre 14

Soit G groupe d'ordre $n = 14 = 7 \times 2$

D'après les théorème de Sylow , les nombres n_2 et n_7 de 2-sous-groupes et 7-sous-groupes respectivement ; sont tel que :

$n_2 = 1 + 2k$ et $n_2|14$, donc $n_2 = \{1, 7\}$

$n_7 = 2 + 7h$ et $n_7|14$, donc $n_7 = \{1\}$

Il y a donc deux cas à examiner :

1er cas

$n_2 = n_7 = 1$. Soit H l'unique 2-sous-groupe de Sylow de G , et T l'unique 3-sous-groupe de Sylow de G

Alors $H \lhd G$, $K \lhd G$, et $H \cap K = \{e\}$

De plus $|H|.|K| = 14$. On a donc $G \simeq H \times K$.

Alors G est commutatif isomorphe à l'un des groupes suivant :

$G \simeq Z/2Z \times Z/7Z \simeq Z/14Z$.

2ème cas

$n_2 = 7$ et $n_7 = 1$

Il existe $K \lhd G$ et $|K| = 7$; $K =< ab >= \{b, b^2, ..., b^6, b^7 = e\}$.

et $H =< a >$; tel que $o(a) = 2$

$$|HK| = \frac{|H| \times |K|}{|H \cap K|} = 14 \ .$$

d'ou $G = HK$. On écrit $G = \{e, a, b, b^2, .., b^6, ab, ab^2, ..., ab^6\}$.

$abab = e$, en effet :

Soit a, b de G ; alors $abab \in G$ .On a $o(ab)$ divise $|G| = 14$:

• Si $o(ab) = 14$

alors $G \simeq Z/14Z$ (impossible) , car G non commutatif

• Si $o(ab) = 7$

$ab \in < ab >$ et $b^6 \in K =< b > \Rightarrow abb^6 \in K$

alors $a \in < b >$ (impossible) .

Donc $o(ab) = 2 \Rightarrow abab = \{e\}$.

Par conséquence $G \simeq D_7$.

Conclusion

La théorie des groupes, plus particulièrement les théorèmes de Sylow, forme un outil incontournable pour étudier la structure d'un groupe fini donné.

Mais parfois la procédure est très longue et demande plusieurs discussions sur les éléments du groupe.

Récemment, pour gagner du temps, les spécialistes de la théorie des groupes ont développé des programmes performants (comme GAP) ; pour que la machine fait ce travail plus rapidement.

Bibliographie

[1] **A. Bouvier , Denis Richard** , Groupes , l'université Claude Bernard Lyon 1 , (Hermann ; éditeur des sciences des arts).

[2] **Fabrice Castel** , Groupes finis , Préparation à l'agrégation externe , université de rennes 1, 2009-2010 .

[3] **Gabriel Lepetit** , Théorème de structure des groupes abéliens finis , ENS Rennes - Université Rennes 1 .

[4] **Nicolas Jacon** , compliment de Théorie des groupes , master mathématique 1ère année , université de Reims .

[5] **Adrien Fontaine** , Leçon 103 : Exemples et applications des notions de sous-groupes distingués et de groupe quotient , 21 décembre 2013

[6] **Odile Lecacheux** , LM325- Introduction à la théorie des groupes , 12 novembre 2008 .

[7] **Adrien Fontaine** , Leçon 103 : Exemples et applications des notions de sous-groupes distingués et de groupe quotient , 21 décembre 2013 .

[8] **Pierre Lissy** , Groupes finis. Exemples et applications , 6 May 2010 .