Université Mohamed El Bachir El Ibrahimi de Bordj Bou Arréridj
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques

Mémoire

Présenté par

SIMOHAMED LOTH
HAKEM AMROUCHE

Pour l'obtention du diplôme de

Master

Filière : Mathématiques
Spécialité : Système Dynamique +mathématiques appliquer

Thème

Introduction à la Théorie des groupes

Soutenu publiquement le 2021 devant le jury composé de

CHEBEL ZOHEIR	Président
DEKKAR KHADRA	Encadrant
BOUREMEL HASSENE	Examinateur

Promotion 2020/2021

REMERCIEMENTS

Nous remercions avant tout Allah qui nous a donné la force et la volonté pour achever ce travail.

Nous tenons à remercier infiniment notre cher encadreur *Mme. Khadra Dekkar* qui a nous orientée durant cette recherche, pour ces inestimables conseils et pour sa patience à notre égard,sans oublier nos familles,nos proches, les personnes qui nous ont aidé de prés ou de loin.

Nous tenons également à remercier les membres du jury d'avoir accepter d'apprécier notre travail.

Enfin, un grand merci à nos collègues de Faculté des *Mathématiques et de l'Informatique.*

TABLE DES MATIÈRES

Introduction **3**

1 Théorie des groupes **5**
1.1 Généralités 5
1.2 Homomorphisme de groupes 8
1.3 Sous-groupes engendrés 11
1.4 Groupes cycliques 12
1.5 Groupes symétriques 14

2 Groupes normaux et groupes quotients **17**
2.1 Lois internes compatibles 17
2.2 Notion de sous-groupes normaux 24
2.3 Théorèmes fondamentaux des isomorphismes 25

3 Théorèmes de Sylow et ses applications **29**
3.1 Action de Groupes 29
3.2 Orbites et stabilisateurs 33
3.3 Théorèmes de Sylow et ses applications 36

Bibliography **43**

INTRODUCTION

La notion de groupe a été introduite explicitement en mathématiques, au début du dix-neuvième siècle. Elle intervient en effet à cette époque, pour la première fois, dans les travaux relatifs aux équations algébriques, sous forme de groupes de permutations des racines de ces équations ; il s'agissait donc de groupes finis. C'est en exploitant cette idée qu'Evariste Galois obtient en 1832 ses résultats définitifs sur la résolution (par radicaux) des équations polynomiales, qui constituent le fondement de ce qu'on développera plus tard sous le nom de théorie de Galois.

A peu près au même moment, des groupes sont mis en évidence en géométrie, notamment, des groupes de symétries de polygones ou polyèdres réguliers (ce sont encore des groupes finis), puis des groupes (finis ou non) de transformations du plan ou de l'espace. Ces familles de groupes ainsi que leurs généralisations et leurs applications seront ultérieurement, à la base, d'une part, de la théorie de la représentation linéaire des groupes, en particulier des groupes finis , et, d'autre part, de la définition et de l'étude des groupes classiques.

Par ailleurs, on peut constater que le champ d'application des groupes a très largement dépassé le domaine des mathématiques au sens restreint, en permettant notamment l'interprétation et l'explication de nombreux phénomènes physiques. C'est ainsi que la théorie de la représentation linéaire des groupes finis est utilisée à propos de questions liées aux symétries des cristaux et des molécules, et que les groupes semi-simples (issus des groupes de Lie) ont été introduits en physique théorique (théorie de la relativité et mécanique quantique). De même, la théorie des groupes classiques est à la base de l'étude des particules élémentaires.[6]

Dans le premier chapitre nous introduisons les notions de base de groupe et de sous-groupe et en donnons des exemples. Nous définissons ensuite le sous-groupe engendré par une partie d'un groupe. Cela nous amène à parler des groupes monogènes. Enfin, nous abordons les homomorphismes de groupe à la fin du chapitre.

Le deuxième chapitre, après un bref rappel sur les relations d'équivalence, aborde les groupes

quotients. On démontre le théorème de Lagrange, pour finir avec les théorèmes d'isomorphisme.

Le troisième chapitre introduit les actions de groupes et s'achève par la démonstration des théorèmes de Sylow.

CHAPITRE 1

THÉORIE DES GROUPES

Nous allons introduire dans ce chapitre la notion de groupe, puis celle de sous-groupe. On étudiera ensuite les applications entre deux groupes : les morphismes de groupes. Finalement nous détaillerons deux groupes importants : les groupes des permutations.

1.1 Généralités

Les groupes sont à la base d'autres notions mathématiques comme les anneaux, les corps, les matrices, les espaces vectoriels,..., mais vous les retrouvez aussi en arithmétique, en géométrie,...

Définition 1.1.1 *Soit G un ensemble non vide muni d'une loi de composition interne $*$: $GG \to G$; $(x, y) \to x * y$. On dit que $(G, *)$ est un* ***groupe*** *si :*

1. *La loi $*$ est associativité c'est-à-dire : Pour tous x, y, z de G, on a $x * (y * z) = (x * y) * z$.*
2. *L'ensemble G possède un élément neutre c'est-à-dire : Il existe un élément noté e dans G tel que : pour tout x de G, on a : $e * x = x * e = x$.*
3. *Si tout élément x de G possède un inverse. c'est-à-dire : Pour tout x de G, il existe un élément y de G, qu'on notera x^{-1}, tel que : $x * y = y * x = e$.*

Si de plus $x * y = y * x$ pour tout $x, y \in G$, le groupe $(G, *)$ est dit commutatif ou abélien.

Remarque 1.1.2 *La plupart du temps, pour simplifier l'écriture, on emprunte en général la notation usuelle de la multiplication et on note xy au lieu de $x * y$, la loi $*$ étant sous-entendue. Alors, les axiomes ci-dessus deviennent :*

1. *$\forall x, y, z \in G$, on a $x(yz) = (xy)z$.*
2. *$\exists e \in G$ tel que : $\forall x \in G$, on a : $ex = xe = x$.*
3. *$\forall x \in G$, $\exists y \in G$, tel que : $xy = yx = e$.*

Conformément à cette notation multiplicative, le symétrique est en général appelé l'inverse et noté x^{-1}. Enfin, le neutre e est souvent noté 1.

Dans le même souci de simplifier les notations, on note en général simplement G au lieu de $(G, *)$. C'est un abus d'écriture, car pour un même ensemble G, il peut y avoir plusieurs lois qui en font un groupe de manière différente.

Exemple 1.1.3 *Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de l'addition usuelle sont des groupes abéliens. Il en est de même pour $\mathbb{Q}^*$, $\mathbb{R}^*$, ou $\mathbb{C}^*$ munis de la multiplication usuelle.*
L'espace $Gl_n(\mathbb{C})$ des matrices carrées inversibles d'ordre n muni de la multiplication usuelle des matrices est aussi un groupe, mais il n'est pas abélien.

Proposition 1.1.4 *Si $\mathbb{K}$ est un corps commutatif, et E un $\mathbb{K}$-espace vectoriel, alors l'ensemble $Gl(E)$ des applications linéaires de $E \to E$ muni de la composition usuelle est un groupe.*

Montrer qu'un ensemble est un groupe à partir de la définition peut être assez long. Il existe une autre technique, c'est de montrer qu'un sous-ensemble d'un groupe est lui-même un groupe : c'est la notion de sous-groupe.

Définition 1.1.5 *Soit $(G, *)$ un groupe. On appelle **sous-groupe** de G, un sous ensemble H de G tel que :*

1. *H est stable par la loi interne : pour tout x et tout y de H, on a $x * y \in H$.*
2. *L'élément neutre de G est dans H ($e \in H$).*
3. *H est stable par inversion : pour tout x de H, l'inverse de x pour la loi de G est dans H ($\forall x \in H \Rightarrow x^{-1} \in H$).*

Un sous-groupe est un groupe, et un groupe inclus dans un groupe (pour les mêmes lois bien sûr) est un sous-groupe de ce groupe. C'est-à-dire, si la restriction $*_{|HH}$ de $*$, $*_{|HH} : HH \to G$ a en fait pour image H, $(H, *_{|HH})$ est un groupe.

Remarque 1.1.6 *Un critère pratique et plus rapide pour prouver que H est un sous-groupe de G est :*
1. H contient au moins un élément.
2. Pour tout $x, y \in H$, $x * y^{-1} \in H$.

Exemple 1.1.7 *1. L'ensemble $\left(\mathbb{R}_+^*, \right)$ est un sous-groupe de $(\mathbb{R}^*,)$.*
2. L'ensemble $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
3. Les ensembles e et G sont les sous-groupes triviaux du groupe G.
4. L'ensemble des matrices diagonales est un sous-groupe de $Gl_n(\mathbb{R},)$.

Proposition 1.1.8 *Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{Z}$. où l'ensemble $n\mathbb{Z}$ désigne l'ensemble des multiples de n.*

Proposition 1.1.9 *Soit G un groupe.*
1. Soient H_1 et H_2 des sous-groupes de G alors $H_1 \cap H_2$ est un sous-groupe de G.
2. Plus généralement, soit $(H_i)_{i \in I}$ une famille de sous-groupes de G alors $\cap_{i \in I} H_i$ est un sous-groupe de G.

Preuve. 1. Soient H_1 et H_2 des sous-groupes de G, puis $H_1 \cap H_2 \neq \varnothing$, Étant donné qu'au moins l'identité (e) est commun à la fois à H_1 et à H_2.
Pour prouver que $H_1 \cap H_2$ est un sous-groupe il suffit de prouver que

$$x \in H_1 \cap H_2, \quad y \in H_1 \cap H_2 \Rightarrow xy^{-1} \in H_1 \cap H_2$$

Prenons

$$x \in H_1 \cap H_2 \Rightarrow x \in H_1 \ \ et \ \ x \in H_2$$

$$y \in H_1 \cap H_2 \Rightarrow y \in H_1 \ \ et \ \ y \in H_2$$

puisque H_1 et H_2 sont des groupes de G par conséquent

$$x \in H_1, \ \ y \in H_1 \Rightarrow xy^{-1} \in H_1, \ \ et \ \ x \in H_2, \ \ y \in H_2 \Rightarrow xy^{-1} \in H_2$$

Alors

$$xy^{-1} \in H_1 \ \ et \ \ xy^{-1} \in H_2 \Rightarrow xy^{-1} \in H_1 \cap H_2$$

par conséquent $H_1 \cap H_2$ est un sous-groupe de G.
2. Notons $\cap_{i\in I} H_i$ n'est pas vide depuis $e \in H_i$ pour chaque $i \in I$. Maintenant laisse

$$x, y \in \cap_{i\in I} H_i \ \ donc \ \ x, y \in H_i \ \ \ pour \ \ chaque \ \ \ i \in I$$

Par le critère de sous-groupe,

$$xy^{-1} \in H_i \ \ pour \ \ chaque \ \ i \in I. \ Ainsi \ \ xy^{-1} \in \cap_{i\in I} H_i.$$

On conclure que $\cap_{i\in I} H_i$ est un sous-groupe de G. ■

Remarque 1.1.10 *L'union de deux sous-groupe H_1 et H_2 n'est pas nécessairement un sous-groupe. Voici la preuve utilisant le raisonnement par l'absurde.*

Preuve. On suppose que l'union $H_1 \cup H_2$ est un sous-groupe de G.
Puisque $H_1 \nsubseteq H_2$(signifie que H_1 n'est pas un sous ensemble de H_2), il existe un élément $x \in H_1$ tel que $x \notin H_2$.
De même pour $H_2 \nsubseteq H_1$, il existe un élément $y \in H_2$ tel que $y \notin H_1$.
Comment on suppose $H_1 \cup H_2$ est un sous-groupe, on a $xy \in H_1 \cup H_2$. Il s'ensuit que soit $xy \in H_1$ ou $xy \in H_2$.
* Si $xy \in H_1$ nous avons $y = x^{-1}(xy) \in H_1$ car x^{-1} et xy sont des éléments de groupe H_1 ; cela contredit notre choix de l'élément y.
* Si $xy \in H_2$ nous avons $x = (xy)y^{-1} \in H_2$ car $y^{-1} \ \ et \ \ xy \in H_2$; ce que contredit le choix de x.

Ainsi, on conclure que l'union $H_1 \cup H_2$ n'est pas un sous-groupe de G. ■

Proposition 1.1.11 *Soient H, K deux sous-groupes non vides d'un groupe G*

$$HK = \{g \in G, \ \ g = hk, \ \ h \in H, \ \ k \in K\}$$

HK est un sous-groupe de G si et seulement si $HK = KH$ dans G.

