الجمهورية الجزائرية الديموقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

N° Réf :……

Centre Universitaire

Abd Elhafid Boussouf Mila

Institut des Sciences et Technologie **Département de Mathématiques et Informatique**

Mémoire préparé en vue de l'obtention du diplôme de Master

En : Mathématiques

Spécialité : Mathématiques Fondamentales

Groupes dont les sous groupes de rang infini ont une propriété donnée

Préparé par :

- **Metaai Nassima**
- **Saouchi Ratiba**

Soutenue devant le jury :

- Fadel Wahida	**(MAA)**	**C.U. Abd Elhafid Boussouf**	**Président**
- Daoui Amina	**(MAA)**	**C.U. Abdelhafid Boussouf**	**Rapporteur**
- Boubellouta Khadidja	**(MCB)**	**C. U. Abdelhafid Boussouf**	**Examinateur**

Année Universitaire : 2021/2022

Dédicace *Nassima*

Grand merci à Dieu.

Je dédie ce modeste travail à mes adorables parents : mon cher père on lui disant Merci infiniment pour son aide, son affection son amour. . . , ma chère mère qui ma encouragé tout au long de mes études ; source de ma vie et la bougie qui a éclairé mon chemin depuis ma naissance,...

- À mon cher frère Fayçal, et mes chères sœurs : Warda, Fatima, Samia, Faryal, Ahlam, et Khalida.
- À Mon neuveu, le fils de ma sœur : Djazil .
- À tous mes avunculaires, leur enfants et la famille METAAI en général.
- À mes chères amies chacune de sont nom et en particulier : Assia, Khaoula, Wissam, Fadila,...
- À ma collègue Ratiba.
- À Tous mes enseignants du : Primaire, CEM, Lycée, ENSC, C.U. Abdelhafid Boussouf ; en particulier mon encadreur DAOUI Amina .

Dédicace *Ratiba*

Grand merci à Dieu.

Je dédie ce modeste travail à mes adorables parents : mon cher père on lui disant Merci infiniment pour son aide, son affection son amour. . . , ma chère mère qui ma encouragé tout au long de mes études ; source de ma vie et la bougie qui a éclairé mon chemin depuis ma naissance,...

- À mes chers frères Mohamed, Karim, Hamza et mes chères sœurs : Halima et Chaima.
- À Mon neuveu, la fille de ma sœur : Beylassane .
- À tous mes avunculaires, leur enfants et la famille SAOUCHI en général.
- À mes chères amies .
- À ma collègue Nassima.
- À mon cher fiançaille Mohamed.
- À mon encadreur DAOUI Amina .

Remerciments

Avant tout, nous remercions ALLAH qui nous a donne le courage, la patience, et la volonté pour faire et réaliser ce mémoire.

Nous remercions nos parent, pour tout leur amour, leur encouragement et leur soutien.

Sans oublie notre encadreur Daoui Amina qui suit fidèlement notre travail, nous tenons à la remercier pour son encadrement et son soutien, et nous vous disons :" vous êtes un excellent modèle pour nous, surtout dans le domaine scientifique".

Nous adressons également nos sincères remerciements aux membres du jury Fadel Wahida et Boubellouta Khadidja pour l'intérêt qu'elles ont porté à notre recherche en acceptant d'examiner notre travail.

Nous adressons aussi nos sincères remerciements à tous les enseignants qui nous ont accompagnés durant toutes les années passées scolaires et universitaires.

Tout simplement, Merci à tous.

TABLE DES MATIÈRES

Notations

$\mathbf{N}$	:	ensemble des entiers naturels
$\mathbf{Z}$	:	ensemble des entiers
S_n	:	groupe symétrique
A_n	:	groupe alterné
G_x	:	stabilisateur de x
Ω_x	:	orbite de x
$C_G(x_i)$	:	centralisateur de x_i dans G
$Z(G)$	:	centre de G
$\mathscr{P}(G)$	:	ensemble des parties de G
G'	:	groupe dérivé de G
$G^{(n)}$	:	dérivé n-ième de G
$H \leqslant G$	:	H sous-groupe de G
$H \lhd G$	:	H sous-groupe normal dans G
$H \sqsubset G$	:	H sous-groupe caractéristique de G
$G \simeq \mathbf{Z}$	:	G isomorphe avec $\mathbf{Z}$
$o(G)$	:	ordre du groupe G
$\langle\ x\ \rangle$	:	sous-groupe enjendré par x
$\lvert E \rvert$	:	cardinal de l'ensemble E
$[x, y]$	:	comutateur de x et y
$PSL(n, F)$	:	groupe projectif spécial linéaire

INTRODUCTION

La théorie des groupes est la branche la plus ancienne de l'algèbre moderne. Ses origines se trouvent dans l'œuvre de Joseph Louis Lagrange (1736-1813), Paulo Ruffini (1765-1822), et Evariste Galois (1811-1832) sur la théorie des équations algébriques. Leurs groupes consistaient en des permutations de variables ou de racines de polynômes, et en fait, pendant une grande partie du XIX^e siècle, tous les groupes étaient des groupes de permutations finies.Néanmoins, bon nombre des idées fondamentales de la théorie des groupes ont été introduites par ces premiers travailleurs et leurs successeurs, Augustin Louis Cauchy (1789-1857), Ludwig Sylow (1832-1918), Camille Jordan (1838-1922) entre autres.

Ces dernières années, une série d'articles a été publiée sur le comportement des groupes de rang infini dans lesquels chaque sous-groupe propre de rang infini a une propriété appropriée. Dans ce mémoire on étude la structure des groupes dans lesquels chaque sous-groupe propre de rang infini contient un sous-groupe abélien d'indice fini.Cette classe a été considérée par F. de Giovanni et F. Saccomanno dans " Groups whose proper subgroups of infinite rank are abélien-by-finite " [9] .

Dans le premier chapitre on a étudie quelques notions fondamental : les groupes symétrique S_n, les groupes alternés A_n, les opérations d'un groupe sur un ensemble et les groupes cycliques.

Dans le deuxième chapitre on a concentré sur les groupes finis en particulier les théorèmes de Sylow et ses applications .

Dans le troisième chapitre on a étudie l'article de ; F. de Giovanni, F. Saccomanno "groupes dont tous les sous groupes de rang infini sont abéliens-par-fini".

CHAPITRE 1

NOTIONS FONDAMENTAUX

Dans ce chapitre on a énoncé quelques notion de base de la théorie des groupes, on a adopté [4] comme référence de base.

1.1 Le groupe S_n et A_n

1.1.1 Groupes symétriques S_n

Pour tout entier $n \geqslant 1$, le groupe symétrique S_n est le groupe des permutations (bijection de $\{1, 2, ..., n\}$ dans $\{1, 2, ..., n\}$) de l'ensemble $\{1, 2, ..., n\}$, noté $\mathbf{N}_n$.
Plus généralement, S_n peut être considéré comme le groupe des permutation de tout ensemble fini de cardinal n.
Rappelons que S_n est un groupe fini d'ordre $n!$, non abélien pour $n > 2$.

1.1.1.1 Notion de σ-orbite (ou orbite suivant σ)

A/ Support d'une permutation :

Définition 1.1. *Soit $\sigma \in S_n$, le support de σ est l'ensemble : $supp(\sigma) = \{i \in \mathbf{N}_n; \quad \sigma(i) \neq i\}$.*

Remarque 1.1.1.

1. Dans $S_n, \sigma = e$ si seulement si $supp\ \sigma = \varnothing$
2. Quel que soit $\sigma \neq e$ dans S_n, la restriction de σ à $supp(\sigma)$ est une permutation de l'ensemble $supp(\sigma)$.

En effet, soit $i \in supp(\sigma)$; posons $\sigma(i) = j$.

si j n'appartenait pas à $supp(\sigma)$, on aurait $\sigma(j) = j$; σ étant injectif, $\sigma(i) = \sigma(j)$ impliquerait $i = j$, ce qui est contraire à l'hypothèse $i \in supp(\sigma)$.

La restriction σ' de σ à son support est donc une application injective de l'ensemble fini non vide $supp(\sigma)$ dans lui-même ; par suite, σ' est une permutation de l'ensemble $supp(\sigma)$, en vertu du théorème suivant : $\ll$ Si E et F sont deux ensembles finis non vides de même cardinal, alors, pour une application f de E dans F, on a :

f injective $\Leftrightarrow$ f surjective ;

donc, en particulier :

f injective $\Rightarrow$ f bijective $\gg$.

3. D'après la remarque précédente, $supp\,(\sigma^{-1}) = supp\,(\sigma)$; on en déduit :
$supp\,(\sigma^k) \subseteq supp\,(\sigma)$, pour tout $k \in \mathbf{Z}$.

Proposition 1.1. *Dans tout groupe S_n, deux permutations dont les supports sont disjoints commutent.*

preuve : La propriété étant immédiate pour $n = 1$, supposons $n > 1$ et considérons $\sigma_1 \neq \sigma_2$ dans S_n tels que

$$supp\,(\sigma_1) \bigcap supp\,(\sigma_2) = \varnothing$$

. Si l'une des deux permutations est l'identité, la propriété est vérifiée ; supposons les deux supports non vides.

Soit $i \in supp(\sigma_1)$, alors $i \notin supp(\sigma_2)$ et $\sigma_1(i) \notin supp\,(\sigma_2)$, par suite :

$$\sigma_1 \circ \sigma_2(i) = \sigma_1(i) \quad \text{et} \quad \sigma_2 \circ \sigma_1(i) = \sigma_1(i).$$

De même pour $i \in supp(\sigma_2)$, on a :

$$\sigma_1 \circ \sigma_2\,(i) = \sigma_2\,(i) \quad \text{et} \quad \sigma_2 \circ \sigma_1\,(i) = \sigma_2\,(i).$$

D'autre part, s'il existe $i \in N_n$ tel que $i \notin supp(\sigma_1) \cup supp(\sigma_2)$, alors $\sigma_1 \circ \sigma_2\,(i) = i$ et $\sigma_2 \circ \sigma_1\,(i) = i$.

On en conclut que $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$. □

B/ Notion de σ-orbite (ou orbite suivant σ). A toute permutation $\sigma \in S_n$,on associe la relation binaire $\mathscr{R}_\sigma$ définie dans $\mathbf{N}_n$ par :

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

Il est facile de vérifier que $\mathscr{R}_\sigma$ est une relation d'équation d'équivalence dans $\mathbf{N}_n$ et que la classe d'équivalence modulo $\mathscr{R}_\sigma$ d'un élément $i \in \mathbf{N}_n$ est :

$$\Omega_\sigma(i) \;=\; \{\sigma^r(i);\;\; r \in \mathbf{Z}\} \tag{1.1}$$

Définition 1.2. *Pour tout $\sigma \in S_n$ et tout $i \in \mathbf{N}_n$,*
$\Omega_\sigma(i)$ s'appelle la σ-orbite de i (ou l'orbite de i suivant σ).

Remarque 1.1.2.

1. Supposons $n > 1$ et $\sigma \neq e$ dans S_n tel que $o(\sigma) = p$, on a alors :

   $$\langle\ \sigma\ \rangle = \{\sigma^r; r \in \mathbf{Z}\} = \{e, \sigma, ..., \sigma^{p-1}\};$$

   par suite, en notant $|\Omega_\sigma(i)|$ le cardinal de la σ-orbite de i, on a, pour tout $i \in \mathbf{N}_n$:

   $$1 \leqslant |\Omega_\sigma(i)| \leqslant p \tag{1.2}$$

   Si $i \notin supp\ (\sigma)$, alors $\Omega_\sigma(i) \;=\; \{i\}$, donc $|\Omega_\sigma(i)| = 1$.
   une σ- orbite de cardinal 1 sera dite ponctuelle.
   Si $i \in supp(\sigma)$, on a nécessairement $2 \leqslant |\Omega_\sigma(i)| \leqslant p$.
2. Si $\{i_1, i_2, ..., i_t\}$ est une famille de représentation des σ-orbites distinctes de $\mathbf{N}_n$, les $\{\Omega_\sigma(i_q)\}_{1\leqslant q\leqslant t}$ forment une partition de $\mathbf{N}_n$, d'où

   $$n = \sum_{1\leqslant q\leqslant t} |\Omega_\sigma(i_q)| \tag{1.3}$$

Exemple 1.1.1. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 6 & 3 & 4 & 7 \end{pmatrix}$
$\Omega_\sigma(1) = \{1, 5, 3\}, \quad \Omega_\sigma(2) = \{2\}, \quad \Omega_\sigma(4) = \{4, 6\}, \quad \Omega_\sigma(7) = \{7\}.$

1.1.1.2 Cycles dans S_n. Transpositions

Considérons la permutation :

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 6 & 2 & 5 & 7 \end{pmatrix}$$

Le support de γ est $\{2, 4, 5, 6\}$ et on remarque que :
$\gamma(2) = 4, \quad \gamma(4) = 6, \quad \gamma(6) = 5 \quad et \quad \gamma(5) = 2.$
On dit que, dans le groupe S_7, γ est un cycle de longueur 4 et γ est noté $(2, 4, 6, 5)$. La notion générale de cycle dans S_n est la suivante :

Définition 1.3. *Une permutation $\gamma \in S_n$ est un cycle de longueur r $(1 \leqslant r \leqslant n$ dans $\mathbf{N})$ s'il existe un ensemble ordonné de r entiers distincts dans $\mathbf{N}_n : j_1, j_2, ..., j_r$, tels que :*
$\gamma(j_1) = j_2, \quad \gamma(j_2) = j_3, ..., \gamma(j_{r-1}) = j_r, \quad \gamma(j_r) = j_1$
et pour tout $k \in \mathbf{N}_n \setminus \{j_1, j_2, ..., j_r\}, \gamma(k) = k$.
un tel cycle sera noté $\gamma = (j_1, j_2, ..., j_r)$.
l'ensemble $\{j_1, j_2, ..., j_r\}$ est le support de γ.

Définition 1.4. *Un cycle de longueur 2 dans S_n $(n \geqslant 2)$ est appelé transposition. Si $\tau = (j_1, \ j_2)$, on a $\tau(j_1) = j_2, \ \tau(j_2) = j_1$ et $\tau(k) = k$, pour tout $k \in \mathbf{N}_n \setminus \{j_1, j_2\}$.*
une transposition dans S_n est donc une permutation qui dans $\mathbf{N}_n$, échange deux éléments et laisse invariants tous les autres (lorsque $n \geqslant 3$).

Exemple 1.1.2.

1. $S_2 = \{e, \tau\}$ où τ est la transposition qui échange 1 et 2.

2. Dans S_3, les permutations $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, sont des transpositions et $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ sont des cycles de longueur 3.

Remarque 1.1.3. Pour $n \geqslant 2$ dans $\mathbf{N}$, le nombre des transpositions dans S_n est égale au nombre de couples $(i, j) \in \mathbf{N}_n \times \mathbf{N}_n$ tel que $i \neq j$; ce nombre est donc $C_n^2 = \dfrac{n(n-1)}{2}$.

Définition 1.5. *Dans S_n $(n \geqslant 2)$, le cycle de longueur n :*

$$\gamma_1 = (1, 2, ..., n) = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ 2 & 3 & 4 & ... & 1 \end{pmatrix}$$

est appelé permutation circulaire des entiers $1, 2, ..., n$.

Remarque 1.1.4.

1. Dans $S_n (n \geqslant 3)$ un cycle de longueur n n'est pas nécessairement la permutation circulaire.
   Par exemple, dans $S_4 : \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ est le cycle $(1, 4, 3, 2)$ différent de $(1, 2, 3, 4)$.

