N° d'ordre :
N° de série :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Superieur et de la Recherche Scientifique

UNIVERSITÉ ECHAHID HAMMA LAKHDAR ELOUED

FACULTÉ DESSCIENCES ET DE TECHNOLOGIE

Mémoire de fin d'étude

LICENCE ACADEMIQUE

Domaine: Mathématiques et Informatique
Filière: Mathématiques
Spécialité: Modélisation mathématiques & simulation numérique

Thème

Groupes nilpotents et les groupes résolubles

Présenté par:
Ben Ali Meriem
Guessoum Imane
Lajdel Ali Tefaha

Sous la supervisionde :

M^{r} :Said-Ameur Meziane

Année universitaire 2014 – 2015

Remerciements

Avant tout, nous remercions ALLAH tout puissant de nous avoir accordé la force, le courage et les moyens pour accomplir ce modeste travail.

Nous tenons à remercier:

Mes parents qui m'ont encouragée et qui m'ont donné les conditions nécessaires à un travail efficace.

Ms SAID AMEUR MIZIANE d'avoir proposé et dirigé ce travail.

Nos sincéres remerciements vont également aux membres du jury.

Tous enseignants de la faculté des science et technologie, département de la mathématiques et informatique.

En fin nous remercions touts ce qui nous ont aidé de prés ou de loin a réaliser se modeste travail.

Notations générales

$(G, *)$	Un groupe.
$H \subset G$	H sous-ensemble de l'ensemble G.
$H \leq G$	H sous-groupe de groupe G.
$H \lhd G$	H sous-groupe distingeé dans G.
$\|G\|$	L'ordre de G.
$\|x\|$	L'ordre d'un élément de G.
$[G : H]$	L'indice de H par raport a G.
$[x, y]$	Le commutateur de $x, y \in G$.
$[G : G]$	La derive groupe de G.
$Z_G(x)$	Le centre d'élément x de G.
$Z_G(H)$	Le centre de groupe H.
G/H	Le quotient groupe de H par G.
$\ker f$	Le noyaux de l'homomorphisme f.
$\mathrm{Im}\, f$	L'image de homomorphisme f.
$Aut\ G$	homomorphisme intérne de G dans G.
$N_G(H)$	Le normalisateur de H.
S_n	Groupe symétrique.
A_n	Groupe altérné.
σ	Permutation $\sigma \in S_n$.
$Sgn(\sigma)$	Signature de σ.
$\{H_i\}_{i \in I}$	Une famille de sous-groupe de G.

Table des matières

Notations générales **ii**

Introduction générale **1**

1 Généralité de groupe **2**

1.1 **Loi de composition interne** 2

1.2 **Structure de groupe** 3

1.2.1 **Groupe** 3

1.2.2 **Sous-groupe** 5

1.2.3 **Morphismes des groupes** 10

2 Divers groupes **12**

2.1 **Le groupe symétrique** 12

2.1.1 **Le Groupe S_n** 12

2.1.2 **Orbites De S_n** 13

2.1.3 **Cycle De S_n** 13

2.1.4 **Signature d'une permutation** 14

2.1.5 **Le groupe alterné A_n** 14

2.2 **Le Groupe Cyclique** 15

2.3 **Le p-groupe** 18

2.3.1 **Théorème de cauchy** 18

2.3.2 **Les théorèmes de sylow** 19

3 Les groupes nilpotentes et les groupes résolubles **20**

3.1 **Les groupes nilpotents** 20

3.1.1 **Suite de composition** 20

3.1.2 **Suite centrale** 20

3.1.3 **Le groupe nilpotent** 21

3.2 **Le groupe résoluble** 25

Conclusion Générale **33**

Bibliographie **34**

Introduction générale

Le théorie des groupes est une displine mathématique c'est la partie de l'algébre générale qui etudi les groupes: structures, propriétés algébrique.L'une des origines de lidée de groupe est l'etude des equations algebriques par Joseph-Louis (1771).La terminologie de groupe est mise en evidence pour la 1^{er} (premiére) fois par Evarieste Galois(1830) .

Dans notre travail nous allons partage notre mémoire en trois chapitres.

Le premier chapitre nous rappelons quelques notions essentielles des groupes (structure, propriétés, sous-groupe, sous-groupe distingée.....) et l'homorphisme de groupe.

Dans le deuxième chapitre expose de quelque divers groupes avec leurs propriétés et leurs charactistiques.

Dans le derniers chapitre sera consacré aux groupes nilpotents et les groupes résolubles finie leurs propreties, leurs devoloppement (théorèmes, propositions, exemples.....), et de comparisation entre les groupes nilpotents et résolubles.

Chapitre 1

Généralité de groupe

1.1 Loi de composition interne

Définition 1.1.1 .

Soit E un ensemble une loi de composition interene (l,c,i) sur E est une application T de $E \times E$ dans E notée généralement xTy plutôt que $T(x, y)$ lors que $(x, y) \in E \times E$.

Exemple 1.1.1 .

La somme et produit sur $\mathbb{N}, \mathbb{Z}$ sont (l,c,i).

Définition 1.1.2 .

1)Une loi de composition interene (l,c,i) T sur E sera dite associtive lors que:

$$\forall x, y, z \in E : (xTy)Tz = xT(yTz)$$

2)Une loi de composition interene (l,c,i) T sur E sera dite commutative lors que:

$$\forall x, yE : xTy = yTx$$

3)Si T est une loi de composition interene (l,c,i) sur E. $e \in E$ est une élément neutre pour T lors que:

$$\forall x \in E : xTe = eTx = x$$

4) Si T admet un élément symétrie x' de x :

$$\forall x, x' \in E, xTx' = x'Tx = e$$

1.2 Structure de groupe

1.2.1 Groupe

Définition 1.2.1 .

Un groupe est un ensemble non vide muni d'une loi de composition interne

$* : G \times G \to G$ *tel que:*

$*$ *est associative:*

$$\forall x, y, z \in G : (x * y) * z = x * (y * z)$$

$*$ *est admet un neutre:*

$$\forall x \in G, \exists e \in G : x * e = e * x = x$$

Tout élément de G *est admet un symétrique* $x^{'}$ *pour* $*$*:*

$$\forall x \in G, \exists x^{'} \in G : x * x^{'} = x^{'} * x = e$$

Définition 1.2.2 .