Preuve. Premier sens : Supposons que HK est un sous-groupe de G. Soit $yx \in KH$, avec $x \in H$, $y \in K$ montrons que $yx \in HK$.
On sait que

$$yx = (x^{-1}y^{-1})^{-1}.$$

H et K sont des sous-groupes, donc

$$x^{-1} \in H; \quad y^{-1} \in K \quad et \quad x^{-1}y^{-1} \in HK,$$

et comme HK est un sous-groupe de G,

$$yx = (x^{-1}y^{-1})^{-1} \in HK.$$

On a donc $KH \subset HK$. Montrons que $HK \subset KH$. Soit $z \in HK$, $z^{-1} \in HK$, donc $\exists x \in H; \quad y \in K; \quad z^{-1} = xy$, d'où $z = y^{-1}x^{-1} \in KH$ (propriété des sous-groupes).
Deuxième sens : $e \in H; K$, donc $e = ee \in HK \neq \varnothing$
Soient $s; t \in HK$, il faudra montrer que $st^{-1} \in HK$ (utiliser les définition et les inverses) . ■

1.2 Homomorphisme de groupes

Nous allons développer dans la suite quelques-unes des techniques de base développées comme les morphismes de groupes

Définition 1.2.1 *Soient deux groupes dont les lois sont notées $*$ et $\cdot$; on appelle **homomorphisme** de G dans G' toute application $f : G \to G'$ telle que, pour tout x et tout y de G, on ait*

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

*Un homomorphisme de groupes est aussi appelé **morphisme** de groupes.*

L'ensemble des homomorphismes d'un groupe G dans un groupe G' sera noté $Hom(G, G')$.
Un homomorphisme d'un groupe G dans lui-même est appelé **endomorphisme** de groupe.
L'ensemble des endomorphismes d'un groupe G sera noté $End(G)$.

Exemple 1.2.2
- *1. Si G est un groupe, l'application identique Id_G de G est un morphisme de G dans lui-même.*
- *2. Si G_1 et G_2 sont des groupes, l'application $G_1 \to G_2$ constante égale à l'élément neutre de G_2 est un morphisme de groupes. En particulier il existe toujours au moins un morphisme d'un groupe dans un autre.*
- *3. Soit G un groupe, le groupe $GL_n(\mathbb{R})$ des matrices inversibles nn avec des entrées réelles. Pour X dans $GL_n(\mathbb{R})$, définissez $\delta(X)$ comme étant le déterminant par X i.e. $(\delta(X) = det(X))$. Puisque X est inversible, son déterminant est non nul. C'est une propriété standard des déterminants qui*

$$det(AB) = det(A)det(B).$$

Il en découle que δ est un homomorphisme.

Définition 1.2.3 *Soit $f \in Hom(G, G')$, alors :*

— *L'ensemble $f(G)$ est appelé **image** de f et est noté Imf.*

$$Imf = \{f(x) \setminus x \in G\}$$

— *L'ensemble $f^{-1}(e_{G'})$ est appelé **noyau** de f et est noté $Kerf$.*

$$Kerf = \{x \in G \setminus f(x) = e_{G'}\}$$

Lemme 1.2.4 *1. Le noyau d'un morphisme de groupes $f : G \to G'$ est un sous-groupe de G. Si $ker(f) = e_G$, alors f est injective et réciproquement.*
2. L'image d'un morphisme de groupes $f : G \to G'$ est un sous-groupe de G'. Si $Im(f) = G'$, alors f est surjective et réciproquement.

Définition 1.2.5 *Un homomorphisme de groupes $f : G \to G'$ est appelé **isomorphisme de groupes** s'il existe un homomorphisme $g : G' \to G$ tel que $g \circ f = id(G)$ et $f \circ g = id(G')$.*
S'il existe un isomorphisme d'un groupe G sur un groupe G', on dit que G et G' sont des groupes isomorphes ; dans ce cas on écrit : $G \simeq G'$

Définition 1.2.6 *G étant un groupe, un isomorphisme de G sur lui-même est appelé un **automorphisme du groupe** G. L'ensemble des automorphismes d'un groupe G est noté $Aut(G)$.*

Corollaire 1.2.7 *Soit G_1 et G_2 des groupes. Un morphisme de groupes $f : G_1 \to G_2$ est un isomorphisme si et seulement s'il est bijectif.*

Remarque 1.2.8 *1. Pour tout morphisme de groupes $f : G_1 \to G_2$, le neutre est envoyé sur le neutre, l'image du symétrique est le symétrique de l'image. Plus formellement :*
$f(e_{G_1}) = f(e_{G_1}e_{G_1}) = f(e_{G_1})f(e_{G_1})$, ce qui montre, en composant à droite par $f(e_{G_1})^{-1}$, que $f(e_{G_1}) = e_{G_2}$
2. Puisque $f(e_{G_1}) = e_{G_2} = f(g * g^{-1}) = f(g) \cdot f(g^{-1})$ on en déduit que $f(g^{-1}) = f(g)^{-1}$ pour tout $g \in G$. On obtient par récurrence que $f(g^n) = f(g)^n$ pour tout $n \in \mathbb{Z}$ et tout $g \in G$.
3. Soient G un groupe et H un ensemble. Si $f : G \to H$ est une application bijective, on peut munir H d'une structure de groupe telle que f soit isomorphisme, et cela de maniéré unique.
4. Soient G un groupe et H un ensemble et $f : G \to H$ une application. L'ensemble $f(G)$ muni de la loi $*$ définie par $f(x) * f(y) = f(xy)$ est un groupe.

Proposition 1.2.9 *Soit $f : G \to G'$ un morphisme de groupes. Alors l'image de tout sous-groupe de G par f est un sous-groupe de G'.*
L'image réciproque de tout sous-groupe de G' par f est un sous-groupe de G.

Preuve. Soit H un sous-groupe de G. Alors l'image de H par f est

$$f(H) = \{f(h) \setminus h \in H\}.$$

L'image $f(H)$ est non vide car il contient $f(e_G) = e_{G'}$.
Soient g_1, g_2 deux éléments de $f(H)$. Il existe donc $h_1, h_2 \in H$ tels que

$$g_1 = f(h_1) \ \ et \ \ g_2 = f(h_2).$$

Ainsi $f(h_2^{-1}) = g_2^{-1}$ (D'après la remarque ci-dessus) et donc

$$g_1 g_2^{-1} = f(h_1)f(h_2^{-1}) = f(h_1 h_2^{-1}) \in f(H).$$

Puisque $h_1 h_2^{-1} \in H$. Donc $f(H)$ est un sous-groupe de G'.
De même, soit L un sous-groupe de G'. Son image réciproque par f est :

$$f^{-1}(L) = \{g \in G, f(g) \in L\}$$

qui est non vide car il contient e_G ($f(e_G) = e_{G'} \in L$).
Soient g_1 et g_2 deux éléments de $f^{-1}(L)$. Alors

$$f^{-1}(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1}$$

comme $f(g_1)$ et $f(g_2)^{-1}$ sont dans L qui est un sous-groupe de G' alors $f(g_1)$ et $f(g_2)^{-1}$ est aussi dans L. Donc

$$g_1 g_2^{-1} \in f^{-1}(L).$$

Ce qui prouve que $f^{-1}(L)$ est un sous-groupe de G. ■

Proposition 1.2.10 *Soient $f_1 : G_1 \to G_2$ et $f_2 : G_2 \to G_3$ deux morphismes de groupes, alors $f_2 \circ f_1$ est un morphisme de groupes.*
Si $f : G_1 \to G_2$ est un isomorphisme de groupes, alors $f^{-1} : G_2 \to G_1$ est aussi un isomorphisme de groupes.

Preuve. Prouvons la première assertion.
Soient g_1 et g_2 deux éléments de G_1, alors

$$f_2 \circ f_1(g_1 g_2) = f_2(f_1(g_1 g_2)) = f_2(f_1(g_1)f_1(g_2)) = f_2 f_1(g_1) f_2 f_1(g_2) = f_2 \circ f_1(g_1) f_2 \circ f_1(g_2).$$

Prouvons la deuxième assertion.
L'application $f : G_1 \to G_2$ étant bijective, il existe une application inverse bijective $f^{-1} : G_2 \to G_1$. Tout élément g' de G_2 s'écrit de manière unique sous la forme $f(g)$. Soient alors deux éléments $f(g_1)$ et $f(g_2)$ de G_2.

$$f^{-1}(f(g_1)f(g_2)) = f^{-1}(f(g_1 g_2)) = g_1 g_2 = f^{-1}(f(g_1)f^{-1}(f(g_2))$$

est donc bien un isomorphisme. ■

1.3 Sous-groupes engendrés

Le sous-groupe engendré par l'ensemble S est le plus petit sous-groupe de G contenant S.

Définition 1.3.1 *Soient G un groupe et soit S un sous ensemble de G, il existe un plus petit sous-groupe de G contenant S appelé* ***sous-groupe engendré*** *par S. Ce sous-groupe est noté $\langle S \rangle$*

Par exemple si $S = \{2\}$ et le groupe est $(\mathbb{R}^*,)$, le sous-groupe engendré par S est $H = \{2^n, \ n \in \mathbb{Z}\}$.
Pour le prouver : il faut montrer que H est un sous-groupe, que $S = \{2\} \subset H$, et que si H' est un autre sous-groupe contenant 2 alors $H \subset H'$. Autre exemple avec le groupe $(\mathbb{Z}, +)$: si $S_1 = \{2\}$ alors le sous-groupe engendré par S_1 est $H_1 = 2\mathbb{Z}$.
Si $S_2 = \{12, 8\}$ alors $H_2 = 4\mathbb{Z}$ et plus généralement si $S = \{a, b\}$ alors $H = pgcd(a, b)\mathbb{Z}$.

Proposition 1.3.2 *Le sous-groupe engendré par S peut être décrit des deux manières suivantes :*
i) C'est l'ensemble des produits $x_1...x_n \in G$ où $n \geq 0$ est entier et pour tout $i \geq 1$, $x_i \in S$ ou $x_i^{-1} \in X$ (on considère que le produit vide est égal à e et fait partie de cet ensemble).
ii) C'est l'intersection des sous-groupes de G contenant S.

Preuve. Notons $H_{i \in I}$ la famille des sous-groupes de G contenant S.
D'après la proposition (1-1-9), l'intersection

$$H = \cap_{i \in I} H_i$$

est un sous-groupe de G. Il est clair que H contient S ; et par ailleurs tout sous-groupe K contenant S est l'un des H_i et donc contient H, qui est leur intersection.
Ceci montre que H est le plus petit des sous-groupes de G contenant S.
Considérons maintenant l'ensemble E des produits $a_1 a_2 ... a_n \in G$ avec n entier et pour tout i, $a_i \in S$ ou $a^{-1} \in S$.
Cet ensemble contient e. De plus, étant donnés deux éléments $a_1...a_n$ et $b_1...b_m$, il est clair que le produit $a_1...a_n b_1...b_m$ est encore dans E, puisque c'est un produit d'un certain nombre d'éléments appartenant, eux ou leur inverse, à S.
Enfin, l'inverse de $a_1...a_n$ est $a_n^{-1}...a_1^{-1}$, c'est encore un élément de E. Il s'ensuit que E est un sous-groupe de G contenant S.
Par ailleurs, si un sous-groupe quelconque H de G contient S, alors d'après les propriétés de sous-groupe, il contient tous les inverses des éléments de S, et aussi tous les produits d'un certain nombre (fini) d'éléments de S et d'inverses d'éléments de S. Donc H contient E.
Finalement E est le plus petit des sous-groupes de G contenant S. ■

Proposition 1.3.3 *Soit S une partie non vide d'un groupe G.*
1. Si la loi de G est l'addition

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} x_i, \quad n \in \mathbb{N}, \quad \forall i \in 1, ..., n, \quad x_i \in S \ \ ou \ \ -x_i \in S \right\}$$

2. Si la loi de G est la multiplication

$$\langle S\rangle = \left\{ \prod_{i=1}^{n} x_i, \quad n \in \mathbb{N}, \quad \forall i \in 1, ..., n, \quad x_i \in S \ \ ou \ \ x_i^{-1} \in S \right\}$$

3.Soit $x \in G$,

$$\langle x\rangle = \{x^n, \ \ n \in \mathbb{Z}\}$$

4. Si $\langle S\rangle = G$, S est une partie génératrice de G, c'est un ensemble de générateurs de G et engendre G.
*5. Si de plus $S = \{x\}$, on dit que $\langle x\rangle$ est **monogène**.*
*6. S'il existe $S \neq \Phi$ et finie telle que S engendre G, on dira que G est de **type fini**.*
Attention on peut être de type fini sans être fini ! Par exemple : $\mathbb{Z} =< 1 >$ n'est pas fini.