2. Dans S_n, un cycle de longueur r $(1 \leqslant r \leqslant n)$ sera appelé un r-cycle.

Proposition 1.2. *Dans tout groupe S_n, un r-cycle est un élément d'ordre r.*

preuve : Soit $\gamma = (j_1, j_2, ..., j_r)$ un r-cycle dans S_n.
- Si $r = 1$, alors $\gamma = e$, donc $o(\gamma) = 1$.
- Supposons $1 < r \leqslant n$; pour tout k $(1 \leqslant k \leqslant r)$, on a :
$\gamma(j_k) = j_{k+1}$, $\gamma^2(j_k) = j_{k+2}, ...,$ $\gamma^{r-k}(j_k) = j_r, ...,$ $\gamma^r(j_k) = j_k$.
D'autre part, si $r < n$ et $i \notin supp(\gamma)$, alors $\gamma(i) = i$. Les r éléments $j_1, j_2, ..., j_r$ étant distincts, r est le plus petit entier positif tel que $\gamma^r = e$, d'où $o(\gamma) = r$. □

Corollaire 1.3. *Si τ est une transposition dans S_n, alors $\tau^2 = e$ donc $\tau^{-1} = \tau$.*

Remarque 1.1.5.

1. Dans tout groupe symétrique S_n, l'inverse d'un r-cycle est un r-cycle . En effet, si $\gamma = (j_1, j_2, ..., j_r)$, alors $\gamma^{-1} = \gamma^{r-1} = (j_r, j_{r-1}, ..., j_1)$.
   Cependant, pour p entier tel que $2 \leqslant p \leqslant r-2$, γ^p n'est pas nécessairement un cycle. par exemple, dans S_4 si γ_1 est la permutation circulaire :
   $\gamma_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ n'est pas un cycle.
2. On déduit de l'exemple précédant qu'un produit de cycles n'est pas nécessairement un cycle.
   On remarquera cependant que pour $1 \leqslant n \leqslant 3$, tout élément de S_n est un cycle.

1.1.1.3 Décomposition d'une permutation en un produit de cycles ou en un produit de transpositions

Remarque 1.1.6. Dans un groupe S_n, on dira que deux cycles sont disjoints, si leurs supports sont disjoints.
D'après la proposition 1.1, deux cycles disjoints commutent.

Théorème 1.4. *Tout permutation $\sigma \neq e$ dans S_n s'écrit sous la forme :*

$$\sigma = \gamma_1 \circ \gamma_2 \circ ... \gamma_s \tag{1.4}$$

où $s \in \mathbf{N}^*, \gamma_1, \gamma_2, ..., \gamma_s$ sont des cycles disjoints, tous différents de e et la décomposition (1.4) est unique à l'ordre des facteurs près.

preuve : Soit $\sigma \neq e$ dans S_n ; le support de σ étant non vide, il existe au moins une σ-orbite non ponctuelle $\Omega_\sigma(i)$.
Si $\Omega_\sigma(i) = \{i, \sigma(i), ..., \sigma^{p-1}(i)\}$ avec $2 \leqslant p \leqslant n$; posons $i = j_1,\ \sigma(i) = j_2, ...,\ \sigma^{p-1}(i) = j_p$ et notons γ le cycle $(j_1, j_2, ..., j_p)$.
La restriction de σ à $\{j_1, j_2, ..., j_p\}$ est égal à la restriction de γ à son support. Ainsi, à toute σ-orbite non ponctuelle Ω, on peut associer un cycle γ dont le support est Ω. Soit $\{\Omega_q\}_{1\leqslant q\leqslant s}$ la famille des σ-orbites non ponctuelles distinctes dans $\mathbf{N}_n$. A tout σ-orbite Ω_q associons, comme plus haut, le cycle γ_q, dont le support est Ω_q les σ-orbites Ω_q $(1 \leqslant q \leqslant s)$ étant deux à deux disjointes, les cycles γ_q $(1 \leqslant q \leqslant s)$ sont deux à deux disjoints, donc ils commutent entre eux.
Posons $\sigma' = \gamma_1 \circ \gamma_2 \circ ... \circ \gamma_s$ et comparons σ' et σ.
Soit

$$j \in \bigcup_{1\leqslant q\leqslant s} \Omega_q$$

il existe l $(1 \leqslant l \leqslant s)$ tel que $j \in \Omega_l$. Puisque $\sigma_{/\Omega_l} = \gamma_{l/\Omega_l}$, on a $\sigma(j) = \gamma_l(j)$.
D'autre part, on peut écrire

$$\sigma' = \gamma_l \circ \prod_{\substack{1\leqslant q\leqslant s \\ q\neq l}} \gamma_q$$

pour $q \neq l, \gamma_q(j) = j$, d'où $\sigma'(j) = \gamma_l(j)$.
De plus, s'il existe

$$k \in \mathbf{N}_n \setminus \bigcup_{1\leqslant q\leqslant s} \Omega_q$$

on a $\sigma(k) = k$ et aussi $\sigma'(k) = k$. On en conclut que $\sigma = \sigma'$.
Supposons que $\sigma = \gamma'_1 \circ \gamma'_2 \circ ... \circ \gamma'_s$ soit une autre décomposition de σ en un produit de cycles disjoints, tous différents de e. Pour tout p $(1 \leqslant p \leqslant r)$, notons Ω'_p la γ'_p-orbite non ponctuelle ; les cycles γ'_p étant disjoints, les σ-orbites non ponctuelles sont alors les Ω'_p, pour $1 \leqslant p \leqslant r$. La décomposition de $\mathbf{N}_n$ en σ-orbites étant unique, on en déduit que $r = s$ et qu'il existe une permutation π dans le groupe symétrique S_s telle que $\Omega'_p = \Omega_{\pi(p)}$ et par suite $\gamma'_p = \gamma_{\pi(p)}$; d'où l'unicité de la décomposition (1.4) à l'ordre des facteurs près. □

Remarque 1.1.7.

1. Compte tenu de son unicité, la décomposition d'une permutation σ sous la forme (1.4) sera appelée : décomposition canonique de σ en un produit de cycles.

2. D'après le théorème 1.4 tout groupe S_n est engendré par l'ensemble de ses cycles.

Exemple 1.1.3. Soit σ la permutation du groupe S_7 considérée dans l'exemple 1.1.1. La décomposition de $\mathbf{N}_7$ en σ-orbites implique $\sigma = \gamma_1 \circ \gamma_2$ où $\gamma_1 = (1,5,3)$ et $\gamma_2 = (4,6)$. on écrira

$$\sigma = (1,5,3)\,(4,6).$$

Remarque 1.1.8. Soit $\sigma \in S_n$, si $\{\Omega_q\}_{1\leqslant q\leqslant t}$ est la famille de toutes les σ-orbites distinctes, alors, en associant éventuellement à toute σ-orbite ponctuelle le cycle e de longueur 1, on obtient, par la méthode du théorème 1.4, une décomposition de σ en produit de t cycles disjoints :

$$\sigma = \gamma_1 \circ \gamma_2 \circ ... \circ \gamma_t$$

telle que

$$\sum_{1\leqslant q\leqslant t} long(\gamma_q) = n$$

car pour tout q $(1 \leqslant q \leqslant t)$, $long(\gamma_q) = |\Omega_q|$.

Proposition 1.5. *Soit $\sigma \neq e$ dans S_n $(n \geqslant 2)$; si $\sigma = \gamma_1 \circ \gamma_2 \circ ... \circ \gamma_s$ est la décomposition canonique de σ, alors l'ordre de σ dans le groupe S_n est égal au PPCM des longueurs des cycles γ_q $(1 \leqslant q \leqslant s)$.*

preuve : Pour tout q $(1 \leqslant q \leqslant s)$ posons $\Omega_q = supp\,(\gamma_q)$ et $r_q = long(\gamma_q) = |\Omega_q|$. Soit l le $PPCM$ des r_q, dans $\mathbf{N}^*$. Quel que soit q $(1 \leqslant q \leqslant s), l$ est multiple de r_q, donc $\gamma_q^l = e$; or, les γ_q commutent donc

$$\sigma^l = \gamma_1^l \circ \gamma_2^l \circ ... \circ \gamma_s^l = e\,;$$

on en déduit que, si $k = o(\sigma)$, alors k divise l.
D'autre part, $\gamma_{q/\Omega_q} = \sigma_{/\Omega_q}$, d'où $\gamma_{q/\Omega_q}^k = (\gamma_{q/\Omega_q})^k = \sigma_{/\Omega_q}^k = e$; Ω_q, étant le support de γ_q^k, on a $\gamma_q^k = e$; par suite, k est multiple de r_q, quel que soit $q\,(1 \leqslant q \leqslant r)$, donc l divise k. On en conclut que $k = l$. □

Théorème 1.6. *Pour tout $n \geqslant 2$ dans $\mathbf{N}$, toute permutation $\sigma \in S_n$ se décompose de manière non unique, en un produit de transpositions non permutables, en général.*

preuve : $n \geqslant 2$ implique qu'il existe au moins une transposition τ dans S_n. $e = \tau^2$, donc e est produit de transposition.
Sachant que toute permutation $\sigma \neq e$ dans S_n est un produit de cycles (théorème 1.4), il suffit de prouve que tout cycle est un produit de transposition.

Soit $\gamma = (j_1, j_2, ..., j_r)$ dans S_n, tel que $1 < r \leqslant n$.
Notons (j_p, j_q) la transposition qui échange j_p et j_q tels que $1 \leqslant p < q \leqslant n$; en écrivant $(j_p, j_q)\,(j_l, j_m)$ à la place de $(j_p, j_q) \circ (j_l, j_m)$, posons :

$$\gamma' = (j_1, j_2)\,(j_2, j_3)...(j_{r-1}, j_r).$$

Pour tout $k\,(1 \leqslant k \leqslant r-1)$, on a $\gamma'(j_k) = j_{k+1} = \gamma(j_k)$; de plus $\gamma'(j_r) = j_1 = \gamma(j_r)$. S'il existe $k \in \mathbf{N}_n \setminus supp(\gamma)$, alors $\gamma'(k) = k = \gamma(k)$.
On en déduit que $\gamma' = \gamma$, d'où

$$(j_1, j_2, ..., j_r) = (j_1, j_2)\,(j_2, j_3)...(j_{r-1}, j_r) \tag{1.5}$$

De la décomposition canonique d'une permutation σ en un produit de cycles, on peut donc déduire une décomposition de σ en produit de transpositions, mais cette dernière n'est pas unique si $n \geqslant 3$, car, étant donné une transposition quelconque (j, k) dans S_n, on vérifie facilement que

$$(j, k) = (1, j)\,(1, k)\,(1, j) \tag{1.6}$$

D'autre part, si j, k, l sont trois entiers distincts dans $\mathbf{N}_n$, on a $(j, k)\,(k, l) \neq (k, l)\,(j, k)$; on en déduit que dans une décomposition d'une permutation $\sigma \in S_n\ (n \geqslant 3)$ en un produit de transpositions, deux transpositions distinctes non disjointes ne sont pas permutables. □

Exemple 1.1.4.

1. Soit $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 6 & 2 & 5 & 7 \end{pmatrix}$; γ est le cycle (2, 4, 6, 5) , dans S_7.
   En appliquant la formule (1.5), on obtient :
   $$\gamma = (2, 4)\,(4, 6)\,(6, 5).$$

2. Soit $\sigma \in S_7$ la permutation de l'exemple 1.1.1, dont la décomposition canonique (1.4) a été déterminée dans l'exemple 1.1.3 $\sigma = (1, 5, 3)\,(4, 6)$.
   Compte tenu de la formule (1.5), on a $\sigma = (1, 5)(5, 3)(4, 6)$.
   D'après la relation (1.6) on peut écrire
   $$(5,\ 3) = (1,\ 5)\ \ (1,\ 3)\ \ (1,\ 5),$$
   on en déduit que $\sigma = (1, 3)\,(1, 5)\,(4, 6)$.

Proposition 1.7. *Tout groupe symétrique S_n $(n \geqslant 2)$ est engendré par l'ensemble des*

$(n-1)$ *transpositions de la forme* $(1,i)$, *telles que* $2 \leqslant i \leqslant n$.
Ce résultat se déduit de la formule (1.6) *et du théorème 1.6.*

Proposition 1.8. *Tout groupe symétrique* S_n $(n \geqslant 2)$ *est engendré par les* $(n-1)$ *transpositions de la forme* $(i, i+1)$, *telles que* $1 \leqslant i \leqslant n-1$.

preuve : Il suffit de montrer que dans S_n toute transposition (p,q) telle que $1 \leqslant p < q \leqslant n$ est produit de transposition de la forme $(i, i+1)$.
On raisonne par récurrence sur $(q-p)$.

- Pour $q-p=1$, on a $(p,q) = (p,p+1)$.
- Pour $q-p>1$, on vérifie que :

$$(p,q) = (q-1,q)\,(p,q-1)\,(q-1,q)\,;$$

l'hypothèse de récurrence implique alors le résultat énoncé. □

1.1.1.4 Signature d'une permutation

Définition 1.6. *Soit* $\sigma \in S_n$ $(n \geqslant 1)$ *; si* t *est le nombre des* σ*-orbites dans* $\mathbf{N}_n$, *on pose :*

$$\varepsilon(\sigma) = (-1)^{n-t} \tag{1.7}$$

et $\varepsilon(\sigma)$ *sera appelée signature de la permutation* σ.

Remarque 1.1.9.

- Si $\sigma = e$, alors $t = n$, donc $\varepsilon(e) = 1$.
- Si τ est une transposition dans S_n, alors $t = n-1$, d'où

$$\varepsilon(\tau) = -1 \tag{1.8}$$

- Si γ est un r-cycle dans S_n, on a $t = n-r+1$, d'où

$$\varepsilon(\gamma) = (-1)^{r-1} \tag{1.9}$$

Lemme 1.9. *Soit* $\sigma \in S_n$ $(n \geqslant 2)$ *; alors, quelle que soit la transposition* $\tau \in S_n$, *on a :*

$$\varepsilon(\sigma \circ \tau) = -\varepsilon(\sigma) \tag{1.10}$$

preuve : Supposons $\tau = (i, j)$.

On remarque que si $\Omega_\sigma(k)$ est une σ-orbite ne contenant ni i, ni j, alors $\Omega_{\sigma\circ\tau}(k) = \Omega_\sigma(k)$. Considérons alors les σ-orbites contenant i ou j.

Premier cas : i et j sont dans deux σ-orbites distinctes ; soit :

$\Omega_\sigma(i) = \{i, \sigma(i), ..., \sigma^{p-1}(i)\}$

$\Omega_\sigma(j) = \{j, \sigma(j), ..., \sigma^{q-1}(j)\}$.

Déterminons $\Omega_{\sigma\circ\tau}(i)$

$\sigma \circ \tau(i) = \sigma(j)$; alors :

pour $1 \leqslant r \leqslant q-1$, $(\sigma \circ \tau)^r(i) = \sigma^r(j)$ et $(\sigma \circ \tau)^q(i) = j$; alors $\sigma \circ \tau(j) = \sigma(i) \Rightarrow (\sigma \circ \tau)^{q+1}(i) = \sigma(i)$,

donc pour $1 \leqslant s \leqslant p-1, (\sigma \circ \tau)^{q+s}(i) = \sigma^s(i)$ et $(\sigma \circ \tau)^{q+p}(i) = i$;

par suite : $\Omega_{\sigma\circ\tau}(i) = \{i, \sigma(j), ..., \sigma^{q-1}(j), j, \sigma(i)..., \sigma^{p-1}(i)\}$.