Si $*$ *est commutative, on dit que* $(G, *)$ *est commutative ou encore abélien.*

$$\forall x, y \in G : x * y = y * x$$

Exemple 1.2.1 .

$(\mathbb{Z}, +)$ *et groupe abélien.*

$(\mathbb{N}, +), (\mathbb{R}, \times)$ *ne sont pas des groupes.*

Remarque 1.2.1 .

1) Il existe deux élément x *et* y *d'un groupe non commutative* $(G, *)$ *on a :*

$$x * y \neq y * x$$

2) Dans un groupe G *tout élément* x *à une unique symétrique* $x^{'}$*.*

3) Dans un groupe G *l'élément neutre est unique.*

Régle de calcul dans groupe

Dans tout le paragraphe, G designe un groupe multiplicatif dont l'élément neutre est noté $e = 1$.

Puissance n$^{\text{ieme}}$ d'un élément Soit $x \in G$ on pose: $xx = x^2, (xx)\,x = x\,(xx) = x^3$, pour tout $(n, m) \in \mathbb{Z}^2$ et $x \in G$:

i) $x^n x^m = x^{n+m}$, d'ou $x^n x^m = x^m x^n$.

ii) $(x^n)^m = x^{mn} = (x^m)^n$.

Règle de simplication Dans un groupe G tout élément $a \neq 0$ est simplifiable à droite et à gauche c'est à dire pour tout x, y dans $G : xa = ya \Longrightarrow x = y$ et $ax = ay \Longrightarrow x = y$.

En effet, si a^{-1} est l'inverse de a:

$xa = ya \Longrightarrow (xa)\,a^{-1} = (ya)\,a^{-1}$ d'ou $x = y$.

Définition 1.2.3 .

$(\mathbb{Z}_n, +)$ est un groupe abelien fini d'ordre n, on appele le groupe de classe de congruence de $\mathbb{Z}$ modulo n

$\mathbb{Z}\diagup_n\mathbb{Z} = \mathbb{Z}_n = \left\{\bar{0}, \bar{1}, ..., \overline{n-1}\right\}$ *tel que* $n \in \mathbb{N}^*$.

Le centralisateur d'un groupe

Le centralisateur d'un sous-groupe A de G noté:

$$Z(A) = \{x \in G : \forall a \in A, xa = ax\}$$

Le normalisateur d'un groupe

Le normalisateur d'un sous-groupe H de groupe G est l'ensemble:

$$N_G(H) = \left\{g \in G : gHg^{-1} = H\right\}$$

L'ordre d'un groupe

Définition 1.2.4 .

1) L'ordre d'un groupe G, noté $|G|$ est le nombre fini ou infini de ses l'élément.

2) L'ordre d'un élément $x \in G$, noté $|x|$ est l'ordre du sous-groupe engendré par ce élément.

Groupe fini

Définition 1.2.5 .

$(G,*)$ groupe fini si le nombre de ses éléments est fini, dans ce cas, son cardinal est appelé l'ordre du groupe G, on le note $|G|$ de plus si le groupe n'est pas fini, il est dit infini.

Exemple 1.2.2 .

$(\mathbb{Z},+)$ est d'ordre infini puis que $\mathbb{Z}$ est infini.

$(\mathbb{Z}/5\mathbb{Z})$ et fini $|\mathbb{Z}/5\mathbb{Z}| = 5$ tel que: $\mathbb{Z}/5\mathbb{Z} = \left\{\mathring{0}, \mathring{1}, \mathring{2}, \mathring{3}, \mathring{4}\right\}$

1.2.2 Sous-groupe

Définition 1.2.6 .

Un sous-groupe d'un groupe $(G,*)$ est une partie non vide, H de G tel que:

1) $*$ induit sur H une loi de composition interne.

2) Muni de cette loi H est un groupe, on note alors $H < G$.

Définition 1.2.7 .

Soit $(G,*)$ un groupe et H une partie non vide de G on dit que H est un sous-groupe G si:

$$\begin{cases} (x,y) \in H \times H \Longrightarrow xy \in H & (1) \\ x \in H \Longrightarrow x^{-1} \in H & (2) \end{cases}$$

Le conditions (1) et (2) impliquent que $e \in H$.

Théorème 1.2.1 [11].

Soit $(G,*)$ un groupe et H une partie non vide de G. on dit que H un sous-groupe de G, si et seulement si:

$$\forall (x,y) \in H \times H \text{ alors } xy^{-1} \in H \qquad (3)$$

Remarque 1.2.2 .

Il est clair que $Z(A)$ et $N_G(H)$ sont des sous-groupes de G.

Définition 1.2.8 .

L'ensemble $\{e\}$ *formé de l'élément neutre de* G *et* H_i $\forall i \in \mathbb{N}$ *sont des sous-groupes de* G *appellés les sous-groupes triviaux de* G.

Remarque 1.2.3 .

1) Un groupe qui n'admet que les sous-groupes triviaux est un groupe simple.

2) Un groupe composé est un groupe qui admet un sous-groupe non trivial.

Définition 1.2.9 .

Soit $(G, *)$ *un groupe,* $(H, *)$ *est un sous-groupe, on dit que* H *est un propre sous-groupe de* G *si:* $H \neq \{e\}$ *et* $H \neq G$.

Notation 1.2.1 .

$H \leq G$: *si* H *est un sous-groupe de* G.

$H < G$: *si* H *est un propre sous-groupe de* G.

Proposition 1.2.1 [11].

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

$\bigcap\limits_{i\in\mathbb{N}} H_i$ *est un sous-groupe de* G.

Remarque 1.2.4 .

En général $\bigcup\limits_{i\in\mathbb{N}} H_i$ *n'est pas un sous-groupe de* G.

Exemple 1.2.3 .

Soit le sous-groupe de $G = (\mathbb{Z}, +)$, $H_1 = 3\mathbb{Z}$ *et* $H_2 = 8\mathbb{Z}$ *on a:* $3+8 = 11$ *et* $11 \notin H_1 \cup H_2$, *donc* $H_1 \cup H_2$ *n'est pas un sous-groupe de* $\mathbb{Z}$.

Proposition 1.2.2 [11].

Soient G *un groupe et* $F = \{H_i\}_{i\in\mathbb{N}}$, *une famille de sous-groupe de* G *ordonnée par inclusion alors* $\bigcup\limits_{i\in\mathbb{N}} H_i$ *est un sous-groupe de* G,

i.e $(H_0 \subset H_1 \subset H_2 \subset ..... \subset H_n)$.