Corollaire 1.3.4 *Soient $f : G \to G'$ un morphisme de groupes et $X \subset G$ un sous-ensemble de G. Alors*

$$f(< X >) =< f(X) > .$$

Preuve. L'image d'un mot de longueur finie en les $x_i \in X$ et leurs inverses x_i^{-1} est un mot de longueur finie en les $f(x_i)$ et les $f(x_i)^{-1}$ car $(f(x_i^{-1}) = f(x_i)^{-1})$.
Donc $f(< X >) \subset < f(X) >$.
Inversement un mot de longueur finie en les $f(x_i)$ et $f(x_i)^{-1}$ est l'image d'un mot de longueur finie en les x_i et les x_i^{-1}, d'où $< f(X) > \subset f(< X >)$.
■

Nous étudierons dans les deux sections suivantes deux autres groupes très importants : les groupes cycliques et le groupe des permutations.

1.4 Groupes cycliques

La notion d'ordre d'un élément est liée aux groupes cycliques. Rappelons qu'on appelle ordre d'un ensemble fini le nombre de ses éléments (on dit aussi cardinal). Il s'agit de deux emplois différents du mot ordre. Mais il y a quand même un lien.

Définition 1.4.1 *On dit que G est un groupe fini, si le **cardinal** de G est fini, en tant que ensemble (autrement dit si G a un nombre fini d'éléments). On dit alors du cardinal $|G|$ que c'est **l'ordre** de G.*
L'ordre d'un élément $x \in G$ est l'ordre du groupe monogène $\langle x\rangle$. C'est le plus petit entier $n > 0$ tel que $x^n = e$. On le note $ord(x) = n$ ou $|x|$ comme le cardinal d'un ensemble.
Si n n'existe pas le groupe $\langle x\rangle$ est infini, on dit que l'ordre de x est infini, et on écrit $ord(x) = \infty$.

Pour un groupe G fini, il est clair que $ord(x) \leqslant |G|$, pour chaque élément x de G, puisque $\langle x\rangle \subset G$. L'élément neutre e est le seul élément de G d'ordre 1. En effet, on a d'abord clairement $|\langle e\rangle| = |\{e\}| = 1$. Réciproquement, si $ord(x) = 1 = |\{x\}|$, alors $\{x\} = x$. Comme tout sous-groupe de G contient e, on a $e \in \{x\}$, et donc $x = e$.

Définition 1.4.2 *Un groupe G est dit **cyclique** s'il est monogène fini.*

Donc toute groupe cyclique est un groupe monogène et fini. Évidemment, G est infini s'il contient un élément d'ordre infini x, puisqu'il contient l'ensemble infini $< x >$. On a vu que le groupe $\mathbb{Z}$ est cyclique.

Théorème 1.4.3 *Tout groupe cyclique est un groupe abélien.*

Preuve. Soit G un groupe cyclique et soit g le générateur de G de sorte que

$$G =< g >= \{g^n, n \in \mathbb{Z}\}$$

Si h_1 et h_2 sont deux élément de G donc il existe deux entiers r et s tels que $h_1 = g^r$ et $h_2 = g^s$. Alors

$$h_1h_2 = g^r g^s = g^{r+s} = g^{s+r} = g^s g^r = h_2h_1.$$

Donc G est abélien. ■
Le résultat suivant est une caractérisation importante de l'ordre d'un élément, qui met en évidence une propriété importante des groupes finis.

Proposition 1.4.4 *Dans un groupe G fini, l'ordre d'un élément x est la plus petite puissance de x qui donne l'élément neutre, c'est-à-dire*

$$ord(x) = min\{n \in \mathbb{N}, \quad x^n = e\}.$$

Le groupe cyclique $\langle x \rangle$ s'écrit alors comme

$$\langle x \rangle = \{e, x, x^2, ..., x^{n-1}\}.$$

Preuve. On sait que

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

Comme x est d'ordre fini, l'ensemble $\{x^k, \quad k \in \mathbb{Z}\}$ l'est aussi. Donc il existe p, q tel que p>q et $x^p = x^q$.
En effet, sinon $x^p = x^q$ impliquerait que $p = q$ et donc que la fonction

$$\mathbb{Z} \to \langle x \rangle \quad avec \quad k \mapsto x^k,$$

serait injective, et donc bijective. D'où $\langle x \rangle$ serait infini, ce qui contredirait notre hypothèse. Puisque $x^p = x^q$, on constate donc que $x^{p-q} = e$ et $p-q > 0$. L'ensemble $\{k \in \mathbb{N}, \quad x^k = e\} \subseteq \mathbb{N}$ est donc non vide, il admet donc un plus petit élément n. Il s'ensuit que $x^n = e$ et

$$\langle x \rangle = \{e, x, x^2, ..., x^{n-1}\}.$$

et donc que $ord\langle x \rangle = |\langle x \rangle| = n$. ■

Lemme 1.4.5 *Soient G, G' deux groupes. Soit $f : G \to G'$ un morphisme de groupes. Si G est monogène, alors Imf est monogène.*

Le groupe G est monogène s'il existe $x \in G$, $G = \langle x \rangle = \{x^k, k \in \mathbb{Z}\}$ donc

$$Imf = f(G) = \{f(x)^k, k \in \mathbb{Z}\} = \langle f(x) \rangle$$

donc Imf est un groupe monogène.

Théorème 1.4.6 *1. Soit G un groupe monogène infini. Si H un sous-groupe de G non réduit à (e_G), alors H est un groupe monogène infini.*
2. Soit G un groupe cyclique, alors si H est un sous-groupe de G, H est un groupe cyclique.

Corollaire 1.4.7 *Si G est un groupe cyclique d'ordre $n \geq 1$, alors le nombre de sous-groupes de G est égal au nombre de diviseurs de n dans $\mathbb{N}$. En d'autre terme : Si G est un groupe cyclique,*

$$card\{H, \quad H \ est \ un \ sous \ groupe \ de \ G\} = card\{m \in \mathbb{N}, \quad m/|G|\}$$

Proposition 1.4.8 *Soit $G \neq \{e\}$ un groupe. On a l'équivalence suivante : Les sous-groupes de G sont exactement $\{e\}$ et G si et seulement si G est un groupe cyclique d'ordre premier.*

1.5 Groupes symétriques

Considérons plus en détail le groupe symétrique S_E, des permutations d'un ensemble E

Définition 1.5.1 *Soit E un ensemble.*
L'ensemble S_E des bijections de E muni de la loi de composition des applications est un groupe (si $E = \phi$, Se est réduit à un élément).
*En particulier, pour tout entier $n > 0$, l'ensemble des bijections de l'ensemble $\{1, ..., n\}$ dans lui-même muni de la loi de composition des applications est un groupe qu'on notera S_n et qu'on appellera **groupe symétrique**. On appellera **permutations** les éléments de S_n.*
***Notation** Pour simplifier la notation, on notera le composé par juxtaposition : $\sigma'\sigma$ signifie $\sigma' \circ \sigma$, en n'oubliant pas que ce produit n'est pas commutatif en général.*

Définition 1.5.2 *On appelle **transposition** de S_n une permutation de S_n qui échange deux éléments de $\{1, ..., n\}$ et laisse les autres fixes. La notation précédente serait lourde pour une telle permutation et on note souvent $\tau = (ij)$ la transposition définie par $\tau(i) = j$,$\tau(j) = i$ et, pour tout entier $k \neq i, j$, $\tau(k) = k$. L'entier n n'apparaît pas dans cette notation, mais le contexte ne laisse, en général, aucune ambiguïté. Comme $\tau\tau = id$, τ est un élément d'ordre 2 de S_n.*

Définition 1.5.3 ***cycles***
On appelle cycle de longueur $r > 1$ de S_n, ou r-cycle, une permutation $c \in S_n$ telle qu'il existe des éléments $x_1, ..., x_r$ de $\{1, ..., n\}$ vérifiant $c(x_1) = x_2, ..., c(x_{r-1}) = x_r$ et $c(x_r) = x_1$ et telle que c laisse fixes les autres éléments de $\{1, ..., n\}$. La notation usuelle pour un cycle est $c = (x_1, ..., x_r)$, l'entier n étant sous-entendu.
En particulier, une transposition est un cycle de longueur 2.

Notation
Décrire une permutation $f : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ équivaut à donner les images de chaque i allant de 1 à n. Nous notons donc f par :

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

Exemple 1.5.4 (Le groupe S_3) *Soit S_3 le groupe des permutations de $\{1, 2, 3\}$*
Nous savons que S_3 possède $3! = 6$ éléments que nous énumérons :

- *l'identité*
$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$
- *une transposition*
$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
- *une deuxième transposition*
$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
- *une troisième transposition*
$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
- *un cycle*
$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
- *l'inverse du cycle précédent*
$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Alors on peut conclure que $S_3 = \{id, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}$

Théorème 1.5.5 ***Théorème de cayley***
Tout groupe G est isomorphe à un sous-groupe du groupe S_G de ses permutations.

Preuve. Soit g un élément de G.
L'application $f_g : G \to G$ définie par $f_g(x) = gx$ est bijective, c'est donc une permutation de G.
L'application

$$F : G \to S_G, \quad g \to f_g$$

est un morphisme de groupe. En effet

$$F(gh) = F(g) \circ F(h).$$

De plus, F est injective.
En effet, si $F(g) = id$, pour tout x de G on a $gx = x$, d'ou $g = e_G$ (i.e. $ker(F) = e_G$).
Par conséquent F est un isomorphisme de G sur son image $F(G)$, qui est un sous-groupe de S_G. ■

CHAPITRE 2

GROUPES NORMAUX ET GROUPES QUOTIENTS

Les sous-groupes et les classes qu'on peut leur associer jouent un rôle important dans l'étude des actions. De plus, lorsque le sous-groupe sera distingué, on pourra définir une notion de groupe quotient. Les notions de sous-groupes et de groupes quotient permettent souvent de diviser en deux la complexité liée à un groupe.

2.1 Lois internes compatibles

Soit E un ensemble muni d'une loi de composition interne $*$. On appelle relation d'équivalence une relation réflexive, transitive et symétrique. Pour les relations d'équivalence, on utilise souvent la notation $x \sim y$ au lieu de $x\mathcal{R}y$. On appelle relation d'ordre une relation réflexive, transitive et antisymétrique.

Définition 2.1.1 *Soit $\mathcal{R}$ une relation **d'équivalence** sur E. On note $\overline{x}$ l'ensemble des $y \in E$ tels que $x \sim y$, c'est à dire*

$$\overline{x} = \{y \in E, \quad x \sim y\}.$$

*et on l'appelle **la classe d'équivalence** de x.*

On note $E/\mathcal{R}$ ou $E/\sim$ l'ensemble des classes d'équivalence des éléments de E, elle est appelé aussi **ensemble quotient** de E par $\mathcal{R}$:

$$E/\mathcal{R} = \{\overline{x}, \quad x \in E\}.$$

Définition 2.1.2 *Soit $f : E \longrightarrow F$ une application vers un ensemble F. Alors, la relation $\mathcal{R}$ définie par : $x \sim x'$ si et seulement si $f(x) = f(x')$ est une relation d'équivalence sur E que l'on appelle la relation d'équivalence associée à f.*

Théorème 2.1.3 *Soit $\mathcal{R}$ une relation d'équivalence sur E. Alors, l'application*

$$\pi : E \longrightarrow E/\mathcal{R}.$$

qui envoie x sur sa classe $\overline{x}$ est surjective, et la relation d'équivalence qui lui est associée est $\mathcal{R}$. De plus π vérifie la propriété universelle suivante :

1. *Pour tout ensemble F et toute application $f : E \longrightarrow F$ telle que $x\mathcal{R}x'$ implique $f(x) = f(x')$.*
2. *Pour tous x, x' dans E, il existe une unique application*

$$f' : E/\mathcal{R} \longrightarrow F$$

telle que $f = f' \circ \pi$.