Les éléments des σ-orbites distinctes de i et de j se trouvent donc regroupés dans une même $\sigma \circ \tau$-orbite .

Deuxième cas : i et j sont dans une même σ-orbite ; soit : $\Omega_\sigma(i) = \{i, \sigma(i), ..., \sigma^{p-1}(i)\}$.

$j \neq i$ et $j \in \Omega_\sigma(i)$ implique qu'il existe un unique entier r tel que $1 \leqslant r \leqslant p-1$ et $\sigma^r(i) = j$.

On détermine $\Omega_{\sigma\circ\tau}(i)$.

$\sigma \circ \tau(i) = \sigma(j) = \sigma^{r+1}(i)$,

d'où, pour $1 \leqslant l < p-r$, $(\sigma \circ \tau)^l(i) = \sigma^{r+l}(j)$ et $(\sigma \circ \tau)^{p-r}(i) = i$; par suite,

$$\Omega_{\sigma\circ\tau}(i) = \{i, \sigma^{r+1}(i), ..., \sigma^{p-1}(i)\}.$$

On constate que $j \notin \Omega_{\sigma\circ\tau}(i)$ et de $\sigma \circ \tau(j) = \sigma(i)$ on déduit

$$\Omega_{\sigma\circ\tau}(i) = \{j, \sigma(i), ..., \sigma^{r-1}(i)\}.$$

La σ-orbite contenant i et j se trouve scindée en deux $\sigma\circ\tau$-orbites distinctes, contenant respectivement i et j.

On en conclut que si t est le nombre des σ-orbites distinctes, dans le premier cas, le nombre des $\sigma \circ \tau$-orbites distinctes est $t-1$ et dans le second cas, il est $t+1$, d'où

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

□

Théorème 1.10. *Soit $\sigma \in S_n (n \geqslant 2)$;*
Si σ est un produit de k transpositions, alors :

$$\varepsilon(\sigma) = (-1)^k \tag{1.11}$$

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

prouve : Pour toute transposition $\tau \in S_n$, on a $\varepsilon(\tau) = -1$ (remarque 1.1.9) ; par suite, la formule (1.11) se déduite facilement de la relation (1.10) du lemme 1.9. D'autre part

$\tau_1 \circ \tau_2 \circ ... \circ \tau_k = \tau'_1 \circ \tau'_2 \circ ... \circ \tau'_l$

implique $(-1)^k = (-1)^l$, donc les entiers k et l sont nécessairement de même parité. □

Remarque 1.1.10. D'après ce qui précède, associer à tout $\sigma \in S_n$ sa signature $\varepsilon(\sigma)$ on peut définir une application

$$\begin{aligned} \varepsilon : S_n &\to \{-1, 1\} \\ \sigma &\mapsto \varepsilon(\sigma). \end{aligned}$$

considérons $\{-1, 1\}$ comme un groupe multiplicatif (sous-groupe de $(\mathbf{Q}^*, \times)$), on démontre le résultat fondamental suivant :

Théorème 1.11. *Pour $n \geqslant 2$ dans $\mathbf{N}$, l'application*

$$\begin{aligned} \varepsilon : S_n &\to \{-1, 1\} \\ \sigma &\mapsto \varepsilon(\sigma). \end{aligned}$$

est un épimorphisme de groupes.

preuve : La condition $n \geqslant 2$ implique la surjectivité de ε ; vérifions que ε est un morphisme de groupes. Soient σ et σ' dans S_n telles que :

$$\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_k \quad \text{et} \quad \sigma' = \tau'_1 \circ \tau'_2 \circ ... \circ \tau'_l$$

où les $\tau_i \, (1 \leqslant i \leqslant k)$ et $\tau'_j \, (1 \leqslant j \leqslant l)$ sont des transpositions.
On a alors $\sigma \circ \sigma' = \tau_1 \circ \tau_2 ... \circ \tau_k = \tau'_1 \circ \tau'_2 \circ ... \circ \tau'_l$, d'où, en appliquant la formule (1.11) :

$$\varepsilon(\sigma \circ \sigma') = (-1)^{k+l} = (-1)^k (-1)^l$$

et par suite

$$\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \, \varepsilon(\sigma').$$

□

Définition 1.7. *Une permutation $\sigma \in S_n$ est dite paire si $\varepsilon(\sigma) = 1$ et impaire si $\varepsilon(\sigma) = -1$.*

Remarque 1.1.11.

1. Tout transposition est une permutation impaire.
2. Une permutation $\sigma \in S_n\,(n \geqslant 2)$ est paire (respectivement impaire) si et seulement si elle est produit d'un nombre paire (respectivement impaire) de transpositions.
3. Quel que soit $\sigma \in S_n$ et $\sigma,\ \sigma^{-1}$ sont de même parité, c'est-à-dire que $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$; en effet, $\varepsilon(\sigma^{-1}) = (\varepsilon(\sigma))^{-1}$ dans le groupe $\{-1, 1\}$.

Exemple 1.1.5.

1. Soit σ dans S_7 la permutation considérée dans l'exemple 1.1.1 ; le nombre t des σ-orbite distinctes est 4, d'où ici $n - t = 7 - 4 = 3$. En appliquant la formule (1.7) on obtient $\varepsilon(\sigma) = (-1)^3 = -1; \sigma$ est une permutation impaire, ce qui est confirmé par le calcul de $\varepsilon(\sigma)$ à partir d'une décomposition de σ en produit de transpositions (exemple 1.1.4), on a $\sigma = (1, 5)(5, 3)(4, 6)$,en appliquant la formule (1.11) on obtient $\varepsilon(\sigma) = (-1)^3 = -1$;σ est une permutation impaire.

2. Soit $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 5 & 6 & 8 & 1 & 9 & 3 & 2 \end{pmatrix}$ dans S_9.
   Déterminons les σ-orbites :
   $\Omega_\sigma(1) = \{1, 4, 6\};\ \Omega_\sigma(2) = \{2, 7, 9\};\ \Omega_\sigma(3) = \{3, 5, 8\}$.
   Il y a $3\,\sigma - orbites$ distinctes, d'après la formule (1.7), $\varepsilon(\sigma) = (-1)^{9-3} = 1$, d'où σ est une permutation paire.

1.1.2 Groupe alterné A_n

Soit le groupe symétrique S_n, notons A_n : l'ensemble des permutations paires de S_n.
Pour $n = 1$, on a $A_1 = S_1 = (e)$.
Pour $n \geqslant 2, A_n = \{\sigma \in S_n; \varepsilon(\sigma) = 1\}$ est le noyau de l'épimorphisme $\varepsilon : S_n \to \{-1, 1\}$.
A_n est donc un sous-groupe de S_n.
On a(A_n= $ker\,\varepsilon$ et ε surjectif) $\Rightarrow \dfrac{S_n}{A_n} \simeq \{-1, 1\}$, par suite, $[S_n : A_n] = 2$, d'où $o(A_n) = \dfrac{n!}{2}$ puisque $o(S_n) = n!$; on en déduit l'énonce suivant :

Proposition 1.12. *Pour tout $n \geqslant 2$, l'ensemble A_n des permutations paires de S_n forme un sous-groupe de S_n d'ordre $\frac{n!}{2}$.*

Définition 1.8. *Pour tout $n \in \mathbf{N}^*$, le groupe A_n des permutations paires de S_n est appelé groupe alterné de degré n.*

Remarque 1.1.12. Pour $n \geqslant 2$, les deux classes de S_n modulo A_n sont A_n et $\tau A_n = \{\tau \circ \sigma; \sigma \in A_n\}$ où τ est une transposition quelconque de S_n.

$A_n = ker\,\varepsilon \Rightarrow \tau A_n = A_n\tau = \{\sigma \circ \tau; \sigma \in A_n\}$.

τA_n est l'ensemble des permutations impaires de S_n et cet ensemble n'est pas un sous-groupe de S_n.

1.2 Actions de groupe

1.2.1 Action d'un groupe sur un ensemble

Définition 1.9. *On dit qu'un groupe G opère sur l'ensemble E s'il existe une application*

$$G \times E \to E$$
$$(g, x) \mapsto gx$$

appelée action de G dans E , telle que

i. $g_1\,(g_2 \cdot x) = (g_1 \cdot g_2)\,x$ *pour tout* $g_1, g_2 \in G$ *et pour tout* $x \in E$ *(associativité mixte).*

ii. $e\,x = x$ *pour tout* $x \in E$ *(neutralité).*

1.2.2 Sous-groupe d'isotropie ou stabilisateur. Orbite

I) Définitions et Exemples

Soit G un groupe opérant sur un ensemble E, grâce à l'application :

$$G \times E \to E$$
$$(g, x) \mapsto gx$$

1. Pour tout $x \in E$. on associe $G_x = \{g \in G; g.x = x\}$.
   On vérifie facilement que G_x est un sous-groupe de G.

Définition 1.10. *E étant un G-ensemble, le sous-groupe G_x de G, associé à tout $x \in E$ et défini ci-dessus, est appelé sous-groupe d'isotropie de x ou stabilisateur de x.*

2. On considère dans E la relation binaire ρ_G définie par :

$$x\rho_G y \Leftrightarrow \exists g \in G, y = g.x \tag{1.12}$$

Les conditions (i). et $(ii.)$ de la définition 1.9 implique que ρ_G est une relation d'équivalence dans E.

Définition 1.11. *E étant un G-ensemble, la classe d'équivalence modulo ρ_G d'un élément x de E est appelé orbite de x suivant G ou G-orbite de x.*
La G-orbite d'un élément x de E sera notée Ω_x :

$$\Omega_x = \{g.x; g \in G\} \tag{1.13}$$

Exemple 1.2.1.

1. G opère sur G par translation à gauche ; pour tout $x \in G$, on a
   $G_x = \{g \in G; gx = x\}$, donc $G_x = (e)$
   $\Omega_x = \{gx; g \in G\} = Gx$, donc $\Omega_x = G$.
2. G opère sur G par conjugaison ; pour tout $x \in G$,
   $G_x = \{g \in G; gxg^{-1} = x\} = C_G(x)$, le centralisateur de x dans G.
   $\Omega_x = \{gxg^{-1}; g \in G\} =$ (classe de conjugaison de x dans G)
   On en déduit que ρ_G coïncide, dans ce cas, avec la relation de conjugaison dans G.
3. G opère sur $\mathscr{P}(G)$ par conjugaison ($\mathscr{P}(G)$: l'ensemble des parties de G) , alors pour $S \in \mathscr{P}(G)$ et $S \neq \varnothing$,
   $G_S = \{g \in G; gSg^{-1} = S\} = \mathbf{N}_G(S)$, le normalisateur de S dans G.
   $\Omega_S = \{gSg^{-1}; g \in G\} =$(classe de conjugaison de S dans $\mathscr{P}(G)$).
   $G_\varnothing = G$ et $\Omega_\varnothing = \{\varnothing\}$.
   ρ_G coïncide avec la relation de conjugaison dans $\mathscr{P}(G)$.
4. Soit $\sigma \in S_n$ ($n > 1$ dans $\mathbf{N}$). Supposons $o(\sigma) = r$ dans le groupe S_n et posons $G = \langle\sigma\rangle$. En considérant G comme opérant de façon naturelle sur $\mathbf{N}_n = \{1, 2, ..., n\}$, on a, pour tout $i \in \mathbf{N}_n$:
   $\Omega_i = \{\sigma^k(i); 1 \leqslant k \leqslant r\}$. Ω_i coïncide avec ce que l'on a appelé la σ-orbite de i.

II) Propriétés des stabilisateurs et des orbites

Théorème 1.13. *Soit E un G-ensemble ; alors, quels que soient x et y dans E, on a*

$x\rho_G y \Rightarrow G_x$ *et* G_y *conjugués dans* $\mathscr{P}(G)$.

preuve : On suppose que G opère sur E par l'application

$$G \times E \to E$$
$$(g, x) \mapsto g.x$$

$$x\rho_G y \Leftrightarrow \exists g \in G, y = g.x,$$

montrons alors que $G_y = gG_xg^{-1}$.

Soit $g' \in G_y$, on a $y = g'.y$, d'où $g.x = g'.(g.x)$ et par suite $x = g^{-1}g'g.x$.

On en déduit que $g^{-1}g'g \in G_x$, donc $g' \in gG_xg^{-1}$, ce qu'implique $G_y \subseteq gG_xg^{-1}$.

Réciproquement, soit $g_1 \in gG_xg^{-1}$, alors :

$$g^{-1}g_1g \in G_x \Rightarrow g^{-1}g_1g.x = x,$$

d'où $g_1g.x = gx$, c'est-à-dire $g_1.y = y$.

On a donc $g_1 \in G_y$, par suite $gG_xg^{-1} \subseteq G_y$.

G_y est donc conjugué de G_x par g. □

Théorème 1.14. *E étant un G-ensemble, pour tout $x \in E$, on a :*

$$|\Omega_x| = [G : G_x] \tag{1.14}$$

$|\Omega_x|$ désignant le cardinal de Ω_x.

preuve : On suppose que G opère à gauche sur E.

Pour démontrer (1.14), montrons qu'il existe une bijection de Ω_x sur $\left(\frac{G}{G_x}\right)_g$.

$\Omega_x = \{g.x; g \in G\}$; posons $Q_x = (\frac{G}{G_x})_g = \{gG_x; g \in G\}$.

Soit

$$\lambda : \Omega_x \to Q_x$$
$$g.x \mapsto gG_x$$

- λ est une application : en effet, supposons $g.x = g'.x$; on a alors $x = g^{-1}g'.x$, donc $g^{-1}g' \in G_x$, ce qui implique $gG_x = g'G_x$;

- la définition de λ implique sa surjectivité ;
- λ est injective : en effet,

$$g_1 G_x = g_2 G_x \Rightarrow g_1^{-1} g_2 \in G_x$$
$$g_1^{-1} g_2 \in G_x \Rightarrow g_1^{-1} g_2 x = x,$$

donc $g_1 G_x = g_2 G_x \Rightarrow g_1.x = g_2.x$

En conclusion, λ est une bijection, d'où l'égalité (1.14).

□

Corollaire 1.15. *Soit G un groupe opérant sur $\mathscr{P}(G)$ par conjugaison ; pour tout $S \in \mathscr{P}(G)$, on a ;*

$$|\Omega_S| = [G : \mathbf{N}_G(S)] \tag{1.15}$$

Corollaire 1.16. *Soit E un ensemble fini et G un groupe opérant sur E. Si $\{x_i\}_{1 \leqslant i \leqslant r}$ est une famille de représentants des G-orbites distinctes, alors :*

$$|E| = \sum_{i=1}^{r} [G : G_{x_i}] \tag{1.16}$$

preuve : E étant fini, chaque G-orbite est un ensemble fini et le nombre des G-orbites est fini. Si $\{x_i\}_{1 \leqslant i \leqslant r}$ est une famille de représentants des G-orbites distinctes de E, les $\Omega_{x_i} (1 \leqslant i \leqslant r)$ forment une partition de E, d'où

$$|E| = \sum_{i=1}^{r} |\Omega_{x_i}|$$

L'application de la forme (1.14) donne alors

$$|E| = \sum_{i=1}^{r} [G : G_{x_i}]$$

. □

Corollaire 1.17. *Soit G un groupe fini opérant sur lui-même par conjugaison.*
Si $\{x_i\}_{1 \leqslant i \leqslant r}$ est une famille de représentants des classes de conjugaison distinctes dans G :

$$o(G) = \sum_{i=1}^{r} [G : C_G(x_i)] \tag{1.17}$$

où : $C_G(x_i)$ est le centralisateur de x_i dans G.
La relation précédente est appelée ≪ équation de classes ≫ du groupe fini G.