Définition 1.2.10 .

Le nombre $[G : H]$ *est appelé indice de* H.

Thèoreme de lagrange [8]

Soit H sous-groupe de G et G est un groupe fini alors :

$|G| = [G : H]\,|H|$, donc $|H|$ devise $|G|$.

Sous-groupe distingue

Définition 1.2.11 .

Soit G un groupe, un sous-groupe H est dit normal ou distingué, si et seulement si :

$\forall x \in G,\ xHx^{-1} = H$, *on not alors* $H \lhd G$.

La caractrisation à desseus équivaut à dire que $\forall x \in G : xHx^{-1} \subset H$.

Exemple 1.2.4 .

$(\mathbb{Z}, +)$ *est un groupe,* $(\mathbb{Z}/3\mathbb{Z}, +)$ *est un sous-groupe d'un groupe* $\mathbb{Z}$,

$\mathbb{Z}_3$ *est un groupe distingue?*

$\forall g \in \mathbb{Z} = G, \forall h \in \mathbb{Z}_3 = H$.

$ghg^{-1} = g + h + g^{'} = g + g^{'} + h = h \in \mathbb{Z}_3$.

$ghg^{-1} \in \mathbb{Z}_3 \Longrightarrow (\mathbb{Z}_3, +)$ *est un groupe distingue.*

Groupe quotient

Définition 1.2.12 .

Soit H est un sous-groupe de groupe G et $H \lhd G$.

L'ensemble K des classes est un groupe muni de la loi :

$$(xH).(yH) = (xy).H, \forall x, y \in G$$

est appelé goupe quotient de G par H on le note $K = G/H$ tel que:

$$G/H = \{xH : x \in G\}$$

Remarque 1.2.5 .

$(G/H = \{xH : x \in G\}, \quad *)$ *est un sous-groupe.*

Exemple 1.2.5 .

Soit $\mathbb{Z}$ l'ensemble des nombers entier, $2\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, constitué des entiers pairs alors le groupe quotient $\mathbb{Z}/2\mathbb{Z}$ est constitué de deux élément représentant la classe des nombre pairs et inpairs.

Commutateurs

Définition 1.2.13 .

Soit G un groupe fini. $[a,z] = aza^{-1}z^{-1} \in G$ est appelé le commutateurs de a et de z. on a $[a,z] = 1$ ssi $az = za$ ssi a et z commutent.

Remarque 1.2.6 .

Si G est abélien, tout commutateur est égal à l'élément neutre de G.

Proposition 1.2.3 [5].

Soient x, y et z appartenant à G avec $\alpha, \beta \in G$

1) $([x,y])^{-1} = [y,x]$.

2) $x[y,z]x^{-1} = [xyx^{-1}, xzx^{-1}]$.

3) $\left[x^{\alpha}, y^{\beta}\right] = x^{(1-\alpha)/2} y^{(1-\beta)/2} [x,y]^{\alpha\beta} y^{(\beta-1)/2} x^{(\alpha-1)/2}, (\alpha, \beta \in \{-1,1\})$.

4) $[x,yz] = [x,z][x,y]^{z}$.

5) $[xy,z] = [x,z]^{y}[y,z]$.

6) $[x,y^{-1},z]^{y}[y,z^{-1},x]^{z}[z,x^{-1},y]^{x} = 1$.

Preuve. [5] ■

Groupe dérivé

Définition 1.2.14 .

Un groupe dérivé de G et noté $D(G)$. est le sous-groupe de G engendré par l'ensemble des commutateurs $[a,b], \forall a, b \in G$

$$D(G) = [G,G] = \langle [g,h] : g, h \in G \rangle$$

Théorème 1.2.2 [11].

1) $[G,G] \trianglelefteq G$.

2) $G/[G,G]$ *est abélien.*

3) Si $N \trianglelefteq G$ *et* G/N *abélien, alors* $[G,G] \leq N$ *et* $G/[G,G]$ *est un quotient abélien groupe de* G*.*

Remarque 1.2.7 .

Si G *est abélien on a* $D(G) = \{1\}$*.*

Définition 1.2.15 .

On pose $D^0(G) = G$

$$D^1(G) = D(G) \text{ et } \forall i \geq 1 \text{ on defini } D^{i+1}(G) = D(D^i(G)).$$

D'aprés ce qui précé de chaque $D^{i+1}(G)$ *est normal dans* $D^i(G)$ *et le quotient* $D^i(G)/D^{i+1}(G)$ *est abélien.*

La suite: $G \rhd D^1(G) \rhd D^2(G) \rhd ... \rhd D^n(G)$ *s'appele la série dérivée de* G *et* $D^i(G)$ *s'appelle le* $i^{éme}$ *groupe derivé de* G*.*

Théorème 1.2.3 [7]*.*

Soit $f : G_1 \to G_2$ *un homorphisme de groupe,* $\forall n \in N : f(D^n(G_1)) \subseteq D^n(G_2)$*, et on a l'égalité si* f *est surjectif. Ou:* $f(D^n(G_1)) = D^n(G_2)$*.*

Théorème 1.2.4 [7]*.*

Soit G *un groupe. Les groupes* $D^n(G)$ *sont des ses groupes caractéristique (et donc distingués) de* G*.*

Proposition 1.2.4 .

Soient G *un groupe et une suit de sous-groupe possédant les propriétés suivantes:*

$G_0 = G$ *et* $\forall n \in \mathbb{N}, G_{n+1}$ *est un sous-groupe distingué de* G_n *tel que:*G_n/G_{n+1} *soit commutatif.*

Alors $D^n(G) \subseteq G_n, \forall n \in \mathbb{N}$*.*

Lemme 1.2.1 [7]*.*

1) $h : G \to G$ *(*h *automorphisme de* G*), on a* $D(G) = h(D(G))$ *pour tout automorphisme de* G *en particulier* $D(G)$ *est un sous-groupe normal de* G*.*

2) Si F *est un sous-groupe de* G *on a* $D(F) \subseteq D(G)$*.*

3) Si $l : G \to G'$ *est un morphisme surjectif, alors* $D(G') = l(D(G))$*.*

4) Soit $H \lhd G$*, alors* G/H *abélien* $\Leftrightarrow D(G) \subseteq H$*.*

Preuve. [7] ■

1.2.3 Morphismes des groupes

Définition 1.2.16 .