L'application π est appelée surjection canonique.

Proposition 2.1.4 *Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Les classes d'équivalence forment une partition de l'ensemble E.*

Preuve. Comme pour tout $x \in E$ les classes d'équivalence sont toutes non vide et ont E pour réunion.
Soient x et y deux éléments de E. Supposons leur classes d'équivalence d'intersection non vide, i.e

$$\exists z \in \bar{x} \cap \bar{y}.$$

On a donc $x \ \mathcal{R} \ z$ et $y \ \mathcal{R} \ z$ (d'où $\mathcal{R} \ y$ par symétrie).
ceci implique que $x \ \mathcal{R} \ y$ (par transitivité) et donc $\bar{x} = \bar{y}$.On a montré que les classes d'équivalence de E sont non vide , deux à deux disjointes et ont E pour réunion. Elle forment donc une partition de l'ensemble E. ■

On va montrer qu'à tout sous-groupe F d'un groupe E est associée une relation d'équivalence $\mathcal{R}$ définie sur E. Si cette relation d'équivalence satisfait certaines conditions de compatibilité, la loi interne de E induit une loi interne sur l'ensemble des classes d'équivalence $E/\mathcal{R}$ qui munit cet ensemble d'une structure de groupe et la projection canonique $\pi : E \to E/\mathcal{R}$ est un morphisme de groupes. On montrera que inversement, à toute relation d'équivalence $\mathcal{R}$ définie sur un groupe E et satisfaisant les conditions de compatibilité, est associé un sous-groupe F de E tel que la relation $\mathcal{R}$ soit la relation associée au sous-groupe F.

Définition 2.1.5 *On dit que une relation $\mathcal{R}$ sur E est **compatible à droite** (respectivement à gauche) avec la loi de composition $*$ si*

$$\forall x, y, a \in E, \quad x\mathcal{R}y \Rightarrow (x * a)\mathcal{R}(y * a)$$

(respectivement :$x\mathcal{R}y \Rightarrow (a * x)\mathcal{R}(a * y)$)
On dira qu'une relation est compatible si elle est compatible à gauche et à droite.
La loi interne $*$ est dit compatible à la relation d'équivalence $\mathcal{R}$ si, pour tous $x, x', y, y' \in E$ on a :

$$x\mathcal{R}x' \quad et \quad y\mathcal{R}y' \Leftrightarrow (x * y)\mathcal{R}(x' * y').$$

Proposition 2.1.6 *Soient $\mathcal{R}$ une relation d'équivalence sur un ensemble E telle que $\pi : E \longrightarrow E/\mathcal{R}$ la surjection canonique, $*$ une loi de composition sur E. Les conditions suivantes sont équivalentes :*

1. *Pour tous $x, x', y, y' \in E$ on a :*

$$x\mathcal{R}x' \text{ et } y\mathcal{R}y' \Leftrightarrow x * y\mathcal{R}x' * y';$$

2. *Il existe une loi de composition*

$$\overline{*} : E/\mathcal{R}E/\mathcal{R} \longrightarrow E/\mathcal{R}$$

telle que pour tous $x, y \in E$ on a

$$\overline{x} \quad \overline{*} \quad \overline{y} = \overline{x * y}.$$

Lorsque les conditions équivalentes de la proposition sont vérifiées, on dit que la loi $*$ passe au quotient en une loi $\overline{*}$ induite sur $E/\mathcal{R}$.

Remarque 2.1.7 *Soient $*$ une loi sur un ensemble G et $\mathcal{R}$ une relation d'équivalence sur G qui sont compatibles. Soit $\overline{*}$ la loi induite sur $G/\mathcal{R}$.*
Il est clair que si la loi $*$ est associative (reps. commutative), alors $\overline{*}$ l'est aussi.
Si e est neutre pour $*$, alors son image $\overline{e}$ est neutre pour la loi induite $\overline{*}$ sur $E/\mathcal{R}$, tout élément de E admet un élément symétrique, il en est de même pour la loi induite sur $E/\mathcal{R}$.

On va maintenant étudier la situation où G est un groupe.

Proposition 2.1.8 *Soient G un groupe et une relation d'équivalence définie sur G, compatible avec la loi de G. Alors l'ensemble quotient $G/\mathcal{R}$, muni de la loi induite par la loi de G est un groupe.*

Exemple 2.1.9 *Pour tout $n \in \mathbb{N}^*$, l'addition de $\mathbb{Z}$ induit une structure de groupe sur $\mathbb{Z}/n\mathbb{Z}$*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n}\}$$

où p désigne la classe d'équivalence de p modulo n. Autrement dit

$$\overline{p} = \overline{q} \Leftrightarrow p = q(mod \ \ n)$$

ou encore $\overline{p} = \overline{q} \Leftrightarrow \exists k \in \mathbb{Z}, \ \ p = q + kn$. On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$\overline{p} + \overline{q} = \overline{p + q}$$

L'exemple de la vie courante est le suivant : considérons seulement les minutes d'une montre ; ces minutes varient de 0 à 59. Lorsque l'aiguille passe à 60, elle désigne aussi 0 (on ne s'occupe pas des heures). Ainsi de suite : 61 s'écrit aussi 1, 62 s'écrit aussi 2, ... Cela correspond donc à l'ensemble $\mathbb{Z}/60\mathbb{Z}$. On peut aussi additionner des minutes : 50 minutes plus 15 minutes font 65 minutes qui s'écrivent aussi 5 minutes. C'est le fait que l'addition soit bien définie, et on peut justifier que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif. C'est facile, l'élément neutre est $\overline{0}$. L'inverse de $\overline{k}$ est $\overline{-k} = \overline{n-k}$. L'associativité et la commutativité découlent de celles de $(\mathbb{Z}, +)$.

Théorème 2.1.10 *Soit G un groupe monogène.*

(1) Si G est fini d'ordre n (G est cyclique), G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

(2) Si G est d'ordre infini, G est isomorphe à $\mathbb{Z}$.

Preuve.

(1) Comme G est monogène et fini d'ordre n alors il est cyclique, ainsi

$$G = \{e, g, g^2, g^3, ..., g^{n-1}\}$$

et que $g^n = e$, le n est le plus petit entier positif tel que $g^n = e$.
Si $k \in \mathbb{Z}$ et $k = nq + r$ pour $0 \leq r < n$, alors $g^s = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r$.
On suppose que $0 < r < s < n$ et $g^r = g^s$, d'où $g^{h-k} = e$ et $0 < r - s < n$. ceci contredis le choix de n. Donc les éléments de G sont $g^0 = e, g, g^2, g^3, ..., g^{n-1}$.
Nous pouvons maintenant construire l'isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et G, soit l'application

$$\begin{array}{rccl} \Phi: & \mathbb{Z}/n\mathbb{Z} & \to & G \\ & \overline{r} & \mapsto & \Phi(\overline{r}) = g^r \end{array}$$

- Il faut tout d'abord montrer que Φ est bien définie.
Si $\overline{r} = \overline{r'}$ (une même classe définie par deux représentants distincts) alors $r \equiv r_1 (mod \ \ n)$ et donc il existe $k \in \mathbb{Z}$ tel que

$$r = r_1 + kn.$$

Ainsi

$$\Phi(\overline{r}) = g^r = g^{r_1+kn} = g^{r_1} g^{kn} = g^{r_1} \left(g^k\right)^n = g^{r_1}$$

Donc

$$\Phi(\overline{r}) = \Phi(\overline{r_1}).$$

Ainsi Φ est bien définie.
Il est clair que Φ est défini une injection et une surjection dans $\mathbb{Z}/n\mathbb{Z}$.
-Aussi :

$$\Phi(r + s) = g^{r+s} = g^r g^s = \Phi(r)\Phi(s).$$

D'où la propriété de homomorphisme est satisfaite et Φ est un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et G.

(2) Pour tout entier positif n, $g^n \neq e$. Dans ce cas, nous affirmons qu'aucun exposant distinct r et s ne peut donner des éléments égaux g^r et g^s de G.
On suppose que $g^r = g^s$ et $r > s$. Alors $g^{r-s} = e$. donc chaque élément de G peut être exprimé comme g^n pour un unique $n \in \mathbb{Z}$.
L'application $\Phi : \mathbb{Z} \to G$ donné par $\Phi(r) = g^r$ est donc défini une injection et une surjection dans $\mathbb{Z}$. Aussi :

$$\Phi(r + s) = g^{r+s} = g^r g^s = \Phi(r)\Phi(s).$$

D'où Φ est un isomorphisme entre $\mathbb{Z}$ et G.

■

Définition 2.1.11 *Soient G un groupe et H un sous-groupe de G ; soient de plus x et y des éléments de G. On dit que $x\ {}_H\mathcal{R}\ y$ si*

$$x^{-1}y \in H;$$

de même, on dit que $x\ \mathcal{R}_H\ y$ si

$$xy^{-1} \in H.$$

On dit aussi que x est congru à y modulo H (à gauche, respectivement à droite). Toutefois, cette dernière terminologie est plus souvent employée lorsque G est abélien.

$\mathcal{R}_H$ (respectivement ${}_H\mathcal{R}$) est une relation d'équivalence, et on a la propriété suivante

$$y\ \mathcal{R}_H\ x\ \Rightarrow y \in Hx \quad et \quad y\ {}_H\mathcal{R}\ x,\ \Rightarrow y \in xH$$

$$xH = \{xh,\ \ h \in H\},\quad pour\ \ x \in G, \tag{2.1}$$

$$(resp.\ \ Hx = \{hx,\ \ h \in H\}).$$

On peut montrer que la classe d'équivalence de x pour la relation $\mathcal{R}_H$ (resp. ${}_H\mathcal{R}$) est bien xH (resp. Hx). On raisonne comme suit.
Par définition, pour $y \in xH$, on a $h \in H$ tel que $y = xh$. Donc $x^{-1}y = h \in H$ et il s'ensuit que $x\ \mathcal{R}_H\ y$.
Réciproquement, soit $y\ \mathcal{R}_H\ x$, alors $h = x^{-1}y \in H$. Il existe donc $h \in H$ tel que $y\ \mathcal{R}_H\ x$, ce qui prouve l'affirmation. On dit que la classe d'équivalence xH (resp. Hx) est une classe à gauche (respectivement à droite) modulo H. On note G/H l'ensemble quotient résultant, c-à-d.

$$G/H = \{gH,\ \ g \in G\}$$

(respectivement $H \setminus G = \{Hg,\ \ g \in G\}$). Pour G noté additivement, on écrit $x + H$ pour la classe d'équivalence de x modulo H.

Proposition 2.1.12 *Soit G un groupe.*
1. Si H est un sous-groupe de G, la relation d'équivalence ${}_H\mathcal{R}$ (respectivement $\mathcal{R}_H$) est compatible à droite (respectivement à gauche) avec la loi de composition de G.
2. Si $\mathcal{R}$ est une relation d'équivalence définie sur G, compatible à droite (respectivement à gauche) avec la loi de composition de G, alors : Il existe un unique sous-groupe H de G tel que $R =_H R$ (respectivement $\mathcal{R} = \mathcal{R}_H$)

Preuve. On montrera pour $\mathcal{R}_H$ et pas pour ${}_H\mathcal{R}$.
1. Soit H un sous-groupe de G. On doit montrer que $\mathcal{R}_H$ est compatible à droite. Soient $x, y, a \in G$ tels que $x\mathcal{R}_H y$. L'hypothèse est équivalente à $xy^{-1} \in H$, on veut montrer que $(x*a)\mathcal{R}_H(y*a)$.

$$xy^{-1} \in H$$

donc

$$xy^{-1} = (xa)(a^{-1}y^{-1}) = (xa)(ya)^{-1} \in H$$

2. Soit $\mathcal{R}$ une relation sur G, compatible à droite. On pose $H = \overline{e_G}$ *modulo* $\mathcal{R}$.
H est un sous-ensemble non vide, montrons que H est un sous-groupe de G.
Soit $x, y \in H$,

$$x\mathcal{R}e \ \ et \ \ y\mathcal{R}e \ \ donc \ \ xy^{-1}\mathcal{R}y^{-1} \ \ et \ \ e\mathcal{R}y^{-1},$$

par transitivité de $\mathcal{R}$,

$$xy^{-1}\mathcal{R}e \Leftrightarrow xy^{-1} \in H,$$

donc H est bien un sous-groupe de G. Soit $x\mathcal{R}y$, montrons que $x\mathcal{R}_H y$.
Par compatibilité à droite : $xy^{-1}\mathcal{R}e$, ce qui équivaut à $xy^{-1} \in H$, ou encore $x\mathcal{R}_H y$.

$$\mathcal{R} \subseteq \mathcal{R}_H$$

Soit $x\mathcal{R}_H y$, alors $xy^{-1} \in H$, donc $xy^{-1}\mathcal{R}e$ d'où $x\mathcal{R}y$, par compatibilité de R. donc

$$\mathcal{R}_H \subseteq \mathcal{R}$$

■

Remarque 2.1.13 *Soit G un groupe abélien. Pour tout sous-groupe H de G,*

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

En particulier, $\dfrac{G}{H} =_H \left(\dfrac{G}{H}\right) = \left(\dfrac{G}{H}\right)_H$ *et la loi de composition sur G est compatible avec* $\mathcal{R}$.