Remarque 1.2.1. Soit G un groupe opérant sur lui-même par conjugaison ; $Z(G)$ étant son centre :

$$x \in Z(G) \Leftrightarrow C_G(x) = G,$$

c'est-à-dire

$$x \in Z(G) \Leftrightarrow [G : C_G(x)] = 1,$$

ou encore,

$$x \in Z(G) \Leftrightarrow \Omega_x = \{x\}.$$

Définition 1.12. *Si E est un G-ensemble, toute G-orbite réduite à un seul élément est dite ponctuelle.*

Théorème 1.18. *Soit G un groupe fini de centre $Z(G)$.*
Soit $\{x_i\}_{1\leqslant i\leqslant r}$ une famille de représentants des classes de conjugaison distinctes et non ponctuelles de G, alors :

$$o(G) = o(Z(G)) + \sum_{i=1}^{k} [G : C_G(x_i)] \tag{1.18}$$

preuve : On remarque que, si G est abélien, toutes les classes de conjugaison sont ponctuelles et $G = Z(G)$, la formule (1.18) est vérifiée.
Supposons G non abélien ; $Z(G) \neq G$ implique qu'il existe des classes de conjugaison non ponctuelles dans G.
Soit, comme dans le corollaire 1.17, $\{x_i\}_{1\leqslant i\leqslant r}$ une famille de représentants des classes de conjugaison distinctes de G ; alors (en changeant éventuellement l'ordre des indices) il existe k $(1 \leqslant k < r)$ tel que

$$x_i \notin Z(G) \quad \text{pour } 1 \leqslant i \leqslant k$$

et $$x_i \in Z(G) \quad \text{pour } k+1 \leqslant i \leqslant r.$$

La relation (1.18) s'obtient alors à partir de la relation (1.17), en remplaçant $[G : C_G(x_i)]$ par 1 pour $k+1 \leqslant i \leqslant r$, et chaque classe de conjugaison de $x_i \in Z(G)$ étant ponctuelle, nécessairement $r - k = o(Z(G))$. □

Remarque 1.2.2. Les hypothèses et les notations étant celles du théorème 1.18, en désignant par Ω_{x_i} la classe de conjugaison de x_i pour $1 \leqslant i \leqslant k$, la formule (1.18) s'écrit :

$$o(G) = o(Z(G)) + \sum_{i=1}^{k} |\Omega_{x_i}| \tag{1.19}$$

et l'égalité $|\Omega_{x_i}| = [G : C_G(x_i)]$ implique que le cardinal de la classe de conjugaison d'un élément quelconque de G divise l'ordre du groupe G.

Théorème 1.19. *Si G est un groupe fini d'ordre p^n, p étant un nombre premier et $n \geqslant 1$ dans* **N**, *alors le centre de G n'est pas réduit à l'élément neutre.*

preuve : Si G est abélien, $Z(G) = G$ et l'hypothèse $n \geqslant 1$ implique $G \neq (e)$.
Supposons G non abélien ; la formule (1.18) implique

$$o(Z(G)) = p^n - \sum_{i=1}^{k} [G : C_G(x_i)],$$

avec $[G : C_G(x_i)] > 1$ pour tout i $(1 \leqslant i \leqslant k)$. Or chaque $[G : C_G(x_i)]$ divise $o(G) = p^n$; on en déduit que p divise $\sum_{i=1}^{k} [G : C_G(x_i)]$ et, par suite, p divise $o(Z(G))$; d'où $o(Z(G)) > 1$. □

Corollaire 1.20. *Si p est un nombre premier, alors tout groupe fini d'ordre p^2 est abélien.*

preuve : Soit G un groupe d'ordre p^2 ; d'après le théorème 1.19 on a $Z(G) \neq (e)$; alors,
Soit $o(Z(G)) = p^2$, donc G est abélien ;
Soit $o(Z(G)) = p$ et dans ce cas $\dfrac{G}{Z(G)}$ est d'ordre premier p, donc cyclique, ce qui implique G abélien. □

Définition 1.13. *On dite qu'un groupe G opère transitivement sur un ensemble E, si E n'a qu'une seule G-orbiter (qui est nécessairement E) ; autrement dit, si :*

$$\forall (x, y) \in E \times E,\ \exists g \in G,\ y = g.x.$$

Dans ce cas, on dit que E est un G-ensemble homogène, ou que G est transitif sur E.
Dans le cas contraire, on dit que G opère intransitivement sur E ou que G est intransitif sur E.

Remarque 1.2.3. Pour un groupe G opère transitivement sur un ensemble E, il faut et il suffit qu'il existe $x \in E$ tel que $\Omega_x = E$.

Proposition 1.21. *G étant un groupe, quel que soit $H \leqslant G$, G opère transitivement par translation à gauche sur l'ensemble $Q_H = \left(\dfrac{G}{H}\right)_g$.*
De plus, si E est un G-ensemble homogène, alors il existe $H \leqslant G$ tel que E soit équipotent à Q_H.

preuve : D'après cette exemple : Soit H un sous-groupe de G ; alors G opère par translation à gauche, sur l'ensemble $\left(\dfrac{G}{H}\right)_g$ des classes à gauche de G modulo H.

En effet, posons $Q_H = \left(\frac{G}{H}\right)_g$, Q_H est une partie non vide de $\mathscr{P}(G)$; vérifions que la correspondance

$$G \times Q_H \to Q_H$$
$$(g, xH) \mapsto gxH.$$

est une application.
Supposons $xH = yH$, donc $y^{-1}x \in H$; pour tout $g \in G$, $(gy)^{-1}gx = y^{-1}g^{-1}gx = y^{-1}x$ appartient à H, d'où $gxH = gyH$.
Ainsi G opère sur Q_H par translation à gauche.

G opère sur Q_H par l' application :

$G \times Q_H \to Q_H$

$(g, xH) \mapsto gxH$

$H \in Q_H$ et $\Omega_H = \{gH; g \in G\} = Q_H$, par suite, G opère transitivement sur Q_H. Soit E un G-ensemble homogène ; on a $E = \Omega_x$, quel que soit $x \in E$.
D'autre part, d'après le théorème 1.14, Ω_x est équipotent à $\left(\frac{G}{G_x}\right)_g$, d'où E équipotent à Q_{G_X}. □

Définition 1.14. *Soit G un groupe opérant sur un ensemble E. On dit que G opère fidèlement sur E, si*

$(g \in G \text{ et } g.x = x, \forall x \in E) \Rightarrow g = e$;

autrement dit, si le morphisme de groupes

$$\gamma : G \to S_E$$
$$g \mapsto \gamma_g$$

tel que $\gamma_g(x) = g.x$ pour tout $x \in E$,est injectif.

Remarque 1.2.4. Si G opère fidèlement sur un ensemble E, alors G est isomorphe à un sous-groupe de S_E.

Exemple 1.2.2.

1. G opère fidèlement sur G, par translation à gauche.
2. G n'opère pas fidèlement sur G, par conjugaison.

1.2.3 Classes de conjugaison. Normalisateur

Définition 1.15. *Soient G un groupe et $S \neq \varnothing$ dans $\mathscr{P}(G)$. On dit que $S' \in \mathscr{P}(G)$ est conjuguée de S, s'il existe $x \in G$ tel que $S' = xSx^{-1}$, où $xSx^{-1} = \{xsx^{-1}; s \in S\}$. On vérifie facilement que la relation de conjugaison est une relation d'équivalence dans $\mathscr{P}(G)$, avec la partie vide comme conjuguée d'elle-même.*
Soit $S \neq \varnothing$ dans $\mathscr{P}(G)$, la classe d'équivalence de S modulo la relation de conjugaison est l'ensemble $\{xSx^{-1}; x \in G\}$, appelé classe de conjugaison de S.

Remarque 1.2.5.

1. Si S et S' sont conjuguées, non vides, dans $\mathscr{P}(G)$ et telles que $S' = xSx^{-1}$, alors S' est l'image de S par l'automorphisme intérieur σ_x ; par suite, S et S' sont des ensembles équipotents ; en particulier, si S est fini, tout S' conjugué de S est fini et $|S'| = |S|$.
2. Si $S = \{g\}$ où $g \in G$, la classe de conjugaison de S est dite classe de conjugaison de conjugaison de g ; elle est formée par l'ensemble des xgx^{-1}, x décrivant G.
   Tout $xgx^{-1} = \sigma_x(g)$ est dit conjugué de g dans G, et la relation de conjugaison dans G est une relation d'équivalence.
3. Si H est un sous-groupe de G, tout conjugué de H étant de la forme
   $H' = xHx^{-1} = \sigma_x(H)$ est un sous-groupe de G isomorphe à H.

Définition 1.16. *Soit une partie non vide S d'un groupe G, on appelle normalisateur de S dans G l'ensemble*

$$N_G(S) = \{x \in G;\ xSx^{-1} = S\} \tag{1.20}$$

On vérifie simplement que, $\forall\ S \neq \varnothing$ dans $\mathscr{P}(G)$, $N_G(S)$ est un sous-groupe de G.
Si $S = \{g\}$, où $g \in G$,

$$N_G(g) = \{x \in G;\ xgx^{-1} = g\} = \{x \in G;\ xg = gx\}.$$

c'est-à-dire que $N_G(g)$ coïncide avec le centralisateur de g dans G, noté $\mathbf{C}_G(g)$.
Pour $S \in \mathscr{P}(G)$, tel que $|S| > 1$, le centralisateur de S dans G :

$$C_G(S) = \{x \in G; xsx^{-1} = s, \forall s \in S\}$$

est, en général, un sous-groupe propre de $N_G(S)$ et on vérifie que $C_G \lhd N_G(S)$. La notion de normalisateur fournit une nouvelle caractérisation des sous-groupe normaux.

Théorème 1.22. *Soit H un sous-groupe d'un groupe G, alors :*

$$H \lhd G \;\Leftrightarrow\; N_G(H) = G.$$

Proposition 1.23. *Soit G un groupe :*

a) pour tout sous-groupe H de G, on a $H \lhd N_G(H)$.

b) Si H et K sont deux sous-groupes de G tels que $H \leqslant K$, alors :

$$H \lhd K \Rightarrow K \leqslant N_G(H).$$

c) $K \leqslant N_G(H) \Rightarrow HK \leqslant G$. et $H \lhd HK$.

preuve :

a) On remarque que la définition de $N_G(H)$ implique $H \subseteq N_G(H)$; d'autre part :

$$x \in N_G(H) \;\Leftrightarrow\; xHx^{-1} = H,$$

d'où $H \lhd N_G(H)$.

b) Si l'on a $H \leqslant K \leqslant G$, alors :

$$H \lhd K \Rightarrow kHk^{-1} = H,\ \forall k \in K,$$

d'où $K \leqslant \mathbf{N}_G(H)$.

c) Soit K un sous-groupe de $N_G(H)$; considérons $h \in H$ et $k \in K$; on a $k \in N_G(H)$, donc $k^{-1} \in N_G(H)$, par suite $k^{-1}Hk = H$; on en déduit qu'il existe $h' \in H$ tel que $k^{-1}hk = h'$, d'où $hk = kh'$, ce qui implique $HK \subseteq KH$.

De façon analogue on montre que $KH \subseteq HK$, donc HK est un sous-groupe de G

$$H \subseteq N_G(H) \quad \text{et} \quad K \subseteq N_G(H) \quad \text{implique } Hk \subseteq N_G(H)\,;$$

or d'après a) H est normal dans $N_G(H)$, qui est un sous-groupe de HK, est normal dans HK.

□

Remarquons que pour tout sous-groupe H de G, $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal.

1.3 Groupes cycliques

1.3.1 Sous-groupe engendré par une partie non vide d'un groupe

Définition 1.17. *Soient G un groupe et S une partie non vide de G ; désignons par $\mathscr{H}_S$ l'ensemble des sous-groupes de G contenant S et posons :*

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

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

On remarque que dans l'ensemble des sous-groupes de G ordonné par l'inclusion, $\langle\ S\ \rangle$ et le plus petit sous-groupe de G contenant S.

Proposition 1.24. *S étant une partie non vide d'un groupe G,*
on a :

$$\langle\ S\ \rangle = \Big\{x_1x_2\dots x_n;\ n\in\mathbf{N}^*,\ x_i\in S \quad ou \quad x_i^{-1}\in S,\ \forall\ i\ (1\leqslant i\leqslant n)\Big\} \tag{1.21}$$

preuve : Posons $H = \Big\{x_1x_2\dots x_n;\ n\in\mathbf{N}^*,\ x_i\in S \quad ou \quad x_i^{-1}\in S,\ \forall\ i\ (1\leqslant i\leqslant n)\Big\}$ et montrons que $H = \langle\ S\ \rangle$.
On remarque que tout x de S appartient à H, d'où $S\subseteq H$.
Montrons que H est un sous-groupe de G. Considérons $x = x_1x_2\dots x_n$ et $y = y_1y_2\dots y_n$ dans H ; alors,
$xy^{-1} = x_1x_2\dots x_ny_p^{-1}y_{p-1}^{-1}\dots y_1^{-1}$ appartient à H. On en déduit que H est un élément de l'ensemble $\mathscr{H}_S$, d'où $\langle\ S\ \rangle\subseteq H$.

D'autre part, tout sous-groupe de G contenant S contient nécessairement tous les éléments de H, par suite $H = \langle\ S\ \rangle$. □

cas particuliers :

1. $S = \bigcup_{i\in I} H_i$, où $\{H_i\}_{i\in I}$ est une famille de sous-groupes de G ; dans ce cas,
   $x\in S\Leftrightarrow x^{-1}\in S$; par suite

$$\langle\ S\ \rangle = \left\{x_1x_2\dots x_n;\ n\in\mathbf{N}^*,\ x_i\in\bigcup_{\alpha\in I} H_i,\ \forall\ \alpha\ (1\leqslant\alpha\leqslant n)\right\} \tag{1.22}$$

2. $S = \{x\}\,,\ x \in G;\ \langle\ S\ \rangle$ s'écrit alors $\langle\ x\ \rangle$ et

$$\langle\ x\ \rangle = \{x^n;\ n \in \mathbf{Z}\} \tag{1.23}$$

Pour $x = e$, nous conserverons la notation (e), à la place de $\langle\ e\ \rangle$.

Remarque 1.3.1. Si la loi de composition du groupe G est notée additivement, les formules (1.21) et (1.23) deviennent respectivement :

$$\langle\ S\ \rangle = \left\{\sum_{i=1}^{n} x_i;\ n \in \mathbf{N}^*,\ x_i \in S, ou - x_i \in S, \forall\ i\ (1 \leqslant i \leqslant n)\right\} \tag{1.24}$$

$$\langle\ x\ \rangle = \{nx;\ n \in \mathbf{Z}\} \tag{1.25}$$

1.3.2 Groupes cycliques

Définition 1.18. *Si S est une partie non vide de G tell que $\langle\ S\ \rangle = G$, on dit que S est une* ***partie génératrice*** *du groupe G, ou que S est un* ***ensemble de générateurs*** *de G, ou encore que S* ***engendre*** *G.*

Définition 1.19. *S'il existe $x \in G$ tel que $\langle\ x\ \rangle = G$, le groupe G est dit* ***cyclique****.*

Plus généralement, s'il existe une partie non vide et finie de G, $S = \{x_1, x_2, \ldots, x_n\}$, telle que $\langle\ S\ \rangle = G$, on dit que le groupe G est de ***type fini****.*
Un groupe fini est nécessairement de type fini, mais la réciproque est fausse.