Soient $(G,*)$ et (H,T) deux groupes, une application de G dans H est un morophisme de groupe lors que:

$$\forall x,y \in G, f(x*y) = f(x)\,T\,f(y)$$

Exemple 1.2.6 .

$f : (\mathbb{R},+) \longmapsto (\mathbb{R}^*,\times)$

$f(x) = 2^x$, *f homorphisme?*

$\forall x,y \in \mathbb{R} : f(x+y) = 2^{(x+y)} = 2^x \times 2^y = f(x) \times f(y)$,

donc f homorphisme.

Remarque 1.2.8 .

Soit $f : G \longrightarrow G$:

1) Si $G = H$ et $* = T$ on parle d'endomorphisme.

2) Si f est un bigective on parle d'isomorphisme.

3) Si f est un endomorphisme f bigective on parle d'automorphisme.

4) Si f est un morphisme surjectif on parle d'épimorphisme.

Proposition 1.2.5 [7].

Quel que proprité élémentaires des morphisme de groupe, f est ici un morphisme de $(G;*)$ dans (H,T):

1) $f(e_G) = e_H$.

2) Si f est un isomorphisme, alors son application reciproque realise un isomorphisme de (H,T) sur $(G,*)$.

3) Si $G_1 < G$ alors $f(G_1) < H$.

4) Si $H_1 < H$ alors $f^{-1}(H_1) < G$.

Définition 1.2.17 .

Soit f un morphisme de G vers H tel que:

$f : G \longrightarrow H$:

1) Noyau de f noté $\ker(f)$ *est l'ensemble de autécedonts par f de e_H:*

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

2) L'image de f, noté $\mathrm{Im}(f)$ *ou $f(G)$, tel que:*

$$\mathrm{Im}(f) = \{y \in H, \exists x \in G : f(x) = y\}$$

Remarque 1.2.9 .

f est surjectif $\Leftrightarrow \mathrm{Im}(f) = G$.

Proposition 1.2.6 [4].

Soit f un morphisme de $(G, *)$ dons (H, T) alors f est injectif si et seulement si son noyau est reduit à $\{e_G\}$.

Chapitre 2

Divers groupes

2.1 Le groupe symétrique

2.1.1 Le Groupe S_n

Définition 2.1.1 .

Soit n un entier naturel non nul.

Le groupe symétrique S_n est l'ensemble de bijections de $\{1, ..., n\}$.

Les éléments du groupe symétrique S_n sont appellés des permutations.

Notation 2.1.1 .

Dans S_n ,on peut écrire une permutation σ sous la forme suivant: $\sigma_r = \begin{pmatrix} 1 & 2 & .... & n \\ \sigma(1) & \sigma(2) & .... & \sigma(n) \end{pmatrix}$

$\sigma_0 = \begin{pmatrix} 1 & 2 & .... & n \\ 1 & 2 & .... & n \end{pmatrix}$ *est une permutation identité.*

Exemple 2.1.1 .

Le groupe S_3 à $3! = 6$ permutations à savoir:

$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$

$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$

On definit le produit de permutation comme composition des applications,comme suite:

soient r et $\sigma \in S_n$, la permutation $\sigma \circ r$ est definis par :

$$\sigma \circ r = \begin{pmatrix} 1 & 2 & .... & n \\ \sigma \circ r(1) & \sigma \circ r(2) & .... & \sigma \circ r(n) \end{pmatrix}$$

avec $\sigma \circ r(i) = \sigma(r(i)), \forall i \in [1, n]$.

Exemple 2.1.2 .

Dans S_3 on a:

$$\sigma_1 \circ r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_2, r_3 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = r_1$$

on remarque que: $\sigma_1 \circ r_3 \neq r_3 \circ \sigma_1$, donc le groupe S_3 est non abélien.

Remarque 2.1.1 .

1) S_n est d'ordre $n!$.

2) S_1 et S_2 sont abélien.

3) Pour $n \geq 3$, S_n n'est pas abélien.

2.1.2 Orbites De S_n

Définition 2.1.2 .

Soit $\sigma \in S_n$ la relation $\Re_\sigma$ définie sur $[[1, n]]^2$ par:

$x \Re_\sigma y \iff \exists n \in \mathbb{Z}, y = \sigma^n(x)$ est une relation d'équivalence.

Ses classes d'équivalences sont appelées les orbites de σ, ou σ-orbites.

On note $orb_{\langle\sigma\rangle}(x) = \{\sigma^n(x), n \in \mathbb{Z}\}$ la σ-orbite de x.

(i.e la classe d'équivalence de x pour la relation $\Re_\sigma$).

2.1.3 Cycle De S_n

Définition 2.1.3 .

On dit qu'une permutation $\sigma \in S_n$ est un cycle s'il existe une seule

σ-orbite O non triviale (i.e card $O > 1$), s'il en est ainsi, le cardinal de O s'appelle la longueur du cycle σ et O en est le support.

Proposition 2.1.1 .

Deux cycles σ et ó à supports disjoints commutents.

Proposition 2.1.2 [11].

Tout permutation $\sigma \in S_n \setminus \{Id\}$ s'ecrit de façon unique (à l'ordre près des facteurs) $\sigma = c_1 c_2 .....c_p$ où les c_i sont des cycles à supports disjoints (deux à deux).

Corollaire 2.1.1 [11].

Soit $n \in \mathbb{N}$, $n \geq 2$.

1) S_n est engendré par les transpositions.

2) S_n est engendré par les $n-1$ transpositions $(1,i)$ où $i \in [[2,n]]$.

3) S_n est engendré par les $n-1$ transpositions $(i,i+1)$ où $i \in [[1,n-1]]$.

2.1.4 Signature d'une permutation

Définition 2.1.4 .

Soit $\sigma \in S_n$,on appelle signature de σ l'entier noté $sgn(\sigma)$ et defini par: $sgn(\sigma) = (-1)^k$ où k est la parité du nombre de transposition dans la décomposition de σ.

Exemple 2.1.3 .

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$, *on a* $\sigma = (1,2)(3,4,5) = (1,2)(3,5)(3,4)$ *donc* $sgn(\sigma) = (-1)^3 = -1$.

Théorème 2.1.1 .

La signature d'une permutation est un mophisme surjectif du groupe.

$\varphi : S_n \longrightarrow \{-1,1\}$.

Théorème 2.1.2 [11].