Proposition 2.1.14 *Soit H un sous-groupe de G. Alors tout conjugue* gHg^{-1} *est également un sous-groupe de G.*

Preuve. Pour prouver que gHg^{-1} est un sous-groupe de G, on vérifie tout d'abord l'élément neutre de G est dans gHg^{-1}, puisque

$$geg^{-1} = e \in gHg^{-1}.$$

Si $a = gxg^{-1}$ et $b = gyg^{-1}$ sont dans gHg^{-1} alors

$$ab = (gxg^{-1})(gyg^{-1}) = g(xy)g^{-1} \in gHg^{-1}.$$

Finalement, pour tout $gxg^{-1} \in gHg^{-1}$,on voit ça

$$(gxg^{-1})^{-1} = (g^{-1})^{-1}x^{-1}g^{-1} = gx^{-1}g^{-1} \in gHg^{-1}.$$

Comme demandé gHg^{-1} est un sous-groupe de G. ■

Corollaire 2.1.15 *Soit G un groupe et H sous-groupe G, les ensembles quotients* G/H *et* $H\backslash G$ *sont en bijection.*
Pour tout $x \in H$*, toute classe à droite* Hx *et toute classe à gauche* xH *est un ensemble fini et même cardinal de H.*

Cette corollaire rend possible la définition suivante, pour tout H sous-groupe d'un groupe G. On dit du cardinal de l'ensemble quotient G/H (qui est égal au cardinal de $H \setminus G$) que c'est **l'indice** de H dans G. On le note

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

. Lorsque G/H est un ensemble fini, on dit que H est d'indice fini dans G. Par exemple, on a $|\mathbb{Z} : n\mathbb{Z}| = n$. L'indice peut donc être fini même si G et H sont infinis. Le théorème suivant permet de calculer l'indice.

Théorème 2.1.16 ***(Théorème de Lagrange).***
Soit G un groupe fini et H est un sous-groupe de G alors :

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

En particulier, l'ordre de tout sous-groupe de G divise l'ordre de G, et l'ordre de tout élément de G divise l'ordre de G.

Preuve. Comme $\mathcal{R}_H$ est une relation d'équivalence, et comme toutes les classes d'équivalences ont cardinal $|H|$, on a l'ensemble des classes d'équivalences G/H forme une partition de G d'après la proposition (2.1.4). On obtient alors

$$|G| = \sum_{xH \in G/H} |xH| = \sum_{xH \in G/H} |H| = |G/H||H| = |H| \ [G : H] .$$

Puisque l'ordre de $x \in G$ est l'ordre du sous-groupe $\langle x \rangle$, on obtient bien l'ordre de tout élément de G divise $|G|$ ■

Corollaire 2.1.17 *Pour G un groupe fini d'ordre n, alors $x^n = e$ pour tout $x \in G$. De plus, Si G est un groupe fini de cardinal premier, alors G est cyclique.*

Preuve. Soit $x \in G$, d'ordre d. Le théorème de Lagrange assure que d divise $|G| = n$. On a donc $k \in \mathbb{N}$ tel que $n = dk$, et on a donc

$$x^n = x^{dk} = (x^d)^k = e^k = e.$$

La preuve de la seconde partie est la suivante :
Soit $a \in G$, $a \neq e$. Comme $Ord(a)/|G|$ et comme $|G|$ est premier, soit $Ord(a) = |G|$ et donc $\langle a \rangle = G$ soit $Ord(a) = 1$. Mais alors, $\langle a \rangle = e$ et donc $a = a^1 = e$ ce que nous avons exclu. ■
On peut généraliser le théorème de Lagrange de la manière suivante :

Théorème 2.1.18 *Soit G un groupe fini et soient H, K deux sous-groupes de G tels que $K \subset H$. Alors,*

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

Preuve. Écrivons G et H comme des réunions disjointes de classes à gauches :

$$H = \bigcup_{1 \leq i \leq |H:K|} x_i K, \qquad G = \bigcup_{1 \leq j \leq |G:H|} y_j H.$$

On en déduit que

$$G = \bigcup_{1\leq i\leq |H:K|, 1\leq j\leq |G:H|} x_i y_j K.$$

Pour montrer le théorème, il suffit de montrer que cette réunion est disjointe.
Supposons donc que $abK = xyK$, ou a et x sont deux éléments du système de représentants de G/H que nous avons choisis : $\{y_1, ..., y_{|G:H|}\}$ et b, y sont de même deux éléments parmi les x_i. Pour démontrer le théorème, il suffit donc de voir que $a = x$ et $b = y$. On a donc :

$$x^{-1}abK = yK;$$

notons que $y \in H$. Donc, comme $K \subset H$, $yK \subset H$. De même, $bK \subset H$.
Par conséquent,

$$x^{-1}a \in H;$$

Donc, $a_H \mathcal{R} x$. Comme ils sont choisis parmi un système de représentants de G/H, $a = x$. Le même raisonnement montre maintenant que $y^{-1}b \in K$ et par suite y et b sont dans la même classe modulo K. Ils sont donc égaux.
Alors

$$G = \bigcup_{1\leq i\leq |H:K|, 1\leq j\leq |G:H|} x_i y_j K \Rightarrow |G| = |H : K| \cdot |G : H||K|.$$

D'après le théorème de Lagrange on a

$$|G| = |G : K| \cdot |K|,$$

$$|G : K| \cdot |K| = |H : K| \cdot |G : H||K|,$$

$$|G : K| = |H : K| \cdot |G : H|.$$

■

2.2 Notion de sous-groupes normaux

Le sous-groupe H est distingué dans G si et seulement si toute classe à gauche modulo H est une classe à droite. Lorsque H est un sous-groupe distingué, on sait mettre une structure de groupe sur l'ensemble des classes. Un sous-groupe distingué sera aussi appelé sous-groupe normal.

Définition 2.2.1 *Soit G un groupe, un sous-groupe N de G, est dit normal (ou distingué) si* ${}_N\mathcal{R} = \mathcal{R}_N$. *c'est-à-dire, si pour tout* $x \in G$, $Nx = xN \Leftrightarrow x^{-1}Nx = N$.*i.e.*

$$\forall x \in N \ \ et \ \ \forall g \in G \ \ alors \ \ gxg^{-1} \in N$$

On note alors $N \lhd G$.

Remarque 2.2.2 *Dans n'importe quel groupe G,* $\{e\}$ *et G sont des sous-groupes normaux de G.*

Définition 2.2.3 *On dit qu'un groupe G est simple si les seuls sous-groupes distingué de G sont $\{e\}$ et lui même.*

Exemple 2.2.4 *Si G est abélien, tout sous-groupe est distingué.*

Proposition 2.2.5 *Le sous-groupe H est distingué dans G si et seulement si toute classe à gauche modulo H est une classe à droite.*

Lorsque H est un sous-groupe distingué, on sait mettre une structure de groupe sur l'ensemble des classes.

2.3 Théorèmes fondamentaux des isomorphismes

Théorème 2.3.1 ***Théorème fondamental des homomorphismes*** *Soit $h : G \to H$ un homomorphisme et soit $f : G \to K$ un épimorphisme.*

$$\begin{array}{ccc} G & \to & H \\ {\scriptstyle f}\ \searrow & \nearrow & {\scriptstyle \exists ? g} \\ & K & \end{array}$$

(i) Il existe un homomorphisme $g : K \to H$ tel que $g \circ f = h$ si et seulement si

$$Ker(f) \subset Ker(h)w.$$

(ii) Si un tel homomorphisme g existe, il est unique.
(iii) On a $Im(g) = Im(h)$, donc g est un épimorphisme si et seulement si h est un épimorphisme. (iv) On a $f(Ker(h)) = Ker(g)$, donc g est un monomorphisme si et seulement si

$$Ker(f) = Ker(h).$$

Théorème 2.3.2 ***Premier théorème d'isomorphisme***
Soient G et G' des groupes. Soit $f : G \longrightarrow G'$ un homomorphisme de groupe.
Rappelons que $Kerf$ est un sous-groupe distingué de G et donc que $G/Kerf$ a une structure de groupe pour la loi induite de celle de G.
Rappelons aussi que l'on a un morphisme surjectif

$$\Pi : G \longrightarrow G/Kerf$$

qui a tout élément de G associe sa classe d'équivalence dans $G/Kerf$.
Ajoutons encore que l'image d'un groupe par un morphisme est un sous-groupe du groupe image. On peut alors affirmer qu'il existe un isomorphisme

$$\overline{f} : G/Kerf \longrightarrow Imf$$

tel que

$$\overline{f} \circ \Pi = \Pi \circ f.$$

Preuve. Posons $H = Kerf$.
Construisons tout d'abord $\overline{f}$. Posons, si $\overline{x} \in G/H$, $\overline{f}(\overline{x}) = f(x)$ où x est un représentant de la classe d'équivalence $\overline{x}$. $\overline{f}$ est bien définie car si y est un autre représentant de la classe d'équivalence associée à x, alors

$$\overline{f}(\overline{y}) = f(y) = f(x.x^{-1}.y) = f(x).f(x^{-1}.y).$$

Cette dernière égalité est vraie car f est un morphisme et x et y étant équivalents dans G/H, $x.y^{-1}$ est élément de Ker f. Donc $f(y) = f(x)$ et $\overline{f}$ est bien définie.
$\overline{f}$ est bien ,par définition ,un homomorphisme de groupe.
Montrons que $\overline{f}$ est injective. Soient $\overline{x}$, $\overline{y} \in G/H$. Supposons que

$$\overline{f}(\overline{x}) = \overline{f}(\overline{y})$$

alors par définition de $\overline{f}$, on a :
$f(x) = f(y)$ donc $f(x).f(y)^{-1} = e_{G'}$
et comme f est un homomorphisme, $f(x.y^{-1}) = e_{G'}$.
Ce qui implique que $x.y^{-1} \in Kerf$ et donc que $\overline{x} = \overline{y}$. Ceci prouve l'injectivité de $\overline{f}$.
Comme une application est surjective sur son image $\overline{f}$ est un isomorphisme de G/H dans Im f.
Enfin par définition de $\overline{f}$ on a bien $\overline{f} \circ \Pi = \Pi \circ f$. ■

Théorème 2.3.3 ***(Deuxième théorème d'isomorphisme)***
Soient H et K deux sou groupes d'un groupe G. On suppose que H est normal dans G. Alors :

(i) $HK = \{x \in G, x = hk, h \in H, k \in K\}$ est un sous-groupe de G.

(ii) $H \cap K$ est normal dans K et

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

Preuve.

(i) Montrons tout d'abord que HK est un sous-groupe de G pour la loi induite de celle de G.
L'élément neutre de G est naturellement élément de HK.
Et si $g_1 = h_1k_1$, $g_2 = h_2k_2$ sont des éléments de HK alors $h_1, h_2 \in H$ et $k_1, k_2 \in K$,

$$g_1g_2 = (h_1k_1)(h_2k_2) = h_1k_1(h_2k_2h_2^{-1})h_2$$

Comme K est un sous-groupe normal de G, le terme entre parenthèses appartient à K.
On a donc :

$$x = k_1(h_2k_2h_2^{-1}) \in K$$

et

$$g_1g_2 == h_1xh_2 = (h_1h_2)(h_2^{-1}xh_2).$$

Donc g_1g_2 est bien un élément de HK par normalité de K.
Maintenant, soient $h \in H$ et $k \in K$, l'inverse de $g = hk$ est $g^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1})$ qui est dans HK.

(ii) H∩K étant normal dans K (voir la proposition ...), K/(K∩H) a une structure de groupe pour la loi induite de celle de K.