Exemple 1.3.1. Puisque tout $n \in \mathbf{Z}$ s'écrit $1 + 1 + \ldots + 1$ si $n > 0$,
$(-1) + (-1) + \ldots + (-1)$ si $n < 0$ et $0 = 1 + (-1)$, $\mathbf{Z}$ est un sous-groupe cyclique engendré par 1.

Proposition 1.25. *Toute image homomorphe d'un groupe cyclique est cyclique.*

prouve : Soit un groupe cyclique $G = \langle\ x\ \rangle$ et soit G' un groupe image homomorphe de G ; f étant un épimorphisme de G sur G',

$$G = \left\{x^k;\ k \in \mathbf{Z}\right\} \Rightarrow Imf = G' = \left\{(f(x))^k\,;\ k \in \mathbf{Z}\right\},$$

donc G' est cyclique engendré par $f(x)$. □

1.3.3 Groupes cycliques finis

Définition 1.20. *On appellera* ***groupe cyclique fini*** *tout groupe cyclique d'ordre fini.*

Corollaire 1.26. $\forall n \in \mathbf{N}^*$, *le groupe* $\dfrac{Z}{nZ}$ *est cyclique fini.*

En effet, $(\mathbf{Z}, +)$ est cyclique engendré par 1 ; d'autre part, la surjection canonique $\pi : (\mathbf{Z}, +) \to \left(\dfrac{\mathbf{Z}}{n\mathbf{Z}}, +\right)$ est un épimorphisme de groupes, donc $\left(\dfrac{\mathbf{Z}}{n\mathbf{Z}}, +\right)$ est cyclique, engendré par $\pi(1) = \bar{1}$, et comme $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ est fini d'ordre n, $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ est cyclique fini.

Théorème 1.27. *Si G est un groupe cyclique, alors G vérifie l'une des conditions suivantes :*

1) $G \simeq \mathbf{Z}$ *; dans ce cas G est cyclique infini.*

2) *Il existe $n > 0$ dans $\mathbf{N}$ tel que $G \simeq \dfrac{\mathbf{Z}}{n\mathbf{Z}}$, alors G est cyclique fini d'ordre n.*

Preuve : soit un groupe cyclique : $G = \langle\ x\ \rangle = \left\{x^k;\ k \in \mathbf{Z}\right\}$
Considérons l'application :

$$\begin{aligned} \psi : \mathbf{Z} &\to G \\ k &\mapsto x^k \end{aligned}$$

La définition de ψ implique sa surjectivité.
D'autre part, $\psi(k+l) = x^{k+l} = x^k x^l$, donc ψ est un épimorphisme de groupes.On a donc deux cas :

premier cas : ψ est injectif ; par suite, ψ est un isomorphisme de groupes, d'où $G \simeq \mathbf{Z}$; G est donc cyclique infini.

deuxième cas : ψ est non injectif ; *ker* ψ est alors un sous-groupe non nul de $\mathbf{Z}$, donc il existe un unique $n > 0$ dans $\mathbf{N}$ tel que *ker* $\psi = n\mathbf{Z}$.

D'après le 1er théorème d'isomorphisme on a :

$$Im\ \psi \simeq \frac{G}{ker\ \psi}$$

donc, $G \simeq \dfrac{\mathbf{Z}}{n\mathbf{Z}}$; G est cyclique fini d'ordre n. □

Proposition 1.28. *Si $G = \langle\ x\ \rangle$ est un groupe cyclique fini d'ordre n, dont l'élément neutre est e, alors :*

$$(k \in \mathbf{Z}\ et\ x^n = e) \Leftrightarrow k \in n\mathbf{Z}$$

et n le plus petit entier strictement positif tel que $x^n = e$.

preuve : Si $G = \langle\ x\ \rangle$ est cyclique fini d'ordre n, $n\mathbf{Z}$ est le noyau l'épimorphisme $\psi : \mathbf{Z} \to G$ tel que $\psi(k) = x^k$; par suite

$$\left(k \in \mathbf{Z}\ et\ x^k = e\right) \Leftrightarrow k \in n\mathbf{Z}.$$

n est donc dans $\mathbf{N}^*$, le plus petit entier tel que $x^n = e$. □

Proposition 1.29. *Tout groupe fini d'ordre premier p est cyclique.*

prouve : Soit G un groupe fini d'ordre premier p ; p étant plus grand que 1, il existe $x \in G$ tel que $x \neq e$. Si $m = o(x)$, on a $m \neq 1$ et m divise p (théorème de Lagrange) ; par suite $m = p$, donc $G = \langle\ x\ \rangle$. □

1.3.4 Sous-groupes d'un groupe cyclique

a) Propriété générale :

Théorème 1.30. *Tout sous-groupe , non réduit à l'élément neutre, d'un groupe cyclique infini est cyclique infini.*

Preuve : D'après le théorème 1.27 il suffit de montrer que tous sous-groupe non nul de $\mathbf{Z}$ est cyclique infini.
On sait que tout sous-groupe non nul de $\mathbf{Z}$ est de la forme $n\mathbf{Z}$, $n \neq 0$ dans $\mathbf{N}$.

$$n\mathbf{Z} = \{nk = kn;\ k \in \mathbf{Z}\},$$

et $k \neq l$ dans $\mathbf{Z}$ implique $kn \neq ln$, donc $n\mathbf{Z}$ est un groupe (additif) cyclique infini engendré par n. □

Théorème 1.31. *Tout sous-groupe d'un groupe cyclique fini est cyclique fini.*

Preuve : D'après le théorème 1.27 il suffit de montrer que pour $n \neq 0$ dans N, tout sous-groupe de $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ est cyclique fini.
Soit $n \neq 0$ dans $\mathbf{N}$ et π l'épimorphisme canonique $\mathbf{Z} \to \dfrac{\mathbf{Z}}{n\mathbf{Z}}$.
Soit K un sous-groupe de $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$, π étant surjectif, on a $K = \pi(\pi^{-1}(K))$; or $\pi^{-1}(K)$ est un sous groupe de $\mathbf{Z}$, donc il existe un unique $k \in \mathbf{N}$ tel que $\pi^{-1}(K) = k\mathbf{Z}$.
K est alors l'image homomorphe par π du groupe monogène $k\mathbf{Z}$, par suite K est cyclique, engendré par $\pi(k)$ (proposition 1.25) et K est cyclique fini, puisque K est fini. □

b) Sous-groupes d'un groupe cyclique fini : Etudions, tout d'abord, les sous-groupes de $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$, pour $n \neq 0$ dans $\mathbf{N}$.
En reprenant les notions de la démonstration du théorème 1.31, on remarque que, K étant un sous-groupe de $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$,
$\pi(0) = \bar{0}$ appartient à K ; par suite, on a :

$$\pi^{-1}(\bar{0} \subseteq \pi^{-1}(K),$$

c'est-à-dire $n\mathbf{Z} \subseteq k\mathbf{Z}$; autrement dit, k divise n dans $\mathbf{N}^*$.

Déterminons l'ordre du sous-groupe K.
Posons $\pi(k) = \bar{k}$; on a $K = \langle\ \bar{k}\ \rangle$ dans $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$, d'où

$$o(K) = o(\bar{k})\ \textit{dans}\ \frac{\mathbf{Z}}{n\mathbf{Z}}$$

$o(\bar{k})$ est le plus petit entier $d > 0$, tel que $d\bar{k} = \bar{0}$.
Or, $d\bar{k} = d\pi(k) = \pi(dk)$, puisque π est un morphisme de groupes additifs. k divisant n dans $\mathbf{N}^*$, $o(\bar{k})$ est nécessairement l'entier $d = \dfrac{n}{k}$.
On a ainsi prouvé la propriété suivante :

Proposition 1.32. *Soient $n \in \mathbf{N}^*$ et π l'épimorphisme canonique $\mathbf{Z} \to \dfrac{\mathbf{Z}}{n\mathbf{Z}}$. Pour tout sous-groupe K de $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ il existe un unique diviseur k de n dans $\mathbf{N}^*$, tel que $\pi(k)$ engendre K et $o(K) = \dfrac{n}{k}$.*

Corollaire 1.33. *Le nombre des sous-groupes de $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ ($n \neq 0$ dans $\mathbf{N}$) est égal au nombre des diviseurs de n dans $\mathbf{N}^*$.*

En effet, d'après la proposition 1.32, $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ n'a pas d'autres sous-groupes que les $\langle\ \pi(k)\ \rangle$ où k divise n dans $\mathbf{N}^*$. De plus, si k et k' sont deux diviseurs de n, tels que $k \neq k'$ dans $\mathbf{N}^*$, les ordres des sous-groupes $\langle\ \pi(k)\ \rangle$ et $\langle\ \pi(k')\ \rangle$ sont respectivement $\dfrac{n}{k}$ et $\dfrac{n}{k'}$, donc ces sous-groupes sont distincts.

Si $n > 1$, on remarque que n a au moins deux diviseurs distincts dans $\mathbf{N}^*$, 1 et n qui correspondent, respectivement, au sous-groupe plein $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$ et au sous-groupe réduit à l'élément neutre $(\bar{0})$.

Exemple 1.3.2. Les diviseurs de 8, dans $\mathbf{N}$, étant $1, 2, 4, 8$, on peut affirmer que $\dfrac{\mathbf{Z}}{8\mathbf{Z}}$ a quatre sous-groupes distincts :

$$\langle\ \bar{1}\ \rangle = \frac{\mathbf{Z}}{8\mathbf{Z}},\ \langle\ \bar{2}\ \rangle = \left\{\bar{2}, \bar{4}, \bar{6}, \bar{0}\right\},\ \langle\ \bar{4}\ \rangle = \left\{\bar{4}, \bar{0}\right\}\ \textit{et}\ \langle\ \bar{8}\ \rangle = (\bar{0}).$$

Proposition 1.34. *Soit G un groupe non réduit à l'élément neutre e ; alors G n'a pas d'autre sous-groupe que G et (e), si et seulement si G est cyclique fini d'ordre premier.*

preuve : Soit G un groupe cyclique fini d'ordre premier p ; $p > 1$ implique $G \neq (e)$; d'après le théorème de Lagrange, l'ordre d'un sous-groupe de G ne peut être que 1 ou p, donc G n'a pas d'autre sous-groupe que (e) et G.

Réciproquement, considérons un groupe $G \neq (e)$ dont les seuls sous-groupes sont G et (e).
Soit $x \neq e$ dans G ; le sous-groupe $\langle\ x\ \rangle$ de G est nécessairement différent de (e), donc $\langle\ x\ \rangle = G$, c'est-à-dire que G est cyclique.

Si G était infini, G serait isomorphe à $\mathbf{Z}$, donc aurait d'autres sous-groupes que G et (e) ; par suite, G est cyclique fini .

G n'ayant pas d'autre sous-groupe que G et (e), l'ordre de G n'a pas dans $\mathbf{N}^*$, d'autre diviseur que lui-même est 1, c'est donc un nombre premier.

□

CHAPITRE 2

GROUPE FINI (THÉORÈMES DE SYLOW)

Théorème de Lagrange : l'ordre d'un sous-groupe H de G divise l'ordre du groupe G. Soit G un groupe d'ordre m, d'après le théorème de Lagrange, toute sous-groupe de G a un ordre qui divise m. Par contre, si d est un entier positive divisant m, il n'existe pas nécessairement un sous-groupe de G, d'ordre d. Par exemple, le groupe alterné A_4, d'ordre 12, n'a pas de sous-groupe d'ordre 6.
Nous allons voir dans ce chapitre que le premier théorème de Sylow peut affirmer que, si le diviseur d de m est une puissance d'un nombre premier, alors le groupe G a au moins un sous-groupe d'ordre d. Le second théorème de Sylow donnera une indication sur le nombre de certains de ces sous-groupes.

2.1 Théorèmes de Sylow

2.1.1 Premier théorème de Sylow

Théorème 2.1. *Soient G un groupe fini et p un nombre Premier divisant l'ordre de G. Si $o(G) = sp^n$, avec s non divisible par p, alors pour tout entier r $(1 \leqslant r \leqslant n)$. il existe un sous-groupe de G d'ordre p^r.*

Il ya plusieurs démonstrations de ce théorème ; celle qui est donnée ici, elle utilise la notion de groupe opérant sur un ensemble et s'appuie sur le lemme suivant :

Lemme 2.2. *Pour a et b entiers positifs, notons C_a^b le nombre de combinaison de a élément b à b.*

Autrement dit, si X est un ensemble fini de cardinal a, le nombre des parties de X de cardinal b est C_a^b. D'après un résultat d'analyse combinatoire :

$$C_a^b = \frac{a(a-1)...(a-b+1)}{b!} = \frac{a!}{b!(a-b)!} \tag{2.1}$$

Compte tenu des notations du théorème 2.1, démontrons que pour tout entier r $(1 \leqslant r \leqslant n)$, on a

$$C_{sp^n}^{p^r} = \lambda p^{n-r}, \text{ où } \lambda \text{ est un entier non divisible par } p \tag{2.2}$$

D'après (2.1),

$$C_{sp^n}^{p^r} = \frac{sp^n}{p^r} \cdot \frac{sp^n-1}{1} \cdot \frac{sp^n-2}{2} \cdots \frac{sp^n-(p^r-1)}{p^r-1}$$

$$C_{sp^n}^{p^r} = sp^{n-r} \cdot \frac{sp^n-1}{1} \cdots \frac{sp^n-(p^r-1)}{p^r-1}$$

$C_{sp^n}^{p^r}$ étant un entier, il suffit de prouver que chaque fraction $\frac{sp^n-k}{k}$ est égale à une fraction irréductible dont ni le dénominateur, ni numérateur n'est divisible par p.

Pour tout k $(1 \leqslant k \leqslant p^r-1)$, on peut écrire : $k = qp^\alpha$, avec $0 \leqslant \alpha < r$ et q non divisible par p dans **N** *, alors $\frac{sp^n-k}{k} = \frac{sp^n-qp^\alpha}{qp^\alpha} = \frac{sp^{n-\alpha}-q}{q}$;*
p ne divise pas q, donc p ne divise pas $sp^{n-\alpha}-q$, ce qui implique la relation (2.2).

Preuve du premier théorème de Sylow : Etant donné entier $r(1 \leqslant r \leqslant n)$, notons $\mathscr{F}$ l'ensemble des parties de G, le cardinal p^r.

D'après le lemme 2.2, $\mathscr{F}$ est un ensemble fini de cardinal $C_{sp^n}^{p^r}$ et en tenant compte de (2.2), on a

$|\mathscr{F}| = \lambda p^{n-r}$, où λ est un entier, non divisible par p.

Si $A \in \mathscr{F}$, pour toute $g \in G$, $|gA| = |A| = p^r$; par suite, G opère sur $\mathscr{F}$ par translation à gauche.