Soit σ une permutation. Soit m le cardinal du support de σ. Soit p le nombre de cycles dans la décomposition de σ en produit de cycles à supports disjoints.

Alors : $sgn(\sigma) = (-1)^{m+p}$.

2.1.5 Le groupe alterné A_n

Définition 2.1.5 .

On appelle groupe alterné A_n le noyau du morphisme sgn: $A_n = \ker(sgn)$. (Ensemble des permutations paires).

Proposition 2.1.3 [1].

1)A_n est un sous groupe normal propre de S_n, d'ordre $\frac{n!}{2}$.

2) A_3 est abélien.

3) Pour $n \geq 3$ A_n n'est pas abélien.

Preuve. [1] ■

Théorème 2.1.3 [1].

pour $n \geq 3$, le groupe alterné A_n est engendré par les 3-cycles.

Preuve. [1] ■

Théorème 2.1.4 [1].

Pour $n \geq 5$, le groupe alterné A_n est simple.

Preuve. [1] ■

2.2 Le Groupe Cyclique

Définition 2.2.1 .

Le groupe G est dit cyclique lors qu'il engendré par de ses éléments.

i.e G est un groupe cyclique $\iff \exists x \in G$ tel que $G = \langle x \rangle$.

Définition 2.2.2 .

Soit $(G, \times)$ un groupe finie , G est dit cyclique s'il existe un élément g de G, tel que $G = \langle g \rangle$. On dit que g est un générateur de G.

Exemple 2.2.1 .

$$C_8 = \{1, g, g^2, g^3, g^4, g^5, g^6, g^7\} \Rightarrow \begin{cases} |1| = 1 \\ |g^4| = 2 \\ |g^2| = |g^6| = 4 \\ |g^3| = |g^5| = |g^7| = |g| = 8 \end{cases}$$

Définition 2.2.3 .

On dit que G est monogéne s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Si de plus, G de fini, on dit alors qu'il est cyclique.

Exemple 2.2.2 .

$(\mathbb{Z}/5\mathbb{Z})$ *et fini* $|\mathbb{Z}/5\mathbb{Z}| = 5$ *tel que:* $\mathbb{Z}/5\mathbb{Z} = \{\mathring{0}, \mathring{1}, \mathring{2}, \mathring{3}, \mathring{4}\}$

$\mathbb{Z} = \langle -1, 1 \rangle$

$1 = 1$

$2 = 1 + 1$

$3 = 1 + 1 + 1$

$4 = 1 + 1 + 1 + 1$

$\mathbb{Z}/5\mathbb{Z} = (\mathbb{Z}_5, \times) = \{\mathring{0}, \mathring{1}, \mathring{2}, \mathring{3}, \mathring{4}\}$

$$\begin{cases} 5^0 = 1 \\ 5^2 = 0 \ \Rightarrow \mathbb{Z}_5 \neq \langle 5 \rangle \\ 5^3 = 0 \end{cases}$$

$$\begin{cases} 2^0 = 1 \\ 2^1 = 2 \\ 2^2 = 4 \ \Rightarrow \mathbb{Z}_5 = \langle 2 \rangle \\ 2^3 = 3 \\ 2^4 = 1 \end{cases}$$

Lemme 2.2.1 .

Soit G un groupe cyclique d'ordre q, alors : $G = \{1, x, x^2, ..., x^{q-1}\}$.

Théorème 2.2.1 .

Tout image d'un groupe cyclique par un epimorphisme est un groupe cyclique.

Théorème 2.2.2 [12].

Tout sous-groupe d'un groupe cyclique fini est cyclique.

Preuve. [12] ■

Théorème 2.2.3 [12].

Tout groupe fini d'ordre permier est cyclique.

Preuve. [12] ■

Théorème 2.2.4 .

Tout sous-groupe fini du groupe multiplicatif $k^* = k \setminus \{0\}$ d'un corps commutatif k est cyclique.

Proposition 2.2.1 .

Soit $(G, \times)$ un groupe cyclique de cardinal n. Le nombre de générateurs de G est $\varphi(n)$.

Proposition 2.2.2 .

Soit $(G, \times)$ un groupe cyclique de cardinal n, G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Remarque 2.2.1 .

Un groupe cyclique est nécessairement commutatif (abélien).

Un groupe cyclique engendré par un élément $g \neq 1$ a au mois deux éléments 1 et g.

Théorème 2.2.5 .

Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n, les générateurs de G sont les g^k, où k est un entier compris entre 1 et $n-1$ premier avec n.

Si $n \geq 2$ est un entier permier avec $\varphi(n)$, alors toute groupe commtatif d'ordre n est cyclique.

Théorème 2.2.6 .

Un groupe commutatif d'ordre pq, où p et q sont deux nombre premier distinctes est cyclique il est donc commutatif et isomorphe à $\mathbb{Z}p/q\mathbb{Z}$.

Théorème 2.2.7 .

Le groupe $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ est cyclique si et seulement si, les entiers p et q sont premiers entre eux-dans se cas $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ est isomorphe a $\mathbb{Z}/pq\mathbb{Z}$.

Théorème 2.2.8 .

Soit $G = \langle g \rangle$ un groupe cyclique d'ordre $n \geq 2$ pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G, c'est le groupe cyclique $H = \left\langle g^{n/d} \right\rangle$.

Théorème 2.2.9 [3].

Si p est un nombre premier impair et $\alpha \geq 2 \implies$ le groupe multiplicatif $(\mathbb{Z}^{\alpha}/\mathbb{Z})$ des éléments inversibles de $(\mathbb{Z}/p^{\alpha}\mathbb{Z})$ est cyclique pour $p = 2$ le groupe multiplicatif $(\mathbb{Z}/2^{\alpha}\mathbb{Z})$ est cyclique pour $\alpha = 1$, $\alpha = 2$ et non cyclique pour $\alpha \geq 3$.

Théorème 2.2.10 [3].

Soient G un groupe et H un sous-groupes distingue de G, les sous-groupes de groupe quotient G/H sont de la forme K/H où K est un sous-groupe de G qui contient H.

2.3 Le p-groupe

Définition 2.3.1 .

Un groupe G est un p-groupe s'il existe $p > 0$ et $\alpha > 0$ tel que:
$|G| = p^{\alpha}$.

Théorème 2.3.1 [2].

Tout groupe d'ordre p^2, $p > 0$,et p premier, est abélien.

Preuve. [2] ■

Théorème 2.3.2 .