Montrons que ce groupe est isomorphe à HK/H. Définissons pour cela l'application

$$\theta : HK \to H/K \cap H$$

par si g=h.k est élément de HK, $\theta(g) = \overline{k}$ où $\overline{k}$ désigne la classe d'équivalence de k dans $H/K \cap H$.

Cette application est bien définie car si g est aussi représenté par le produit h'.k' de HK alors h.k=h'.k' et k.k'$^{-1}$=h^{-1}.h'.

Le produit du second membre de l'égalité est élément de H et le produit du premier membre élément de K. On en déduit que $k(k')^{-1}$ est élément de $H \cap K$. Donc

$$\overline{k(k')^{-1}} = e_{H/H\cap K} \quad et \quad \theta(g) = \overline{k} = \overline{k'}.$$

Comme $K \cap H$ est un sous-groupe normal de K alors l'application θ (qui à un élément de HK associe sa classe d'équivalence...) est un homomorphisme de groupe.

Calculons alors Ker(θ). Soit g=h.k$\in HK$ tel que

$$\theta(g) = \overline{k} = \overline{e_{H/H\cap K}}.$$

k est donc élément de $H \cap K$.

Par conséquent g est un produit de deux éléments de K et est élément de K. On vient d'établir Kerθ $\subset$K. Prenons un élément k de K. Par définition de θ, θ(k)= $e_{H/H\cap K}$.

Ceci prouve l'inclusion réciproque. En conclusion : Kerθ=K.

θ est surjective. En effet, si $\overline{h}$ est élément de $H/H \cap K$ alors θ(h)= $\overline{h}$.

Appliquons enfin le premier théorème d'isomorphisme à

$$\theta : \frac{HK}{H} \simeq \frac{H}{H \cap K}.$$

■

Théorème 2.3.4 ***(Troisième théorème d'isomorphisme)***
Soient G un groupe, H et K deux sous-groupes normaux de G. On suppose de plus que $H \subset K$. Alors :

(i) le sous-groupe H est normal dans K et K/H est un sous-groupe normal de G/K.
(ii) Le quotient $(G/H)/(K/H)$ est isomorphe à G/K.

Preuve.

(i) Comme H est normal dans G, il l'est dans K.

Soit g un élément de G. Notons $\overline{x}$ sa classe d'équivalence dans G/H et $\overline{\overline{x}}$ sa classe d'équivalence dans G/K.

Montrons que K/H $\triangleleft$G/H. Pour cela choisissons un élément $\overline{g}$ dans G/H et une élément $\overline{k}$ dans K/H. Alors $\overline{g}.\overline{k}.\overline{g}^{-1} = \overline{g.k.g^{-1}}$. Mais K étant normal dans G, il existe k'$\in$ K tel que ce dernier élément soit égal à $\overline{k'}$;

(ii) Soit

$$\theta : G/H \to G/K$$

l'application qui à un élément $\overline{k}$ de G/H associe l'élément $\overline{\overline{g}}$ de G/K.

θ est bien définie et est un morphisme du groupe G/H dans le groupe G/K.

De plus, H étant inclue dans K, θ est surjective.

On peut alors appliquer le premier théorème d'isomorphisme. Ceci nous permet d'affirmer que

$$\frac{G/H}{K/H} \simeq G/K.$$

■

CHAPITRE 3

THÉORÈMES DE SYLOW ET SES APPLICATIONS

La notion suivante est fondamentale ; d'une part les groupes apparaissent naturellement dans la plupart des problèmes à travers leurs actions (ou représentations) et d'autre part, pour étudier les groupes eux-mêmes, on verra qu'il est souvent avantageux de les faire agir.

3.1 Action de Groupes

Dans cette partie, on donne la définition usuelle d'action de groupe qu'on illustre par l'exemple de l'action par translation à gauche.

Définition 3.1.1 *Soient X un ensemble et G un groupe. On dit que G* ***opère à gauche*** *sur X si on a une application : $* : GX \to X$ $(g, x) \to g * x$, vérifiant :*

(1) $(g_1 g_2) * x = g_1 * (g_2 * x)$ pour tout $x \in X$ et tous $g_1, g_2 \in G$.

(2) $e * x = x$ pour tout $x \in X$.

Une telle application est aussi appelée ***action à gauche*** *de G sur X :*

On appelle cette application loi de composition externe. On définit de façon analogue **l'action à droite** d'un groupe sur un ensemble. C'est la donnée d'une application $* : XG \to X$ $(x, g) \to x * g$ vérifiant :

(1) $x * (g_1 g_2) = (x * g_1) * (g_2)$ pour tout $x \in X$ et tous $g_1, g_2 \in G$.

(2) $x * e = x$ pour tout $x \in X$.

Mais si l'on s'est donné une action à droite, on en déduit une action à gauche de G sur X en posant $g * x = x * g$; cela permet de ramener l'étude des actions à droite à celle des actions à gauche (et réciproquement). Donc, chaque résultat que nous démontrerons sur les actions à

gauche aura un analogue pour les actions à droite.
Dans tout ce qui suit, on ne parlera ici que des actions à gauche quand on dira que G agit sur X et on notera de la même manière $*$ et $\cdot$ par $\cdot$ sans faire de différence (de notation) entre la loi interne et externe. on entendra par G **agissant sur** X, l'action à gauche de G sur X .

On va énoncer ici plusieurs exemples d'actions de groupes.

Exemple 3.1.2 *Un exemple fondamental est l'action d'un groupe sur lui-même ; l'action est en fait simplement la loi du groupe. Il est clair que les conditions sont vérifiées.*

(1) Soit G un groupe et soit l'application
$* : GG \to G$
$(g, x) \to g * x = gx.$
Il est facile de voir que l'application $*$ est bien définie. De plus, pour tous $g_1, g_2, x \in G$, on a :

(i) $(g_1g_2) * x = (g_1g_2)x = g_1(g_2x) = g_1 * (g_2x) = g_1 * g_2 * x.$

(ii) $e * x = ex = x$

*Donc $*$ définit une action de G sur lui-même appelée action par **translations** à gauche.*

(2) Soit G un groupe et soit l'application
$* : GG \to G$
$(g, x) \to g * x = gxg^{-1}.$
Il est facile de voir que l'application $*$ est bien définie. De plus, pour tous $g_1, g_2, x \in G$, on a :

(i) $(g_1g_2) * x = (g_1g_2)x(g_1g_2)^{-1} = (g_1g_2)x((g_2^{-1}g_1^{-1})) = g_1(g_2xg_2^{-1}) = g_1 * (g_2xg_2^{-1}) = g_1 * (g_2 * x).$

(ii) $e * x = exe^{-1} = exe = x.$

*Donc $*$ définit une action de G sur lui-même appelée action par **conjugaison**.*

(3) Soit $\mathbb{V}$ un espace vectoriel sur un corps $\mathbb{K}$. Le groupe multiplicatif $\mathbb{K}^*$ agissant sur l'ensemble $\mathbb{V}$ suivant l'application :
$* : \mathbb{K}^*\mathbb{V} \to \mathbb{V}$
$(\lambda, v) \to \lambda * v = \lambda v$
qui est la restriction de la loi externe de $\mathbb{KV}$ à $\mathbb{K}^*\mathbb{V}$. Donc $*$ est bien définie. De plus, pour tous $\alpha, \beta \in \mathbb{K}^*$ et $v \in \mathbb{V}$ on a :

(i) $(\alpha\beta) * v = (\alpha\beta)v = \alpha * (\beta v) = \alpha * (\beta * v).$

(ii) $1 * v = 1v = v.$

On montre dans la partie suivante qu'on peut transformer la définition d'action précédante pour obtenir une définition d'action de groupe en terme de morphisme de groupes. Cette définition ayant l'avantage d'être plus simple à manipuler car on sait manipuler les morphismes de groupes, par exemple, les restreindre ou les passer au quotient.

Proposition 3.1.3 *Soit G un groupe opérant sur un ensemble X. On a les propriétés suivantes :*
1. Pour $g \in G$ fixé, on considère l'application :

$$\begin{array}{rccc} \alpha_g : & X & \to & X \\ & x & \mapsto & gx \end{array}$$

qui est une permutation de X.
2. L'application

$$\begin{array}{rccc} \alpha : & G & \to & S_X \\ & g & \mapsto & \alpha_g \end{array}$$

est un morphisme de groupes. Son noyau $ker(\alpha)$ est alors appelé noyau de l'action de G sur X.

Preuve. 1. Montrons que c'est une application bijective, dans ce langage, l'axiome (1) est synonyme de $\alpha_{1_G} = id_X$ et l'axiome (2) est synonyme de $\alpha_g \circ \alpha_{g'} = \alpha_{gg'}$ pour tous $g, g' \in G$. On en déduit alors que α_g est une bijection de X dans lui-même d'inverse $\alpha_{g^{-1}}$ puisque

$$\alpha_g \circ \alpha_{g^{-1}} = \alpha_{gg^{-1}} = \alpha_{1_G} = id_X \quad et \quad \alpha_{g^{-1}} \circ \alpha_g = \alpha_{g^{-1}g} = \alpha_{1_G} = id_X.$$

c'est-à-dire que l'application $\alpha_g \in S_X$ L'application

$$\begin{array}{rccc} \alpha : & G & \to & S_X \\ & g & \mapsto & \alpha_g \end{array}$$

est un morphisme de groupes puisque $\alpha_g \circ \alpha_{g'} = \alpha_g \circ \alpha_{g'} = \alpha_{gg'}$ pour tous $g, g' \in G$. Ainsi, à partir de l'action de groupe, on a construit un morphisme de groupes de G dans S_X. On dit que α est le morphisme associé à l'action de groupe.

■

On peut donc associer à toute action de groupe G sur X un morphisme $\alpha \in Hom(G, S_X)$. Le noyau de l'action est le noyau du morphisme de groupe α. On s'intéresse à présent à la construction en sens inverse, un tel morphisme α définit une action à gauche de G sur X avec :

$$g \cdot x = \alpha(g)(x)$$

Proposition 3.1.4 *Soit $\alpha \in Hom(G, S_X)$, on peut lui associer une loi de composition externe sur X, qui construire une action de groupe :*

$$\begin{array}{rccc} * : & GX & \to & X \\ & (g, x) & \mapsto & g * x = \alpha(g)(x) \end{array}$$

Preuve. Montrons que $*$ est une action de G sur X. Il s'agit de montrer que $*$ vérifie les axiomes (1) et (2) de la définition précédante. En effet,
Soient $g_1; g_2 \in G$, alors : $\alpha(g_1g_2) = \alpha(g_1) \circ \alpha(g_2)$
Soit $x \in X$,

$$(g_1g_2) * x = \alpha(g_1g_2)(x) = \alpha(g_1) \circ \alpha(g_2)(x) = \alpha(g_1)(\alpha(g_2)(x)) = g_1 * (g_2 * x)$$

Donc l'axiome (1) est vérifié.
Comme α est un morphisme de groupe, on a $\alpha(1_G) = 1_{S_X} = id_X$. Si $x \in X$; $1_G * x = \alpha(1_G)(x) = id_X(x) = x$ et l'axiome (2) est vérifié. ■
On peut vérifier que le passage d'action à morphisme de groupes et de morphisme de groupes à action sont bien inverses l'un de l'autre c'est-à-dire que l'action associée au morphisme associé à une action $*$ n'est autre que $*$ et que le morphisme associé à l'action associée au morphisme α n'est autre que α. Finalement, la morale de tout ceci se résume par « se donner une action de groupe de G sur X, c'est la même chose que de se donner un morphisme de groupes de G dans S_X ».