Soit $\{A_i\}_{1 \leqslant i \leqslant k}$ une famille de représentants des $G-$ orbites distinctes de $\mathscr{F}$, donc,

$$|\mathscr{F}| = \sum_{i=1}^{k} [G : G_{A_i}],$$

où, pour toute i $(1 \leqslant i \leqslant k)$, G_{A_i} est le stabilisateur de A_i dans G ; par suite on a :

$$\sum_{i=1}^{k} [G : G_{A_i}] = \lambda p^{n-r}, \ \lambda \text{ est un entier non divisible par } p.$$

On en déduit qu'il existe au moins un entier h $(1 \leqslant h \leqslant k)$ tel que λp^{n-r+1} ne divise par $[G : G_{A_h}]$.
posons alors $H = G_{A_h}$.
$o(G) = sp^n \Rightarrow sp^n = o(H)[G : H]$.
par hypothèse, p^{n-r+1} ne divise pas $[G : H]$, donc, $[G : H] = s'p^\alpha$, où s' divise s
et $0 \leqslant \alpha \leqslant n - r$, dans $\mathbf{N}$.
En posant $s = s's''$, on a $o(H) = s''p^{n-\alpha}$; $0 \leqslant \alpha \leqslant n - r \Rightarrow r \leqslant n - \alpha \leqslant n$,
par suite, p^r divise $o(H)$, d'où $p^r \leqslant o(H)$.

D'autre part, $H = G_{A_h}$, où $A_h \in \mathscr{F}$.
$\forall g$ *et* g' dans G_{A_h}, on a

$$gA_h = g'A_h = A_h$$

et $g \neq g' \Rightarrow gx \neq g'x,\ \forall x \in A_h$.

On en déduit que $|G_{A_h}| \leqslant |A_h| = p^r$, c'est-à-dire $o(H) \leqslant p^r$, ce qui conduit à la conclusion : $o(H) = p^r$. □

L'application du théorème 2.1 dans le cas $r = 1$, puis le cas $r = n$, donne les deux résultats suivants :

Corollaire 2.3. *(Théorème de Cauchy) :*
G étant un groupe fini, si p est un nombre premier divisant l'ordre de G, alors G a au moins un élément d'ordre p.

Corollaire 2.4. *si G est un groupe fini d'ordre sp^n, où p est un nombre premier ne divisant pas s, alors G contient au moins un sous-groupe d'ordre p^n.*

2.1.2 p-groupe et p-sous-groupe

Définition 2.1. *Si G est un groupe fini, on dit que G est un **p-groupe**, si $o(G) = p^n$, où p est un nombre premier et $n \in \mathbf{N}$.*

Exemple 2.1.1.

1. $(\mathbb{Z}/_{4\mathbb{Z}}, +)$ est 2-groupe car $|\mathbb{Z}/_{4\mathbb{Z}}| = 2^2$.
2. $(\mathbb{Z}/_{27\mathbb{Z}}, +)$ est 3-groupe car $|\mathbb{Z}/_{27\mathbb{Z}}| = 3^3$.
3. S_2 est 2-groupe car $|S_2| = 2! = 2$

4. A_3 est 3-groupe car $|A_3| = \dfrac{3!}{2} = 3$

Définition 2.2. *Soit un groupe fini G et un nombre premier p divisant $o(G)$, un sous-groupe H est un* ***p-sous-groupe*** *de G, si $o(H) = p^r,\ r \geqslant 0$ dans $\mathbf{N}$.*

Définition 2.3. *Si G est un groupe fini d'ordre sp^n, où p est un nombre premier ne divisant pas s, alors tout sous-groupe d'ordre p^n de G est appelé :* ***p-sous-groupe de Sylow*** *de G.*

Exemple 2.1.2. Dans $(\mathbb{Z}/_{12\mathbb{Z}}, +)$ le sous groupe engendré par $\bar{3}$ est $\langle\ \bar{3}\ \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$
on a : $|\mathbb{Z}/_{12\mathbb{Z}}| = 12 = 3 \times 2^2$, et $|3\mathbb{Z}/_{12\mathbb{Z}}| = 2^2$
alors, $3\mathbb{Z}/_{12\mathbb{Z}}$ est 2-sous-groupe de Sylow de $\mathbb{Z}/_{12\mathbb{Z}}$.

2.1.3 Second théorème de Sylow

Théorème 2.5. *soient G un groupe fini et p un nombre Premier divisant l'ordre de G ; alors,*

1. *tout p-sous-groupe de G est contenue dans un p-sous-groupe de Sylow de G.*
2. *les p-sous-groupe de Sylow de G sont conjugués.*
3. *le nombre des p-sous-groupe de Sylow de G est congru à 1 modulo p et divise l'ordre de G.*

La démonstration de ce théorème s'appuie sur les lemmes suivants :

Lemme 2.6. *Soit G un groupe fini d'ordre p^n, p étant un nombre Premier et $n \geqslant 1$ dans $\mathbf{N}$. Si G opère sur un ensemble fini E, alors :*

$$|E_G| \equiv |E| \ (mod\ p).$$

preuve : $x \in E_G \Leftrightarrow \Omega_x = \{x\}$.
$|E_G|$ est donc égal au nombre des G-orbites ponctuelles de E.
Soient $\{\Omega_{x_i}\}_{1 \leqslant i \leqslant k}$ les G-orbites non ponctuelles de E $(k \in \mathbf{N})$;
on a :

$$|E| = |E_G| + \sum_{i=1}^{k} |\Omega_{x_i}|.$$

Pour tout i $(1 \leqslant i \leqslant k)$, $|\Omega_{x_i}| = [G : G_{x_i}]$ et $|\Omega_{x_i}| \neq 1$;
on en déduit que $|\Omega_{x_i}|$ divise p^n et est de la forme p^{n_i}, $n_i \geqslant 1$ dans $\mathbf{N}$; par suite $|E| - |E_G|$ est un multiple de p, d'où $|E_G| \equiv |E| \ (mod\ p)$. □

Lemme 2.7. *soient deux sous-groupes H et K d'un groupe G tels que $[G : H] = r (r \in \mathbf{N}^*)$ et $o(K) = p^n$, p étant un nombre Premier ne divisant pas r et $n \geqslant 1$ dans $\mathbf{N}$. alors K est contenue dans un conjugué de H.*

preuve : posons $E \equiv \left(\frac{G}{H}\right)_g$; E est un ensemble fini de cardinal r. Considérons le groupe K comme opérant par translation à gauche sur E ; E_K étant l'ensemble des points fixes du K-ensemble E, d'après le lemme 2.6 :

$$|E_K| \equiv r \ (mod\ p).$$

p ne divise pas r, par suite, on a $E_K \neq \varnothing$.
Donc

$$xH \in E_K \Leftrightarrow K \leqslant G_{xH},$$

où G_{xH} est le stabilisateur de xH dans l'action de G sur E ; or $G_{xH} = xHx^{-1}$,
d'où $K \leqslant xHx^{-1}$. □

Lemme 2.8. *G étant un groupe fini, si S est un p-sous-groupe de Sylow de G, alors S est l'unique p-sous-groupe de $N_G(S)$.*

preuve : posons $o(G) = p^n s,\ p$ ne divise pas s. On remarque que S est un p-sous-groupe de Sylow de tout sous-groupe de G contenant S ; en particulier, S est un p-sous-groupe de Sylow de $N_G(S)$.
Si $o\left(N_G(S)\right) = p^n s'$, et si K est un p-sous-groupe de Sylow de $N_G(S)$, on a
$[N_G(S) : K] = s',\ p$ ne divisant pas s'.
De l'application du lemme 2.7, avec $H = S$,
on déduit qu'il existe $x \in N_G(S)$ tel que $K \leqslant xSx^{-1}$;
alors, $xSx^{-1} = S$ et $o(K) = o(S) \Rightarrow K = S$. □

Preuve du deuxième théorème de Sylow : comme ci-dessus, on pose $o(G) = p^n s,\ p$ ne divise pas s.

1. Soit H un p-sous-groupe de G ; si S un p-sous-groupe de Sylow de G, on a $[G : S] = s$ d'après le lemme 2.7 : il existe $x \in G$ tel que $H \leqslant xSx^{-1}$; mais $o(xSx^{-1}) = o(S)$, donc xSx^{-1} est un p-sous-groupe de Sylow de G.
2. Si S et S' sont deux p-sous-groupes de Sylow de G, le raisonnement ci-dessus montre qu'il existe $x \in G$ tel que $S' \leqslant xSx^{-1}$; xSx^{-1} étant un p-sous-groupe de Sylow de G, on a nécessairement $S' = xSx^{-1}$.

3. Soit $\mathscr{S}$ l'ensemble des p-sous-groupes de Sylow de G.

   D'après le résultat précédent, G opère transitivement par conjugaison sur $\mathscr{S}$. Notons Ω_S la classe de conjugaison d'un élément $S \in \mathscr{S}$, alors :

$$|\mathscr{S}| = |\Omega_S| = [G : N_G(S)]\,;$$

   par suite, $|\mathscr{S}|$ divise $o(G)$ et, plus précisément, $|\mathscr{S}|$ divise $[G : S] = s$ puisque $[G : N_G(S)]$ divise $[G : S]$.

   D'autre part, S opère sur $\mathscr{S}$ par conjugaison ; si $\mathscr{S}_s$ désigne l'ensemble des points fixes du S-ensemble $\mathscr{S}$, d'après le lemme 2.6, on a

$$|\mathscr{S}| \equiv |\mathscr{S}_S| \ (mod\ p).$$

   Or,

$$S' \in \mathscr{S}_S \Leftrightarrow S' = yS'y^{-1},\ \forall y \in S$$
$$S' \in \mathscr{S}_S \Leftrightarrow S \leqslant N_G(S').$$

   Mais, d'après le lemme 2.8 $N_G(S')$ ne contient qu'un seul p-sous-groupe de Sylow de S' ; on en déduit que

$$|\mathscr{S}_S| = 1,\ d'où\ |\mathscr{S}| \equiv 1(mod\ p)$$

   En résumé et en vue des applications pratiques, on retiendra que, si $o(G) = p^n s,\ p$ premier ne divise pas s et si n_p est le nombre des p-sous-groupe de Sylow de G, alors :

$$n_p \equiv 1\ (mod\ p)\ et\ n_p\ divise\ s$$

□

Du théorème 2.5 on peut déduire les résultats suivantes :

Corollaire 2.9. *Un groupe fini G a un unique p-sous-groupe de Sylow S, si et seulement si S est normal dans G.*

En particulier, dans un groupe fini abélien G, pour tout nombre premier p divisant l'ordre de G, il n'existe qu'un seul p-sous-groupe de Sylow.

2.2 Les applications des théorèmes de Sylow

Lemme 2.10 (G.Frattini). *soit H un sous-groupe fini et normal d'un groupe G. soit S un p-sous-groupe de Sylow de H, alors $G = HN_G(S)$.*

preuve : Soit $g \in G$, alors $gSg^{-1} \leqslant gHg^{-1} = H$, et $|gSg^{-1}| = |S|$;
par suite, gSg^{-1} est un p-sous-groupe de Sylow de H, donc est conjugué de S dans H, c'est-à-dire qu'il existe $h \in H$ tel que $gSg^{-1} = hSh^{-1}$, d'où $S = h^{-1}gSg^{-1}h$.
On en déduit que $h^{-1}g \in N_G(S)$, donc $g \in HN_G(S)$,
par suite $G = HN_G(S)$. □

Corollaire 2.11. *Soient G un groupe fini et S un p-sous-groupe de Sylow G ; alors pour H sous-groupe de G, on a :*

$$N_G(S) \leqslant H \Rightarrow N_G(H) = H$$

preuve : $N_G(S) \leqslant H \leqslant G \Rightarrow S \leqslant H \leqslant G$.
S étant un p-sous-groupe de Sylow de G, S est aussi un p-sous-groupe de Sylow de H.
D'autre part, on a $H \lhd N_G(H)$; en appliquant le lemme 2.10 à H considéré comme sous-groupe de $N_G(H)$, on obtient :

$$N_G(H) = HN_G(S)$$

et $N_G(H) \leqslant H$ implique alors $N_G(H) = H$.

□

Théorème 2.12. *Soit G un groupe fini tel que $o(G) = pq$, où p et q sont deux nombres premiers distincts, tels que $q \not\equiv 1 \ (mod\ p)$; alors G a un unique p-sous-groupe de Sylow*

preuve : Soit n_p le nombre des p-sous-groupes de Sylow de G ; d'après le second théorème de Sylow, on a $n_p \equiv 1(mod\ p)$ et n_p divise $[G : S] = q$; l'hypothèse $q \not\equiv 1 \ (mod\ p)$ implique donc $n_p = 1$. □

Remarque 2.2.1. Si G est un groupe fini, non abélien, d'ordre p^n, où p est premier, alors G n'est pas simple.

Proposition 2.13. *Si G est un groupe simple, fini, non abélien et si p premier divise $o(G)$, alors le nombre n_p des p-sous-groupes de Sylow de G est plus grand que 1.*

preuve : Soit S un p-sous-groupe de Sylow de G ; on a $S \neq (e)$ et, d'après la remarque 2.2.1, S est nécessairement un sous-groupe propre de G. Si S était l'unique p-sous-groupe de Sylow de G, S serait normale dans G (corollaire 2.9), ce qui est impossible, car G est simple ; par suite on a $n_p > 1$. □

Proposition 2.14. *Si G est un groupe fini d'ordre pq, où p et q sont deux nombres premiers distincts, alors G n'est pas simple.*

preuve : On peut supposer $p > q$; alors $q - 1$ n'est pas divisible par p ; d'après le théorème 2.12, G a un unique p-sous-groupe de Sylow S ; on a

$$(e) < S < G \quad et\ S \lhd G \quad (corollaire\ 2.9),$$

donc G n'est pas simple. □

Proposition 2.15. *Soient p et q deux nombres premiers distincts tels que $p \not\equiv 1\ (mod\ q)$ et $q \not\equiv 1\ (mod\ p)$; alors tout groupe d'ordre pq est cyclique.*

preuve : Soit G un groupe fini tel que $o(G) = pq$.
D'après le théorème 2.12 G a un unique p-sous-groupe de Sylow S et un unique q-sous-groupe de Sylow T ; on a $S \lhd G$ et $T \lhd G$.
S et T sont d'ordres premiers, donc ils sont cycliques ; posons

$$S = \langle\ x\ \rangle \quad et \quad T = \langle\ y\ \rangle.$$

p et q étant premiers entre eux, $S \cap T = (e)$.

Montrons que x et y sont commutent :
$[x, y] = x^{-1}y^{-1}xy$, alors $(S \lhd G\ et\ T \lhd G) \Rightarrow [x, y] \in S \cap T$,
d'où $[x, y] = e$, et par suite, $xy = yx$.
On en déduit que l'ordre de xy est pq, d'où $G = \langle\ xy\ \rangle$ □

Proposition 2.16. *Soit p un nombre premier impair.*
Si G un groupe fini d'ordre $2p$, alors on a :

$$G \simeq C_{2p} \quad G \simeq D_p\ (groupe\ diédral).$$

preuve : p premier impair implique $p > 2$; $2 \not\equiv 1(mod\ p)$, donc G a un unique p-sous-groupe de Sylow $S \simeq C_p$.

Le nombre n_2 des 2-sous-groupes de Sylow de G est congru à 1 modulo 2 et divise p, donc $n_2 = 1$ ou $n_2 = p$:

- si $n_2 = 1$, on vérifier que : $G \simeq C_p \times C_2 = C_{2p}$.
- si $n_2 = p$, S étant le p-sous-groupe de Sylow de G, soit $y \in G \backslash S$, alors :

$$(o(G) = 2p \text{ et } y \in S) \Rightarrow o(y) = 2.$$

G a un unique sous-groupe cyclique S d'ordre $p > 2$, tel que $[G : S] = 2$ et tout élément de $G\backslash S$ est d'ordre 2 ; on en déduit que le groupe G d'ordre $2p$ est isomorphe au groupe diédral D_p.