Si G est un p-groupe fini avec $|G| > 1$, alors si $|G| = p^{\alpha}$, $\alpha \geq 1$, alors $|Z(G)| > 1$

Proposition 2.3.1 [2].

Tout p-groupe d'ordre p ou p^2 est abélien.

Preuve. [2] ■

2.3.1 Théorème de cauchy

Soit G un groupe fini d'ordre n et $\forall p > 0$ est premier et $p \mid n$, alors G possède un élément d'ordre p donc un sous-groupe d'ordre p.

2.3.2 Les théorèmes de sylow

Premier théorème de sylow

Soit G un groupe fini , soit p un nombre premier divisant $|G| = mp^n$ avec $n \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$ non divisible par p. Alors, pour tout entier $1 \leq r \leq n$ il existe un sous-groupe de G d'ordre p^r.

Second théorème de sylow

Soit G un groupe fini d'ordre $p^n m$ où p est premier, n et m sont entier positive et $p \wedge m = 1$. Alors tout les p-sous-groupe de sylow dans G sont conjugués et isomorphes.

Troisieme théorème de sylow

Soit G un groupe d'ordre $p^n m$ avec $n \geq 1$, p un nombre premier et $m \wedge p = 1$.

Alors un nombre n_p de p-sous-groupe sylow de G est $1 + kp$, (pour $k > 0$ et $n_p \nmid p^r m$.On a

$n_p \equiv 1 \,[\mathrm{mod}\, p]$).

Lemme 2.3.1 [2].

Soit S un p-groupe de sylow de G, et H un sous-groupe de G. alors il existe $a \in G$ tel que:

$aSa^{-1} \cap H$ est un p-groupe de sylow de H.

Preuve. [2] ■

Chapitre 3

Les groupes nilpotentes et les groupes résolubles

3.1 Les groupes nilpotents

3.1.1 Suite de composition

Définition 3.1.1 .

On appelle suite de compositon de G tout chaine finie des sous-groupes $G = G_0 \rhd G_1 \rhd ... \rhd G_i \rhd G_{i+1} \rhd ... \rhd G_n = \{e\}$ où $G_i \rhd G_{i+1}$ sinifie que G_{i+1} est un sous-groupes.

3.1.2 Suite centrale

Définition 3.1.2 .

On appelle suite centrale de G tout chaine finie ou infini des sous-groupes G.

On écrite $Z_i = Z_i(G)$ pour facilité l'écriture de cette suite.

$Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq Z_3 \trianglelefteq Z_4 ..... Z_n \trianglelefteq Z_{n+1} .....$

Avec $Z_1 \trianglelefteq Z(G/Z_0) ..... Z_{n-1} \trianglelefteq Z(G/Z_n)$ ce que assure que cette suite est une suite normale.

3.1.3 Le groupe nilpotent

Définition 3.1.3 .

Un groupe G est nilpotent s'il existe une suite central fini.

$Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq Z_3 \trianglelefteq Z_4 ..... Z_n = G.$

Avec $Z_1 \trianglelefteq Z\left(G/Z_0\right) ..... Z_{n-1} \trianglelefteq Z\left(G/Z_n\right)$

$n \geq 0$ *tel que* $Z_n\left(G\right) = \{1_G\}$ *ou* $Z_n\left(G\right) = G.$

Remarque 3.1.1 .

1) Tout groupe abélien est nilpotent.

car $Z\left(G\right) = G.$

2) Le groupe G est abélien si et seulement s'il est nilpotent de classe $\leq 1.$

Théorème 3.1.1 [7].

Un sous-groupe (resp-un groupe quotient) d'un groupe nilpotent est nilpotent.

Preuve. [7] ■

Proposition 3.1.1 [5].

Si G est un groupe, les propriétés suivantes sont équivalentes:

(i) G est nilpotent, de classe $\leq n.$

(ii) il existe une suite fini (H_k), $k = 0, ..., n$, *de sous-groupes normaux de G tel que* $\{1\} = H_0 \leq H_1 \leq ..... \leq H_{n-1} \leq H_n = G$ *avec* $H_{k+1}/H_k \leq Z\left(G/H_k\right)$, $\forall k = 0, ..., n - 1.$

Preuve. [5].

(i)⇒(ii). Il suffit de prendre $H_k = Z_k(G)$ pour $k = 0, 1, ..., n.$

(ii)⇒(i). A l'aide d'une récurrence sur k, montrons l'inclusion $H_k \subseteq Z_k(G)$ pour $k = 0, 1, ..., n$ (d'où $Z_n(G) = G$). L'inclusion étant triviale pour $k = 0$, supposons que l'on ait $H_k \subseteq Z_k(G)$. Soient $h \in H_{k+1}$ et $x \in G$. Puis que $H_{k+1}/H_k \leq Z(G/H_K)$, on a

$[h, x] \in H_k$, d'où $[h, x] \in Z_k(G)$. En d'autres termes, la classe de h modulo $Z_k(G)$ est

dans $Z(G/Z_k(G)) = Z_{k+1}(G)/Z_k(G)$, d'où $h \in Z_{k+1}(G)$, ce qui prouve l'inclusion $H_{k+1} \subseteq Z_{k+1}(G)$. ■

Proposition 3.1.2 [5].

Un groupe G est nilpotent si et seulement si la suite $(\gamma_k(G)), k \geq 1$ atteient le sous-groupe réduit à l'unité, le plus petit entier $k \geq 0$ tel que $\gamma_{k+1}(G) = \{1\}$ est égal à la classe de nilpotent de G.

Preuve. [5].

Supposons d'abord que G est nilpotent de classe n et montrons à l'aide

d'une récurrence sur k l'inclusion $\gamma_k(G) \leq Z_{n-k+1}(G)$ $(1 \leq k \leq n+1)$. Pour $k = 1$, on a $\gamma_1(G) = G = Z_n(G)$, d'où l'inclusion. Supposons que $\gamma_k(G)$ est inclus dans $Z_{n-k+1}(G)$ pour un entier k fixé; pour établir l'inclusion $\gamma_{k+1}(G) \leq Z_{n-k}(G)$, il suffit de montrer que $[y, x]$ est dans $Z_{n-k}(G)$ pour tout $x \in G, y \in \gamma_k(G)$. Or, $Z_{n-k+1}(G)/Z_{n-k}(G) \leq Z(G/Z_{n-k}(G))$ et $y \in Z_{n-k+1}(G)$ d'après l'hypothèse de récurrence d'où $[y, x] \in Z_{n-k}(G)$.