Exemple 3.1.5 *Soit X un ensemble. On peut toujours définir une action de G sur X de façon triviale. Précisément, on considère le morphisme de groupes $\alpha : G \to S_X$ tel que $\alpha(g) = id_X$ pour tout $g \in G$. En suivant le principe de les deux propositions précédentes, on en déduit que G agit sur X. L'action ainsi construite est donnée par*

$$\begin{array}{rccc} * : & GX & \to & X \\ & (g,x) & \mapsto & g * x = x \end{array} .$$

*On dit que c'est l'action **triviale** de G sur X.*

Exemple 3.1.6 *Si le groupe G agit sur lui même par conjugaison :$(g,h) \mapsto ghg^{-1}$, le morphisme de groupes correspondant de $(G,\cdot)$ dans $(S_G,\circ)$ est noté : $Ad_g : G \to G, h \mapsto ghg^{-1}$. L'image de Ad est le groupe $Int(G)$ des automorphismes intérieurs de G.*

La prochaine étape de notre cheminement consiste à faire agir G sur G/H. Pour ce faire, on exploite l'action de G sur lui-même translations à gauche $GG \to G$ avec $g * h \to gh$. Plus généralement, on considère $X = p(G)$ c'est-à-dire l'ensemble des parties de G. On a alors l'action de $Gp(G) \to p(G)$, avec $g \cdot X = gX = \{gx \quad x \in X\}$.
Si $X = H$ est un sous-groupe de G, on a la définition suivante :

Définition 3.1.7 *Soit H un sous-groupe de G, alors G opère par translation à gauche sur l'ensemble $(G/H)_g$: les classes d'équivalence à gauche modulo H.*

$$\begin{array}{rccc} G\,(G/H)_g & \to & (G/H)_g \\ (g,xH) & \mapsto & gxH \end{array} .$$

Cette définition a un sens car, si on vérifie l'indépendance des choix : soient $x, y \in G$ tels que $xH = yH$ Alors $xH = yH \Rightarrow y^{-1}x \in H$. Montrons que $gxH = gyH$. $(gy)^{-1}gxH = y^{-1}g^{-1}gxH = y^{-1}xH = H$ Donc $gxH = gyH$.
Nous sommes maintenant presque prêts à aborder la classification des actions de groupes.

3.2 Orbites et stabilisateurs

On peut poursuivre ce genre de constructions les notions de stabilisateurs, d'orbites, et plusieurs autres concepts de la théorie des groupes y jouent un rôle fondamental.

Définition 3.2.1 *Soient G un groupe agissant sur un ensemble X et $x \in X$.*

*(1) L'ensemble $G(x) = \{g(x), g \in G\}$ est un sous-ensemble de X appelé **l'orbite** de x.*

(2) Une action est dite transitive si elle n'a qu'une seule orbite, c'est-à-dire si $G(x) = X$ pour tout x dans X.

*(3) On vérifie que l'ensemble $G_x = \{g \in G, g(x) = x\}$ est appelé sous-groupe **d'isotropie** ou **stabilisateur** de x.*

Proposition 3.2.2 *Pour tout groupe G agissant sur un ensemble X et $\forall x \in X$, le stabilisateur G_x est un sous-groupe de G.*

Preuve. La condition (1) garantit que l'élément d'identité de G est dans G_x.
Si $g_1 g_2 \in G_x$ de sorte que

$$g_1 x = x = g_2 x,$$

alors la condition (2) garantit que

$$(g_1 g_2) * x = g_1 * (g_2 * x) = g_1 * x = x.$$

De sorte que $g_1 g_2 \in G_x$. On a aussi si $g \in G_x$, $g * x = x$ .Donc

$$g^{-1} * x = g^{-1} * (g * x) = (g^{-1} * g) * x = e_G * x = x.$$

Alors $g^{-1} \in G_x$ donc G_x est un sous-groupe de G. ■
la proposition suivante ouvre la porte à la description de toutes les actions de groupes. Elle suggère aussi que la compréhension des orbites est importante.

Proposition 3.2.3 *Soit G un groupe agissant sur un ensemble X, et $x \in X$, alors la relation « l'élément x est dans l'orbite de l'élément y » est une relation d'équivalence sur X. En conséquence, X est la réunion disjointe des orbites.*

On relie l'étude des orbites à l'étude des stabilisateurs via la proposition suivante. De plus la proposition révèle un lien important entre stabilisateurs d'éléments qui se trouvent dans une même orbite. Cela nous sera fort utile pour comprendre les actions transitives.

Proposition 3.2.4 *Pour tout groupe G opérant sur un ensemble X, et $x \in X$, on a les propriétés suivantes.*
1. Il y a une bijection entre $Orb(x)$ et les classes à gauche de $Stab(x)$. En particulier, si $Orb(x)$ est fini, alors $Stab(x)$ est d'indice fini et

$$|Orb(x)| = [G : Stab(x)]\,.$$

2. Si $Orb(x) = Orb(y)$, alors $Stab(x)$ et $Stab(y)$ sont conjugués.

Lemme 3.2.5 *Toute G-orbite est réunion disjointe de H-orbites.*

Preuve. Soit x un élément de X. Il est clair que $H(x) \subset G(x)$; on peut donc définir sur $G(x)$ une relation d'équivalence en posant, pour tous $y_1, y_2 \in G(x)$, $y_1 R y_2$ si et seulement s'il existe $h \in H$ tel que $h(y1) = y2$. Cette relation d'équivalence induit une partition de $G(x)$ et les classes d'équivalence sont des H-orbites. ■

Définition 3.2.6 *Soit G un groupe agissant sur un ensemble X et soit g un élément de G. L' ensemble des points fixes de g est $X^g = \{x \in G, g(x) = x\}$.*

Théorème 3.2.7 ***(Formule de Burnside)***
Soient G un groupe fini agissant sur un ensemble fini X et N le nombre d'orbites de l'action, alors :

$$N = \frac{1}{\mid G \mid} \sum_{g \in G} \mid X^g \mid$$

Le nombre d'orbites est donc égal au nombre moyen de points fixes de g lorsque g parcourt le groupe G.

Preuve. Considérons l'ensemble
$S = \{(g, x) \in GX, g(x) = x\}$
Nous allons évaluer $Card(S)$ de deux manières différentes :

(i) $Card(S) = \sum_{g \in G} Card(\{x \in X, g(x) = x\}) = \sum_{g \in G} |X^g|$

(ii) $Card(S) = \sum_{x \in X} Card(\{g \in G, g(x) = x\}) = \sum_{x \in X} |G_x|$

Soient $X_1, ..., X_N$ les N orbites de l'action et choisissons des représentants $x_1, ..., X_N$ de chaque orbite. Pour $i = 1, ..., N$ si $x \in X_i$, on obtient
$|G_x| = |G|/|G(x)| = |G|/|G(x_i)|$ car $G(x) = G(x_i)$.
L'égalité (ii) devient $Card(S) = \sum_{i=1}^{N} \sum_{x \in X_i} |G_x| = |G| \sum_{i=1}^{N} \sum_{x \in X_i} 1/|G(x_i)| = |G|N$ ■

Définition 3.2.8 *Soit G un groupe. **Le centre** $Z(G)$ du groupe G est l'ensemble :*
$Z(G) = \{g \in G, gx = xg\}$ *pour tout $x \in G$.*
C'est donc le sous-ensemble des éléments de G qui commutent avec tous les éléments de G.

Exemple 3.2.9 *Soit $\mathbb{K}$ un corp et soit*

$$H(\mathbb{K}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} ; a, b, c \in \mathbb{K} \right\}$$

Le groupe de Heisenberg sur $\mathbb{K}$ muni du produit usuel des matrices.
On suppose que la matrice

$M = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in Z(H)$ *et soit* $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ *un élément de* $H(\mathbb{K})$.

Puisque M *est dans le centre,on a* $AM = MA$, *alors*

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

aprés la calcul de produit, on trouve $az = cx$,*cette égalité doit etre vraie pour tout* $a, c \in \mathbb{K}$.
On prend $x = z = 0$ *et* $a = 0, c = 1$ *(Notons que depuis* $\mathbb{K}$ *est un corp donc* $0, 1 \in \mathbb{K}$ *).*
Donc la matrice M *devient* $M = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *.Il ressort clairement du calcul de* $AM = MA$ *que cette matrice est au centre pour tout* y. *Par conséquence nous avon déterminer le centre de groupe de heisenberg* $Z(H(\mathbb{K})) = \left\{ \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ; \forall y \in \mathbb{K} \right\}$.

On peut monter aussi que le centre $Z(H(\mathbb{K}))$ *est isomorphe au groupe* $\mathbb{K}$.
Considérons l'application $\phi : Z(H(\mathbb{K})) \to \mathbb{K}$ *qui envoie* $M = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in Z(H(\mathbb{K}))$ *à* $y \in \mathbb{K}$.
Nous prouvons que l'application ϕ *est isomorphisme de groupes.*
Soient $M = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *et* $M' = \begin{pmatrix} 1 & 0 & y' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *deux éléments quelconques dans le centre* $Z(H(\mathbb{K}))$ *et on a :*
$MM' = \begin{pmatrix} 1 & 0 & y+y' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.*Par conséquence nous avons* $\phi(M + M') = y + y' = \phi(M) + \phi(M')$.
Ainsi ϕ *est un homomorphisme de groupe.*
Par la définition de ϕ,*il est claire que cette homomorphisme est injectif et surjectif; et par conséquent* ϕ *est un isomorphisme de groupe.*
Donc le centre $Z(H(\mathbb{K}))$ *de groupe de heisenberg est isomorphe à le groupe* $\mathbb{K}$

Définition 3.2.10 *Soient* G *un groupe et* x *un élément de* G. ***Le centralisateur*** *de* x *dans* G *est* $C_G(x) = \{g \in G, gx = xg\}$.

On notera aussi que le centralisateur de x est le stabilisateur de x lorsque G opère sur lui même par conjugaison.

Proposition 3.2.11 *Le groupe* $Int(G)$ *des automorphismes intérieurs de* G *est isomorphe au groupe quotient* $G/Z(G)$ *; où* $Z(G)$ *est le centre de* G.

Preuve. Le noyau du morphisme de groupes $Ad : G \to S_G$ est formé des $g \in G$ tels que $Ad_g = Id_G$; c'est-à-dire des $g \in G$ tels que $ghg^{-1} = h$ pour tout $h \in G$; ce qui équivaut à $gh = hg$

pour tout $h \in G$. Le noyau de Ad est donc le centre $Z(G)$ de G : Comme $Im(Ad) = Int(G)$; on en déduit que $G/Z(G) = G/ker(Ad)$ est isomorphe à $Im(Ad) = Int(G)$. ■

3.3 Théorèmes de Sylow et ses applications

Définition 3.3.1 *Soit G un groupe d'ordre $p^m k$ où p est un nombre premier ne divisant pas k. Un p-**sous-groupe de Sylow** H de G est un sous-groupe de G d'ordre p^m. On dit aussi plus brièvement que H est un p-**Sylow de** G.*

Définition 3.3.2 *Soit p un nombre premier. On dit que G est un p-**groupe** si G est un groupe dont le cardinal est une puissance de p. De même, pour un p sous-groupe. Enfin, on dit qu'un sous-groupe H de G est un ı un sous-groupe de Sylow si $|H| = p^{\upsilon_p(|G|)}$ Où $\upsilon_p(|G|)$ est l'unique entier tel que $|G| = p^{\upsilon_p(|G|)}m$ avec p ne divisant pas m.*

Théorème 3.3.3 *Soit G un groupe fini ; alors pour tout nombre premier p divisant $|G|$, il existe un p sous-groupe de Sylow de G.*

Preuve. nous allons procéder par récurrence sur $|G|$ (notons aussi qu'il n'y a rien à démontrer si $|G|$ est une puissance d'un nombre premier). Supposons le théorème vrai pour tout groupe de cardinal $< n$ (pour $n \geq 2$) et soit G de cardinal n. ■ Nous allons provisoirement admettre le lemme suivant :

Lemme 3.3.4 *Soit G un groupe abélien et p un nombre premier divisant $n = |G|$. Alors, il existe un sous-groupe H de G d'ordre exactement p.*

Soit H un sous-groupe strict de G (il en existe puisqu'il suffit de prendre par exemple $H = \{e\}$). Si $Pgcd(|G : H|, n) = 1$, tout sous-groupe de Sylow de H est un sous-groupe de Sylow de G, ce qui permet de conclure par l'hypothése de récurrence. On peut donc supposer que $p||G : H|$ pour tout sous-groupe strict H de G.
Faisons opérer G sur lui-meme par conjugaison. La formule des classes nous donne :

$$|G| = |Z_G| + \sum_{i \in I} |G : G_i|$$

ou Z_G est le centre de G et les G_i sont différents de G. Par hypothèse,

$$p||G : G_i|$$

puisque G_i est un sous-groupe strict de G pour tout $i \in I$ (dire que $G_i = G$ revient à dire que l'orbite associée à cette classe de conjugaison est réduite à un seul élément, c'est-à-dire que ce point appartient au centre Z_G de G, ce que nous avons exclu). Comme p divise aussi $|G|$, on en déduit que $p||Z_G|$. Soit donc $a \in Z_G$ un élément de Z_G d'ordre exactement p (il en existe au moins un par le lemme précédent). Posons alors $H =< a >$. Le sous-groupe H est distingué dans G puisqu'il est contenu dans Z_G. Considérons la projection

$$\pi : G \to G/H$$

par hypothèse de récurrence, G/H contient un p-Sylow K'. Posons $K = \pi^{-1}(K')$. Comme a est d'ordre p, le cardinal de K' est

$$p^{\upsilon_p(|G/H|)} = p^{\upsilon_p(|G|)-\upsilon_p(o(a))} = p^{\upsilon_p(|G|)-1}.$$

Par le théorème de factorisation, la projection

$$K \stackrel{\pi}{\to} K'$$

se factorise à travers K/H , et l'on a une bijection

$$\tilde{\pi} : K/H \simeq K'.$$

Donc, le cardinal de K vaut

$$|K| = |K'|.p = p^{\upsilon_p(|G|)}.$$

Donc, K est un p-Sylow de G.