□

Théorème 2.17. *Soit un groupe fini $G \neq (e)$, tel que $o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geqslant 1$ dans* **N**, *les p_i $(1 \leqslant i \leqslant k)$ étant des nombres premiers distincts et les α_i des entiers strictement positifs. Si pour tout i $(1 \leqslant i \leqslant k)$, G a un unique p_i-sous-groupe de Sylow P_i, alors :*

$$G = P_1 P_2 \cdots P_k \simeq \prod_{1 \leqslant i \leqslant k} P_i \tag{2.3}$$

Preuve : Pour tout i $(1 \leqslant i \leqslant k)$, on a $P_i \lhd G$ (corolaire 2.9) ; on en déduit que $H = P_1 P_2 \cdots P_k$ est un sous-groupe normal de G et en vérifie que, H et isomorphe au produit direct des p_i-groupes P_i $(1 \leqslant i \leqslant k)$; alors :

$$H \simeq \prod_{1 \leqslant i \leqslant k} P_i \Rightarrow o(H) = \prod_{1 \leqslant i \leqslant k} o(P_i) \Rightarrow o(H) = o(G),$$

d'où la relation (2.3) . □

Corollaire 2.18. *Si $G \neq (e)$ est un groupe abélien fini, d'ordre $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geqslant 1$ dans* **N**, *les p_i $(1 \leqslant i \leqslant k)$ étant des nombres premiers distincts et les α_i des entiers positifs non nuls, ;alors G est isomorphe au produit direct de ses p_i-sous-groupe de Sylow distincts.*

Remarque 2.2.2. Si la loi de composition d'un groupe abélien fini $G \neq (e)$ est notée additivement, la relation (2.3) s'écrit :

$$G = P_1 \oplus P_2 \oplus \dots \oplus P_k.$$

CHAPITRE 3

GROUPES DONT TOUS LES SOUS-GROUPES DE RANG INFINI SONT ABÉLIEN-PAR-FINI

Ces dernières années, une série d'articles a été publiée sur le comportement des groupes de rang infini dans lesquels chaque sous-groupe propre de rang infini a une propriété appropriée. Ce chapitre est une étude de la structure des groupes dans lesquels chaque sous-groupe propre de rang infini contient un sous-groupe abélien d'indice fini.Cette classe a été considérée par F. de Giovanni et F. Saccomanno dans " Groups whose proper subgroups of infinite rank are abélien-by-finite " [9]

3.1 Quelques Notions

3.1.1 Groupes résolubles

Définition 3.1. *Soit G un groupe ; à tout couple (x, y) d'éléments de G, on associe l'élément $x^{-1}y^{-1}xy$ noté $[x, y]$. $[xy]$ s'appelle le commutateur de x et y dans G.*

Définition 3.2. *Soit G un groupe, on appelle groupe dérivé de G le sous-groupe de G engendré par l'ensemble des commutateurs de G ; on le note G'.*

Théorème 3.1. *Soit G un groupe ; on a :*

1. $G' \triangleleft G$.
2. $N \triangleleft G$, *alors* $\dfrac{G}{N}$ *est un groupe abélien si et seulement si* $G' \subseteq N$;

Preuve :

1. Soit x , y , z dans G,

   d'un part :

   $$z^{-1}[x,y]z = z^{-1}x^{-1}y^{-1}xyz,$$

   d'autre part :

   $$\begin{aligned}[z^{-1}xz, z^{-1}yz] &= z^{-1}x^{-1}zz^{-1}y^{-1}zz^{-1}xzz^{-1}yz \\ &= z^{-1}x^{-1}y^{-1}xyz\end{aligned}$$

   d'où

   $$z^{-1}[x,y]z = [z^{-1}xZ, z^{-1}yz].$$

   On déduit que G' est normal dans G.

2. $$\frac{G}{N} \text{ abélien } \Leftrightarrow \bar{x}\bar{y} = \bar{y}\bar{x},\ \forall \bar{x}, \bar{y} \text{ dans } \frac{G}{N}.$$
   $$\bar{x}\bar{y} = \bar{y}\bar{x} \Leftrightarrow (yx)^{-1}xy \in N$$
   $$\bar{x}\bar{y} = \bar{y}\bar{x} \Leftrightarrow [x,y] \in N$$

   d'où $\dfrac{G}{N}$ abélien $\Leftrightarrow\ G' \subseteq N$.

□

Définition 3.3. *Un groupe G est* ***résoluble*** *s'il existe un entier $n \geqslant 0$ tel que $G^{(n)} = (e)$.*

Remarque 3.1.1. Si $G \neq (e)$ est résoluble, et si n est le plus petit entier positif tel que $G^{(n)} = (e)$, alors $\forall i\ (0 \leqslant i \leqslant n-1)$, on a : $G^{(i+1)} < G^{(i)}$.
Et d'après que $G^{(i+1)} \triangleleft G^{(i)}$ on a :

$$G = G^{(0)} > G^{(1)} > \cdots > G^{(n)} = (e)$$

est une suite de composition de G.

Théorème 3.2. *Si G est un groupe résoluble, alors tout sous-groupe de G et tout quotient de G est résoluble.*

Preuve : Supposons qu'il existe $n \in \mathbf{N}$ tel que $G^{(n)} = (e)$.

$*$ Soit H un sous-groupe de G.

$$H \leqslant G \Rightarrow H' \leqslant G'$$

$$H' \leqslant G' \Rightarrow H^{(2)} \leqslant G^{(2)}.$$

Ainsi de suite, on obtient $H^{(n)} \leqslant G^{(n)} = (e)$

d'où $H^{(n)} = (e)$; H est donc résoluble.

$*$ Soit $N \triangleleft G$; et soit $\pi : G \to \dfrac{G}{N}$ l'épimorphisme canonique tel que $\pi(x) = \bar{x},\ \forall x \in G$.

Donc toute commutateur de $\dfrac{G}{N}$ est l'image par π d'un commutateur de G.

On en déduit que $\left(\dfrac{G}{N}\right)' = \pi\,(G')$.

De même on a $\left(\dfrac{G}{N}\right)^{(2)} = \pi(G^{(2)})$ et de proche en proche on obtient :

$$\left(\frac{G}{N}\right)^{(n)} = \pi\,((G)^n) = (\bar{e})$$

d'où $\dfrac{G}{N}$ est résoluble.

□

Définition 3.4. *Un groupe est **localement résoluble** si tout sous-groupe de type fini est résoluble.*

Définition 3.5. *Un groupe G est dit **résoluble-par-fini** s'il a un sous-groupe normal N qui est résoluble et le quotient G/N est fini.*

3.1.2 Groupe nilpotent

Définition 3.6. *Pour un groupe G, une suite de composition*

$$G = G_0 \geqslant G_1 \geqslant ... \geqslant G_{n-1} \geqslant G_n = (e)$$

*sera appelée **suite centrale**, si c'est une suite normale telle que $\dfrac{G_i}{G_{i+1}} \leqslant Z(\dfrac{G}{G_{i+1}})$, quel que soit i $(0 \leqslant i \leqslant n-1)$*

Définition 3.7. *Un groupe est dit **nilpotent** s'il possède une suite centrale.*

Suite centrale descendante : G étant un groupe, posons :

$\Gamma_1 = G,\ \Gamma_2 = [G, G] = G',\ \Gamma_3 = [\Gamma_2, G]$

et, d'une façon générale :

$\Gamma_{k+1} = [\Gamma_k, G],\ \forall\, k \in \mathbf{N}^*$

$\Gamma_2 \leqslant \Gamma_1$ implique $[\Gamma_2, G] \leqslant [\Gamma_1, G]$, c'est-à-dire $\Gamma_3 \leqslant \Gamma_2$.

Par récurrence sur k, on prouve, sans difficulté, que :

$\Gamma_{k+1} \leqslant \Gamma_k, \forall\, k \in \mathbf{N}^*$

Ainsi, pour tout groupe G, on définit la chaîne descendante de sous-groupe :

$$G = \Gamma_1 \geqslant \Gamma_2 \geqslant ... \geqslant \Gamma_k \geqslant \Gamma_{k+1} \geqslant ... \tag{3.1}$$

Définition 3.8. *: On dit qu'un groupe G a une suite centrale descendante de longueur r ($r \geqslant 1$ dans $\mathbf{N}$), si la chaîne descendante (3.1) s'écrit :*

$$G = \Gamma_1 > \Gamma_2 > ... > \Gamma_r > \Gamma_{r+1} = (e) \tag{3.2}$$

Dans ce cas, le groupe G est nilpotent.

Suite centrale ascendante : G étant un groupe, posons $Z_0 = (e),\ Z_1 = (G)$.

On sait que Z_1 est caractéristique dans G, par suit l'unique sous-groupe Z_2 de G, contenant Z_1, tel que $\dfrac{Z_2}{Z_1} = Z(\dfrac{G}{Z_1})$, est caractéristique dans G.

De proche en proche, on définit, pour tout $i \in \mathbf{N}$, le sous groupe Z_{i+1} tel que

$$\frac{Z_{i+1}}{Z_i} = Z(\frac{G}{Z_i})$$

et Z_{i+1} est caractéristique dans G.

On détermine ainsi une chaîne ascendante de sous-groupe de G :

$$(e) = Z_0 \leqslant Z_1 \leqslant ... \leqslant Z_i \leqslant Z_{i+1} \leqslant ... \tag{3.3}$$

dans laquelle, pour tout $i \in \mathbf{N}$, on a $Z_i \sqsubset G$, donc $Z_i \lhd G$ et Z_{i+1} est le plus grand sous-groupe de G contenant Z_i, tel que

$[Z_{i+1}, G] \leqslant Z_i$

S'il existe un entier $s \geqslant 0$ tel que $Z_s = G$, la chaîne (3.3) s'écrit :

$$(e) = Z_0 \leqslant Z_1 \leqslant ... \leqslant Z_{s-1} \leqslant Z_s = G \tag{3.4}$$

Et, d'après ce qui précède, la chaîne (3.4) est une suite centrale de G.
De plus, si $G \neq (e)$ et si s est le plus petit entier positif tel que $Z_s = G$, alors, pour tout i $(0 \leqslant i \leqslant s-1)$, on a $Z_i < Z_{i+1}$, car $Z_i = Z_{i+1}$ implique $Z_j = Z_i$ quel que soit $j \geqslant i$.

Définition 3.9. *: On dit qu'un groupe G a une suite centrale ascendante de longueur s $(s \geqslant 1$ dans $\mathbf{N})$, si la chaîne ascendante (3.3) s'écrit :*

$$(e) = Z_0 < Z_1 < ... < Z_{s-1} < Z_s = G; \tag{3.5}$$

le groupe G est nilpotent.

Définition 3.10. *Un groupe est* ***localement nilpotent*** *si tout sous-groupe de type fini est nilpotent.*

Définition 3.11. *Un groupe G est* ***nilpotent-par-fini*** *s'il a un sous-groupe normal N qui est nilpotente et le quotient G/N est fini.*

3.1.3 Quelques définitions

Définition 3.12. *Un groupe G est dit* ***simple*** *s'il a exactement deux sous-groupes normaux : étant l'élément neutre et G lui-même.*

Définition 3.13. *Un groupe G est dit* ***localement fini*** *si tout sous-groupe de type fini de G étant fini.*

Définition 3.14. *Un groupe G est dit* ***localement gradué*** *si tout sous-groupe non trivial de type fini de G a un sous-groupe d'indice fini.*

Définition 3.15. *Un groupe est dit* ***hypercentral*** *(également* ***hypernilpotent****) si sa série centrale ascendante se termine à l'ensemble du groupe, ou de manière équivalente, s'il est égal à son hypercentre.*

Définition 3.16. *Un groupe de type fini qui est une extension d'un groupe abélien par un groupe nilpotent est* ***résiduellement fini****.*

Définition 3.17. *Un groupe* ***de torsion*** *ou un groupe périodique est un groupe dans lequel chaque élément a un ordre fini. L'exposant d'un tel groupe, s'il existe, est le plus petit commun multiple des ordres des éléments. L'exposant existe pour tout groupe fini, et il divise l'ordre du groupe.*

Remarque 3.1.2. Un groupe ***sans torsion*** est un groupe dont le seul élément d'ordre fini est l'identité.

Définition 3.18. *Un groupe G est dit* ***de rang fini*** *s'il existe un entier positif r tel que tous les sous-groupes de G de type fini peuvent être générés par au plus r éléments où r est le plus petit entier positif avec une telle propriété ; sinon, si un tel r n'existe pas, le groupe est dit* ***de rang infini****.*

Définition 3.19. *Un groupe G est dit* ***abélien-par-fini*** *s'il a un sous-groupe normal N qui est abélien et le quotient G/N est fini.*

Remarque 3.1.3. Un groupe G est appelé X-par-Y s'il a un sous-groupe normal N qui appartient à la classe X et le quotient G/N appartient à la classe Y.

3.2 Groupes dont tous les sous-groupes de rang infini sont abéliens-par-fini

Dans [9] F. de Giovanni et F. Saccomanno ont étudie les groupes dont tous les sous-groupes de rang infini sont abéliens-par-fini et ils ont commencé par le Lemme suivant :

Lemme 3.3. *Supposons que G soit un groupe infini simple localement fini. Alors G a tous les sous-groupes propres nilpotent-par-(rang fini) si et seulement si $G \simeq PSL(2, F)$ ou $G \simeq S_Z(F)$, pour un corps infini localement fini F ne contenant aucun sous-corps propre infini.*

Théorème 3.4. *Soit G un groupe localement (résoluble-par-fini) dans lequel tout sous-groupe propre est nilpotent-par-(rang fini). Supposons que G n'est pas un p-groupe parfait. Si G n'a pas d'images simples infinies alors G est nilpotent-par-(rang fini).*

Théorème 3.5. *Soit G un groupe avec tous les sous-groupes propres sont nilpotents-par-(rang fini) et supposons que G est localement (résoluble-par-fini) et localement de rang fini. Supposons que G n'est pas localement fini, alors G est nilpotent-par-(rang fini).*

Un résultat similaire est également valable pour les groupes dans lesquels chaque sous-groupe propre est abélien-par-(rang fini).

Théorème 3.6. *Soit G un groupe dont les sous-groupes propres sont abéliens-par-(rang fini). Si G est localement nilpotent, ou localement fini sans images simples infinies, alors G est abélien-par-(rang fini).*

Enfin, les auteurs ont un résultat correspondant pour les groupes dans lesquels chaque sous-groupe propre est (nilpotent de classe c)-par-(rang fini).

Théorème 3.7. *Supposons que G est un groupe dont les sous-groupes propres sont (nilpotent de classe c)-par-(rang fini).*

1. *Si G est localement résoluble alors G est nilpotent-par-(rang fini) et soit G est (nilpotent de classe c)-par-(rang fini) soit G est résoluble.*
2. *Si G est localement (résoluble-par-fini) et localement de rang fini, mais pas localement fini, alors G est nilpotent-par-(rang fini) et soit G est (nilpotent de classe c)-par-(fini rang) soit G est résoluble.*

Maintenant, les auteurs étudient des groupes de rang infini dans lesquels tous les sous-groupes propres de rang infini ont un sous-groupe abélien d'indice fini.