Pour $k = n+1$, l'inclusion qui vient d'être montré donne $\gamma_{n+1}(G) \leq Z_0(G)$, d'où

$\gamma_{n+1}(G) = \{1\}$ car $Z_0(G) = \{1\}$. De plus, si $m \geq 0$ est le plus petit entier tel que

$\gamma_{m+1}(G) = \{1\}$, on a $m \leq n$.

Supposons maintenant que la suite $(\gamma_k(G))$, $k \geq 1$ atteint le sous-groupe réduit à l'unité et notons m le plus petit entier tel que $\gamma_{m+1}(G) = \{1\}$. La suite (H_k) $k = 0, 1, ..., m$ définie par $H_k = \gamma_{m-k+1}(G)$ est constituée de sous-groupes normaux de G tels que:

$\{1\} = H_0 \leq H_1 \leq ... \leq H_{m-1} \leq H_m = G$.

De plus, pour $x \in G, y \in H_{k+1}$ (i.e. $y \in \gamma_{m-k}(G)$) on a $[y, x] \in \gamma_{m-k+1}(G)$ (i.e.

$[y, x] \in H_k$). En d'autres termes, on a établi l'inclusion $H_{k+1}/H_k \leq Z(G/H_k)$ pour tout entier $k \in \{0, 1, ..., m-1\}$. Donc G est nilpotent de classe $n \leq m$, d'où le résultat. ■

Proposition 3.1.3 [2].

Si un groupe G a un sous-groupe normal et nilpotent N tel que G/N soit nilpotent, alors G est nilpotent.

Preuve. [2] ■

Proposition 3.1.4 .

Soit G un groupe nilpotent.Alors tous sous-groupe propre H de G est strictement contenu dans son normalisateur $N_G(H) = \{g : g \in G, gHg^{-1} = H\}$.

Définition 3.1.4 .

Si un groupe G est engendré par une partie $S \subseteq G$, alors $\gamma_n(G)$ est engendré par les éléments de la forme $x^{-1}[a_1, ..., a_n]\, x$, $(a_1, ..., a_n \in S, x \in G)$.

Définition 3.1.5 .

G un groupe engendré par une partie $S \subseteq G$.Supposons que pour un entier fixé $n > 0$, on ait $[a_1, ..., a_n] = 1$ pour tout $a_1, ..., a_n \in S$. Alors G est nilpotent, de classe $< n$.

Définition 3.1.6 .

$\forall n \geq 1, \gamma_n(G)$ est engendré par les éléments de la forme $[x_1, ..., x_n]$ $(x_1, ..., x_n \in G)$.

Lemme 3.1.1 [11].

Un groupe G est nilpotent si et seulement s'il existe entier $n \geq 1$ tel que $[x_1, ..., x_n] = 1$ quel que soit $x_1, ..., x_n \in G$.Si n est le plus petit entier vérifiant cette condition, la classe de nilpotent de G est égale à $n - 1$.

Preuve. [11] ■

Corollaire 3.1.1 .

Soient G est un groupe nilpotent de classe n et H sous-groupe de G. Alors:

1) H est nilpotent de classe $\leq n$.

2) Si H est normal dans G, G/H est nilpotent de classe $\leq n$.

Théorème 3.1.2 [5].

Soient G un groupe et H un sous-groupe de G inclus dans $Z(G)$ (H est donc normal dans G). Si G/H est nilpotent de classe n, alors G est nilpotent, de classe $\leq n + 1$.

Preuve. [5].

Pour tout $x_1, ..., x_n \in G$, on a $[x_1, ..., x_n] \in H$, d'où, pour tout $x_{n+1} \in G, [x_1, ..., x_n, x_{n+1}] = 1$ car $H \leq Z(G)$ ■

Corollaire 3.1.2 [7].

Tout p-groupe fini alors G est nilpotent.

Preuve. [7].

Soit G un p-groupe d'ordre $p^n, (n \geq 0)$. Raisonnons par récurrence sur n.

Si $n = 0, G$ est nilpotent ($G = \{1\}$).

Considérons maintenant un entier $n > 0$ et supposons que tous les p-groupes d'ordre $p^{n'}$ sont nilpotents (pour tout entier $n' < n$).

D'après la proposition précédente, $Z(G) = \{1\}$, donc $G/Z(G)$ est d'ordre $p^{n'}$ $(n' < n)$; le groupe $G/Z(G)$ est donc nilpotent. Le théorème (3.1.2) montre qu'il en est de même pour G. ■

Proposition 3.1.5 [7].

Si G est un groupe, les propriétés suivantes sont équivalentes:

1) G est nilpotent.

2) chaque sous-groupe de G est sous-groupe normal.

3) chaque sous-groupe de sylow de G est normal.

Preuve. [7] ■

Proposition 3.1.6 [2].

G un groupe nilpotent et H un sous-groupe normal de G. Alors, si H est distinct de $\{1\}, H \cap Z(G)$ est aussi distinct de $\{1\}$.

Preuve. [2].

Soit $h \in H \backslash \{1\}$. Considérons l'ensemble E des entiers $n > 0$ vérifiant :

$[h, x_1, ..., x_n] = 1$ pour tout $x_1, ..., x_n \in G$.

Cet ensemble étant non vide (il contient tout entier supérieur ou égal à la classe de nilpotence de G), notons k son plus petit élément. L'entier $k - 1$ n'est pas dans E: il existe donc des éléments $a_1, ..., a_{k-1}$ dans G tels que $u = [h, a_1, ..., a_{k-1}] = 1 (u = h$ si $k = 1$). Par contre k est dans E, d'où l'égalité $[u, x_k] = [h, a_1, ..., a_{k-1}, x_k] = 1$ pour tout $x_k \in G$. En d'autres termes, l'élément u est dans $Z(G)$. Mais il est aussi dans H ($h \in H$ et $H \rhd G$), d'où l'existence d'un élément distinct de 1 dans $H \cap Z(G)$. ■

Proposition 3.1.7 .

Soient $H_1, ..., H_k$ des sous-groupe normaux d'un groupe G, si ces sous-groupe sont nilpotents de classes respectives $c_1, ..., c_k$, alors $H_1...H_k$ est nilpotent de classe au plus $c_1 + ... + c_k$.

Preuve. .