Lemme 3.3.5 *Soit H un p-groupe agissant sur un ensemble fini X. Alors,*

(1) le nombres de points fixes de l'action est $\equiv |X| mod(p)$;

(2) si l'action de H a exactement un point fixe, alors $|X| \equiv 1 mod(p)$;

(3) si $p||X|$, le nombre de points fixes de l'action est divisible par p.

Preuve. bien entendu, les points (2) et (3) découlent de (1).
Soit I un système de représentants des orbites de X non triviales sous l'action définie par H. La formule des classes s'écrit :

$$|X| = |\{\text{points fixes}\}| + \sum_{i\in I} |H : H_i| = |\{\text{points fixes}\}| + p(\star),$$

en effet, puisque H est un p-groupe, $|H : H_i|$ est un multiple de p sauf si $H_i = H$, ce que l'on a exclu puisque l'on a mis séparément les points fixes. D'où le point (1) et par suite le lemme.

■

Théorème 3.3.6 *Soit G un groupe fini, et p un nombre premier divisant $|G|$.Alors :*

(1) si H est un p sous-groupe de G, il est contenu dans un p-sous-groupe de Sylow de G ;

(2) tous les p-Sylow sont conjugué

(3) le nombre de p-Sylow est un diviseur de $|G|$. De plus, il est $\equiv 1 mod(p)$.

Preuve. montrons tout d'abord (1). Soit H un p sous-groupe de G et P un p-Sylow. Nous allons tout d'abord supposer que $H \subset N_P$. En particulier, $HP \subset N_P$, nous savons que

$$|HP : P| = |H : H \cap P|.$$

Si $H \nsubseteq P$, $|HP : P| \neq 1$ et donc, la formule ci-dessus montre que l'ordre de HP est une puissance de p, strictement supérieure à $|P|$ ce qui contredit le fait que P est un p-Sylow. Donc, $HP = P$ et par suite, $H \subset P$.
Nous allons maintenant montrer que l'on peut se ramener au cas $H \subset N_P$. Considérons l'ensemble : $S = \{\text{conjugués de} P\}$.
Le groupe G agissant sur S par conjugaison, et, par restriction à H de cette action, H agissant sur S. Notons que le cardinal de S est exactement

$$|G : N_P|.$$

Comme $P \subset N_P$, on a donc $pgcd(|S|, p) = 1$ et donc, par le lemme précédent, l'action de H sur S admet au moins un point fixe, disons Q. Notons que puisque Q est un conjugué de P, c'est aussi un p-Sylow de G. Puisque Q est fixé par l'action de H, on a :

$$\forall h \in H, \forall x \in Q, hxh^{-1} \in Q.$$

Ceci revient à dire que $H \subset NQ$. Par la première partie de la preuve, on en déduit donc que $H \subset Q$ Ceci démontre le point (1), mais aussi le point (2), en faisant $H = P$.
Montrons maintenant le point (3). Notons $\mathcal{R}$ la valuation en p de $|G|$ et soit $\mathcal{F}$ l'ensemble des sous-ensembles de G de cardinal p^r. On fait agir G sur $\mathcal{F}$ par translation à gauche. Soit H un p-Sylow de G ; l'orbite de H pour cette action est l'ensemble des classes à gauches de H. Le stabilisateur de H est égal à H.
Soit maintenant χ une orbite de $\mathcal{F}$ pour cette action et X un élément de χ . Notons G_X le stabilisateur de X. On a donc :

$$\forall g \in G, gX = X.$$

Par suite, $G_X.X = X$ et donc,

$$x \in X, G_X.x \subset X.$$

et donc,

$$|G_X| \leq |X| = p^r.$$

Inversement, on a

$$|\chi| = |G : G_X| = mp^r \frac{mpr}{|G_X|}$$

Supposons que

$$pgcd(|\chi|, p) = 1.$$

La relation précédente nous assure alors que $|G_X|$ est un multiple de p^r. En particulier, $|G_X| \geq p^r$. Ceci assure que $|G_X| = p^r$. Donc, il existe un élément $x \in G$tel que

$$X = G_X.x.$$

Puisque G agissant sur $\mathcal{F}$ par translation à gauche, $x^{-1}G_X x = x^{-1}.X \in \chi$ est un sous-groupe de G d'ordre p^r.
En conclusion, χ contient un sous-groupe K de G d'ordre p^r.

Inversement, puisque χ est l'ensemble des classes à gauches de K, l'orbite χ contient un sous-groupe de G d'ordre p^r et un seul : c'est K.

Nous avons donc démontré le résultat intermédiaire suivant : l'ensemble des sous-groupes de G d'ordre p^r est en bijection avec l'ensemble des orbites χ de $\mathcal{F}$ pour l'action de G d'ordre premier à p. Le cardinal de l'ensemble des p sous-groupes de Sylow est donc égal au cardinal de l'ensemble de telles orbites qu'il s'agit maintenant d'estimer pour établir le point (3).
Nous allons maintenant montrer le lemme combinatoire suivant :

■

Lemme 3.3.7 *Soit p un nombre premier et m un entier premier à p. Soit de plus $\mathcal{R}$ un entier ≥ 1. Alors,*

$$\binom{mp^r - 1}{p^r - 1} \equiv 1 mod(p)$$

et

$$\binom{mp^r}{p^r} \equiv m mod(p)$$

Preuve. par définition

$$\binom{mp^r - 1}{p^r - 1} = \frac{mp^r - 1}{1}\frac{mp^r - 2}{2}...\frac{mp^r - p^r + 1}{p^r - 1}$$

Pour chaque entier i compris entre 1 et $p^r - 1$, remarquons maintenant que $v_p(mp^r - i) = v_p(i)$

puisque la valuation de i est plus petite que $\mathcal{R}$. Après simplification par $p^{v_p(i)}$, le quotient $\frac{mp^r - i}{i}$ est donc premier à p. On peut donc considérer sa réduction dans $\mathbb{Z}/p\mathbb{Z}$ qui vaut -1. Au total, on a donc

$$\binom{mp^r - 1}{p^r - 1} \equiv (-1)^{p^r - 1} \mathrm{mod} p$$

si p est impair, p^{r-1} est pair, ce qui montre bien que

$$\binom{mp^r - 1}{p^r - 1} \equiv 1 mod p$$

Si $p = 2$, $1 = -1$ et l'on a aussi le résultat. Pour la deuxième égalité, on remarque que

$$\binom{mp^r}{p^r} = \frac{mp^r}{p^r}\binom{mp^r - 1}{p^r - 1}$$

et le lemme suit.

Revenons maintenant à la preuve du théorème précédent. Séparons les orbites de $\mathcal{F}$ en deux parties : ε étant l'ensemble des orbites dont le cardinal est premier à p et ε' l'ensemble des orbites dont le cardinal est un multiple de p. Notons que si $\chi \in \varepsilon$, alors $|\chi| = m$. En effet, on a

vu que χ contient un sous-groupe K d'ordre p^r et donc χ est l'ensemble des classes à gauches de K. Le cardinal de χ vaut donc :

$$|G : K| = \frac{mp^r}{p^r} = m$$

Ecrivons maintenant la formule des classes :

$$|\mathcal{F}| = \sum_{\chi \in \varepsilon'} |\chi| + \sum_{\chi \in \varepsilon} |\chi|.$$

En tenant compte de la remarque précédente, cette formule entraine en particulier :

$$|\mathcal{F}| = \sum_{\chi \in \varepsilon} |\chi| \mathrm{mod} p \equiv m|\varepsilon| \mathrm{mod} p$$

Mais, $\mathcal{F}$ est l'ensemble des parties de G à p^r éléments. Par suite,

$$|\mathcal{F}| = \binom{mp^r}{p^r}$$

Par le lemme précédent, on a donc

$$\binom{mp^r}{p^r} \equiv m|\varepsilon| \mathrm{mod} p \equiv m \mathrm{mod} p$$

Comme m est premier à p, on en déduit que

$$|\varepsilon| \equiv 1 \mathrm{mod} p$$

Mais, on a vu que le nombre de p-sous-groupes de Sylow de G est égal à $|\varepsilon|$. On a donc montré que le nombre de p-sous-groupes de Sylow de G est

$$\equiv 1 \mathrm{mod} p$$

Pour conclure la preuve du point (3), rappelons que comme par le point (2) les sous-groupes de Sylow sont tous conjugués, leur nombre est égal à $|G : N_H|$ Ce nombre divise donc $|G|$, d'ou le théorème. ■

Proposition 3.3.8 *Soit G un groupe fini.Soit P un psylow sous-groupe de G et soit N un sous-groupe de G.Alors :*

(1) $P \cap N$ est un p sous-groupe de sylow de N.

(2) pN/N est un est un p sous-groupe de sylow de G/N.

Preuve. Remarquons d'abord qu'une façon de montrer qu'un sous-groupe H d'un groupe G est un p-sous-groupe Sylow de G est de vérifier que H est un p-sous-groupe et aussi que l'indice de H dans G n'est pas divisible par p.

(1) Puisque N est un sous-groupe normal de G, et $\langle P, N\rangle = PN$ puisque $P \cap N$ un sous-groupe de P, son ordre est une puissance de p.il ne reste plus qu'à montrer que $|N : P \cap N|$ ne divise pas p.On sait que

$$|N : P \cap N| = |PN : N|.$$

Cependant,

$$|G : P| = |G : PN||PN : P|.$$

De sorte que $|PN : P|$ divise $|G : P|$.S'ensuit que $|PN : P|$ n'est pas divisible par p, de sorte que $P \cap N$ est un sous-groupe de N d'indice non divisible par p. D'où, $P \cap N$ est un p-sous-groupe Sylow de N.

(2) Puisque $PN/N \cong P/(P \cap N), PN/N$ est un p sous-groupe de G/N.Comme dans la preuve 1 $|G : PN|$ ne divise pas p, et donc PN/N est un p sous-groupe de sylow de G/N.

■

Conclusion

Pour de nombreuses utilisations en mathématique, en physique, et dans d'autres domaines, il importe de mieux comprendre la structure des groupes, et leurs propriétés. Parmi les problèmes centraux et encore de grande actualité : la recherche des plus petits ensembles de générateurs d'un groupe, où la détermination de tous ses sous-groupes, sont deux problèmes difficiles de la théorie générale des groupes. Un autre axe très important est la recherche en théorie de la représentation des groupes. Enfin, une des grandes réalisations des algébristes du XXe siècle a été de classifier tous les groupes finis.

BIBLIOGRAPHIE

[1] J. Calais, Eléments de théorie des groupes, Presses Universitaires de France, 1984. (QA174.2C25)

[2] S. David, Introduction à la théorie des groupes :module licence L3 LM325

[3] F.Ulmer,Théorie des Groupes, Ellipses (2012).

[4] J. Escofier, S. David, Toute l'algebre de la licence, Cours et exercices corriges, Dunod (2006).

[5] A. Jeanneret, D. lines, Invitation à l'algèbre : Théorie des groupes, des anneaux, des corps et des modules, Cépaduès (2008).

[6] R.Deheuvels,Formes quadratiques et groupes classiques, Presses Universitaires de France, 1981.

[7] B. John, F. Victor, J. Katz, A first course in abstract algebra-Addison, Wesley (2003).

[8] F. John, Humphreys, A course in group theory, Oxford University Press (1996).

[9] A. Kostrikin, Introduction à l'algèbre, Éditions MIR, 1986. (QA154.2K6714)