Lemme 3.8. *Soit G un groupe dont les sous-groupes propres de rang infini sont abéliens-par-finis. Si le groupe G/G' est de rang infini, alors tout sous-groupe propre de G est abélien-par-fini.*

Preuve : Soit X un sous-groupe quelconque de rang fini de G. Alors XG' est proprement contenu dans G, et donc il existe un sous-groupe propre Y de G de rang infini tel que $XG' \leqslant Y$. Donc X est abélien-par-fini. □

Théorème 3.9. *Un non-parfait localement gradué minimal non-(abélien-par-fini) groupe est périodique.*

Proposition 3.10. *Si G est un groupe minimal périodique localement gradué non (abélien par fini), alors $G/G' \simeq Z(p^\infty)$, pour un p premier, et si G n'est pas un p-groupe, alors G' est un p'-groupe, et il existe un sous-groupe $A \simeq Z(p^\infty)$ tel que $G = AG'$.*

Lemme 3.11. *Soit G un groupe de rang infini dont les sous-groupes propres de rang infini sont abéliens-par-finis. Si G contient un sous-groupe propre qui n'est pas abélien-par-fini, alors $G' = [G', G]$ et G est soit parfait ou métabélien.*

Preuve : Puisque G/G' est de rang fini d'après le lemme 3.8 et que $G'/[G', G]$ est une image homomorphe du produit tensoriel

$$(G/G') \otimes (G/G'),$$

il s'ensuit que le groupe nilpotent $G/[G', G]$ est également de rang fini. Puis $[G', G]$ doit avoir un rang infini, et donc tous les sous-groupes propres de $G/[G', G]$ sont abéliens-par-finis. Supposons par contradiction que $[G', G]$ soit proprement contenu dans G'. Alors $G/[G', G]$ ne peut pas être abélien-par-fini, puisque G n'a pas de sous-groupes propres d'indice fini, et donc le théorème 3.9 et la proposition 3.10 montrent que

$$(G/[G', G])/(G/[G', G])' \simeq G/G'$$

est un groupe de type $p^{\propto}$ pour un nombre premier p. Il s'ensuit que le groupe nilpotent $G/[G', G]$ est abélien, et cette contradiction montre que $G' = [G', G]$.
Supposons maintenant que G' est un sous-groupe propre de G. alors G' a un rang infini, donc c'est abélien-par-fini, et donc il contient un sous-groupe caractéristique abélien A d'indice fini. Comme le groupe G/A a un sous-groupe de commutateur fini, il est nilpotent-par-fini D'un autre côté, G n'a pas de sous-groupes propre d'indice fini, de sorte que G/A est nilpotent et donc même abélien par la première partie de la preuve.
Par conséquent, $G' = A$ est abélien. □

Le résultat général suivant est sur les groupes localement (résolubles-par-fini).

Lemme 3.12. *Soit G un groupe localement (résoluble-par-fini) contenant un sous-groupe normal propre N tel que G/N soit de rang fini. Alors G admet une image homomorphe non triviale qui est soit finie soit abélienne.*

preuve : Supposons que G n'a pas de sous-groupes propres d'indice fini. Comme G/N est (localement résoluble)-par-fini par un résultat de $N.S.$ Černikov, il est même localement résoluble.
Alors il existe un entier positif k tel que $G^{(k)}N/N$ soit hypercentral, et il s'ensuit que le sous-groupe commutateur de G est un sous-groupe propre. □

Le lemme suivant améliore le résultat obtenu par Bruno et Phillips sur la périodicité des groupes non-(abéliens-par-finis) minimaux non parfaits.

Lemme 3.13. *Soit G un groupe localement (résoluble-par-fini) de rang infini. Si tous les sous-groupes propres de rang infini de G sont abéliens-par-fini, alors G est soit abélien-par-fini soit périodique.*

Preuve : Supposons pour une contradiction que le groupe G n'est abélien-par-fini ni périodique.

En particulier, G n'a pas de sous-groupes propres d'indice fini et il ne peut pas donc être de type fini. Comme les groupes abéliens par finis de type fini sont évidemment de rang fini, il résulte des hypothèses que tout sous-groupe de type fini de G est de rang fini.

De plus, il est également clair que chaque sous-groupe propre de G est abélien-par-(rang fini).

Alors soit G est résoluble, soit il contient un sous-groupe normal abélien A tel que G/A soit de rang fini d'après le théorème 3.7, tel que l'application du lemme 3.12 montre que G' est un sous-groupe propre de G.

Il résulte du théorème 3.7 que G contient des sous-groupes propres qui ne sont pas abéliens-par-finis. Alors G/G' doit être de rang fini d'après le lemme 3.8, et G' est un sous-groupe abélien de rang infini d'après le lemme 3.11.

Supposons d'abord que le groupe G/G' n'est pas périodique. Puisque G/G' est divisible, G peut être décomposé en produit de deux sous-groupes normaux propres de rang infini. Alors G est nilpotent-par-fini, et donc nilpotent.

De nouveau le Lemme 3.11 donne maintenant la contradiction que G est abélien. Donc G/G' doit être périodique, et donc G' n'est pas périodique.

Soit T le sous-groupe constitué de tous les éléments d'ordre fini de G'. Si T est de rang infini, alors tous les sous-groupes propres de G/T sont abéliens-par-fini, et donc le groupe non périodique G/T est abélien-par-fini d'après le théorème 3.9.

Alors G/T est abélien, une contradiction, car T est proprement contenu dans G'. Donc T est de rang fini, et le groupe G/T est également un contre-exemple, de sorte que sans perte de généralité on peut supposer que G' est un groupe abélien sans torsion. Si q_1 et q_2 sont des nombres premiers distincts, d'après le lemme 3.8 il existe un sous-groupe G-invariant N de G' tel que G'/N est périodique et q_1, q_2 appartiennent à $\pi(G'/N)$.

Comme G' est sans torsion, le sous-groupe N est de rang infini, et donc tous les sous-groupes propres de G/N sont abéliens-par-finis.

D'autre part, G/N n'est pas abélien-par-fini, et son sous-groupe de commutateurs n'est pas un groupe primaire, ce qui contredit le théorème 3.9. L'énoncé est prouvé. □

Maintenant le résultat principal est prêt d'être démontré .

Théorème 3.14. *Soit G un groupe localement (résoluble-par-fini) de rang infini dont les*

sous-groupes propres de rang infini sont abéliens par fini. Alors tous les sous-groupes propres de G sont abéliens-par-finis.

Preuve : Supposons pour une contradiction que l'hypothèse est faux. En particulier, G n'est pas abélien-par-fini, et donc il n'a pas de sous-groupes propres d'indice fini. De plus, G est périodique d'après le lemme 3.13, donc localement fini. Supposons que G contienne un sous-groupe normal propre K tel que G/K soit simple. Alors G/K doit avoir un rang infini d'après le Lemme 3.12 et donc il est isomorphe soit à $PSL(2, F)$ soit à $S_Z(F)$ pour un corps infini localement fini F ne contenant pas de sous-corps propres infinis comme conséquence du Lemme 3.3 Par contre, chacun des deux derniers groupes contient un sous-groupe propre de rang infini qui n'est pas abélien-par-fini .
Cette contradiction montre que G n'a pas d'images homomorphes simples infinies, de sorte que le théorème 3.6 assure qu'il contient un sous-groupe abélien normal N tel que G/N est de rang fini, et donc G' est un sous-groupe propre de G par le lemme 3.12 .

Il résulte des Lemmes 3.8 et 3.11 que G' est un groupe abélien de rang infini. Soit X un sous-groupe de rang fini de G qui n'est pas abélien-par-fini. Clairement, X ne peut être contenu dans aucun sous-groupe propre de rang infini de G, et donc $XG' = G$. Alors $X/X \cap G' \simeq G/G'$ n'a pas de sous-groupes propres d'indice fini, et donc il est divisible. De plus, le sous-groupe normal abélien $X \cap G'$ de G est de rang fini, il est donc le produit direct de ses composantes primaires, et il a un recouvrement par des sous-groupes caractéristiques finis.
Alors $X/C_X(X \cap G')$ est résiduellement fini, puisque $X/X \cap G'$ ne contient pas de sous-groupes propres d'indice fini, il s'ensuit que $X \cap G'$ est contenu au centre de X, et donc X est nilpotent.
Considérons maintenant un sous-groupe normal abélien maximal A de X contenant $X \cap G'$. Alors $C_X(A) = A$, et donc le groupe divisible X/A est isomorphe à un groupe d'automorphismes de A. D'autre part, A a un recouvrement par des sous-groupes caractéristiques finis, de sorte que son groupe d'automorphismes complet est résiduellement fini. Donc $X = A$ est abélien, et cette contradiction prouve l'énoncé. □

C'est une question ouverte de savoir si un groupe localement gradué quelconque de rang infini doit contenir un sous-groupe propre de rang infini. Ceci semble être le principal obstacle à l'extension de théorème au cas des groupes localement gradués. Cependant, les auteurs

soulignerons que cela est au moins possible pour une classe spéciale de groupes localement gradués, ils pouvont prouver que le théorème principal reste vrai dans la classe des groupes fortement localement gradués.

Lemme 3.15. *Soit G un groupe fortement localement gradué de rang infini. Si tous les sous-groupes propres de rang infini de G sont localement (résoluble-par-fini), alors G est localement (résoluble-par-fini).*

Preuve : Supposons d'abord que G soit un groupe non trivial de type fini, de sorte qu'il contienne un sous-groupe propre H d'indice fini. Alors H est un sous-groupe de type fini de rang infini, donc il est résoluble-par-fini et donc G lui-même est résoluble-par-fini.

Supposons maintenant que G n'est pas de type fini, de sorte que tout ses sous-groupes de type fini de rang infini sont résolubles-par-fini.

D'autre part, il découle du résultat de $\check{C}$ernikov que tout sous-groupe X de G de rang fini de type fini doit être résoluble-par-fini. Donc G est localement (résoluble-par-fini). □

Corollaire 3.16. *Soit G un groupe fortement localement gradué de rang infini dont les sous-groupes propres de rang infini sont abéliens-par-fini. Alors tous les sous-groupes propres de G sont abéliens-par-finis.*

Preuve : Le groupe G est localement (résoluble-par-fini) d'après le lemme 3.15, et donc l'énoncé est une conséquence directe du théorème 3.14. □

CONCLUSION

Dans ce mémoire nous constatons que si G est un groupe fortement localement gradué de rang infini dont les sous groupes propres de rang infini sont abéliens-par-fini, alors tous les sous-groupes propres de G sont abéliens-par-finis.

BIBLIOGRAPHIE

[1] A. L. Mal'cev, "On certain classes of infinite soluble groups", Mat. Sb. 28, 567–588 (1951) ; Amer. Math. Soc. Transl. 2, 1–21 (1956).

[2] B. Bruno : "On groups with abelian-by-finite proper subgroups", Bollettino U.M.I. (6) 3-B (1994), 797-807.

[3] B. H. Neumann, "Groups with finite classes of conjugate subgroups", Math.Z. 63, 76–96 (1955).

[4] D.J.S Robinson : "A couse in the theory of groupe", Second Edition Spinger, 1996.

[5] D.J.S Robinson : "Finitness Conditions and Generalized Soluble Groups", part I and II, Springer-Verlag, New York, 1972.

[6] D.J.S. Robinson : "Groups in which normality is a transitive relation", Proc. Cambridge Philos. Soc 68 (1964), 21-38.

[7] D.J.S. Robinson : "Groups which are minimal with respect to normality being transitive", Pacifc J. Math. 31 (1969), 777-785.

[8] D. McDougall, "Soluble groups with the minimum condition for normal subgroups", Math. Z. 118, 157–167 (1970).

[9] F. de Giovanni, F. Saccomanno : "A note on groups of infinite rank whose proper subgroups are abelian-by-finite", Colloq. Math. 137 (2014), 165-170.

[10] G. M. Romalis ans N. F. Sesekin, "Metahamiltonian groups", Ural. Gos. Univ. Mat. Zap. 5, 101–106 (1966).

[11] G. M. Romalis and N. F. Sesekin, “Metahamiltonian groups. II”, Ural. Gos. Univ. Mat. Zap. 6, 52–58 (1968).

[12] G. M. Romalis and N. F. Sesekin, “Metahamiltonian groups. III”, Ural. Gos. Univ. Mat. Zap. 7, 195–199 (1969/70).

[13] J. E. Roseblade, “On groups in which every subgroup is subnormal”, J. Algebra, 2, 402–412 (1965).

[14] L. A. Kurdachenko and H. Smith, “Groups in which all subgroups of infinite rank are subnormal”, Glasgow Math. J. 46, 83–89 (2004).

[15] M. De Falco, F. de Giovanni, and C. Musella, “Groups whose finite homomorphic images are metahamiltonian”, Comm. Algebra, 37, 2468–2476 (2009).

[16] M. De Falco, F. de Giovanni, and C. Musella, “Groups whose proper subgroups of infinite rank have a transitive normality relation”, Mediterranean J. Math. 10, 1999-2006 (2013).

[17] M. R. Dixon, M. J. Evans, and H. Smith, “Locally (soluble-by-finite) groups with all proper insoluble subgroups of finite rank”, Arch. Math. (Basel), 68, 100–109 (1997).

[18] M. R. Dixon, M. J. Evans and H. Smith : "Locally (soluble-by-finite) groups with all proper non-nilpotent subgroups of finite rank", J. Pure Appl. Algebra 135 (1999), 33-43.

[19] M. R. Dixon and Y. Karatas, “Groups with all subgroups permutable or of finite rank”, Centr. Eur. J. Math. 10, 950–957 (2012).

[20] N. N. Semko and S. N. Kuchmenko, “Groups with almost normal subgroups of infinite rank”, Ukrain. Math. J. 57, 621–639 (2005).

[21] N. S. Černikov, “A theorem on groups of finite special rank”, Ukrain. Math. J. 42, 855–861 (1990).

[22] V. P. Šunkov, “On locally finite groups of finite rank”, Algebra Logic, 10, 127–142 (1971).

[23] W. MÖhres, “AuflÖsbarkeit, von Gruppen, deren Untergruppen alle subnormal sind”, Arch. Math. (Basel), 54, 232–235 (1990).

ملخص

درسنا في الفصل الأول بعض المفاهيم الأساسية: الزمر المتماثلة S_n، الزمر المتناوبة A_n، عمليات زمرة على مجموعة، الزمر الدورية.

في الفصل الثاني ركزنا على الزمر المحدودة (نظريات Sylow وتطبيقاتها).

درسنا في الفصل الثالث بنية الزمر التي تملك زمر جزئية ذات الرتب اللانهائية متميزة تبديليا ذات مؤشر منتهي.

الكلمات المفتاحية

زمرة، زمرة منتهية، زمرة جزئية، رتبة منتهية، تبديلي ذو مؤشر منتهي .

Résumé

Dans le premier chapitre on a étudie quelques notions fondamental : les groupes symétrique S_n , les groupes alternés A_n , les opérations d'un groupe sur un ensemble, les groupes cycliques.

Dans le deuxième chapitre on a concentré sur les groupes finis en particulier les théorèmes de Sylow et ses applications.

Dans le troisième chapitre on a étudier la structure des groupes dont tous les sous groupes de rang infini sont abéliens-par-fini.

Mots-clés

Groupe , groupe fini, sous-groupe, rang fini, abelien-par-fini.

Abstact

In the first chapter we studied some fundamental notions: symmetric groups S_n , alternating groups A_n , operations of a group on a set, cyclic groups.

In the second chapter we concentrated on finite groups in particular Sylow theorems and their applications.

In the third chapter we have studied the structure of the groups of which all the subgroups of infinite rank are abelian-by-finite.

Keywords

group, finit group, sub-group, finit rank, abelian-by-finite.