Il suffit de prouver cette proposition pour $k = 2$; le cas général résulte

ensuite d'une récurrence sur k. Pour cela, il faut montrer que pour $n = 1 + c_1 + c_2$, on a $[a_1, ..., a_n] = 1$ pour tout $a_1, ..., a_n \in H_1 \cup H_2$. Notons n_1 (resp. n_2) le cardinal de l'ensemble des indices i tels que a_i soit dans H_1 (resp. H_2). On ne peut donc pas avoir simultanément les inégalités $n_1 \leq c_1$ et $n_2 \leq c_2$ car $n_1 + n_2 \geq 1 + c_1 + c_2$; supposons par exemple que l'on ait $n_1 > c_1$, c'est à dire $n_1 \geq 1 + c_1$. Soit i_0 le plus petit indice tel que a_{i_0} soit dans H_0. A l'aide d'une récurrence sur m ($i_0 \leq m \leq n$), il est facile de voir que $[a_1, ..., a_m] \in \gamma_{m'}(H_1)$, où m' est le nombre d'indices $i \in \{1, ..., m\}$ tels que a_i soit dans H_1. Il en résulte que $[a_1, ..., a_n]$ est dans $\gamma_{n_1}(H_1) = \{1\}$, d'où $[a_1, ..., a_n] = 1$. ■

Proposition 3.1.8 [2].

Les p-groupes sont nilpotents.

Preuve. [2].

On va en donner deux démonstrations.

• Soit p un p-groupe; alors p peut se plonger dans $GL_n(Z/pZ)$ pour un entier n suffisamment grand. Donc p est contenu dans un p-Sylow de $GL_n(Z/pZ)$, qui est conjugué diagonaux égaux à 1.

• On peut supposer $p \neq \{1\}$. Faisons opérer p sur lui-même par automorphismes intérieurs; l'ensemble des points fixes est le centre $C(p)$ de p. Comme p est un p-groupe,$|p| \equiv |C(p)| (\mathrm{mod}\, p)$, donc $C(p) \geq \{1\}$. Ainsi $p/C(p)$ est d'ordre strictement inférieur à celui de p. ■

3.2 Le groupe résoluble

Définition 3.2.1 .

Un groupe G est résoluble lorsqu'il existe une suite finie $G_0 \leq G_1 \leq \ldots \leq G_n$ de sous-groupes de G telle que :

où $\forall i \in [0, n-1], G_i \trianglelefteq G_{i+1}$ et le groupe quotient G_{i+1}/G_i est abélien .

Définition 3.2.2 .

Un groupe G est dit résoluble s'il existe un nombre naturel n tel que $D^n(G) = 1$ Dans ce cas, le plus petit nombre naturel n tel que $D^n(G) = 1$ est appelé la classe de résolubilité de G. On dit aussi que G est résoluble de classe n.

Exemple 3.2.1 .

1) Tout groupe fini d'ordre impair est résoluble.

2) Le groupe symétrique S_n n'est résoluble que si $n \leq 4$.

Pour S_4:

$H_0 = S_4, H_1 = A_4, H_2 = \{e, (12)(34), (13)(24), (14)(23)\}, H_3 = \{e\}$

On note H_0/H_1 est groupe d'ordre 2, H_1/H_2 est groupe d'ordre 3,

et $H_2/H_3 \cong H_2$ est groupe d'ordre 4, et tous les groupes quotients est abelien.

3) Tout groupe abélien est résoluble.

Remarque 3.2.1 .

1) Si G est un groupe résoluble de classe n, la suite finie est évidemment strictement décroissante.

2) Un groupe est résoluble de classe 0 si et seulement s'il est réduit à l'élément neutre.

3) Un groupe est résoluble de classe 1 si et seulement s'il est commutatif et non réduit à l'élément neutre.

4) Un groupe résoluble non réduit à l'élément neutre est distinct de son dérivé.

5) Un groupe G est résoluble si et seulement si $D(G)$ est résoluble. Si $D(G)$ est résoluble de classe n et que G n'est pas réduit à l'élément neutre (auquel cas, d'après la remarque précédente, $D(G)$ est distinct de G), G est résoluble de classe $n+1$.

6) Un groupe simple non commutatif n'est pas résoluble.

7) Soit $f : G_1 \to G_2$ un homomorphisme d'un groupe G_1 dans un groupe G_2. Nous avons vu que pour tout n, $f(D^n(G_1))$ est égal à $D^n(f(G_1))$. Il en résulte que si G est un groupe résoluble de classe n, $f(G)$ est résoluble de classe $\leq n$. En particulier, si H est un sous-groupe distingué de G, si G est résoluble de classe n, alors G/H est résoluble de classe $\leq n$.

8) Nous avons vu que si H est un sous-groupe d'un groupe G, $D^n(H)$ est contenu dans $D^n(G)$ pour tout n. Donc si G est un groupe résoluble de classe n, tout sous-groupe de G est résoluble de classe $\leq n$.

Proposition 3.2.1 [7].

On suppose G non réduit à $\{1\}$.

G est résoluble ssi il existe une suite finie décroissante de sous-groupes de G:

$\{1\} = H_n \subset H_{n-1} \subset ... \subset H_0 = G$, tels que pour tout i compris entre 0 et $n-1, H_{i+1}$ est normal dans H_i et H_i/H_{i+1} est abélien.

Preuve. [7].

($\Rightarrow$) Comme G est résoluble, il existe un entier $n > 0, (G = \{1\})$ tel que $D^n(G) = \{1\}$.

Pour tout i compris entre 0 et n, on pose $H_i = D^i(G)$. $H_0 = G, H_n = \{1\}$

Comme $D^{i+1}(G) = D(D^i(G)) \subset D^i(G), (H_i)$ est une suite décroissante.

D^{i+1} est normal dans $D^i(G)$ et $D^i(G)/D^{i+1}(G)$ est abélien donc H_{i+1} est normal dans H_i et H_{i+1}/H_i est abélien.

($\Leftarrow$) Soit $(H_i)_{0 \leq i \leq n} (n > 0)$ une suite finie décroissante de sous-groupes de G, telle que $H_0 = G, H_n = \{1\}$, pour tout i compris entre 0 et $n-1, H_{i+1}$ est normal dans H_i et H_i/H_{i+1} est abélien.

H_1 est normal dans H_0 et H_0/H_1 est abélien, donc $D(G)$ est inclus dans H_1.

H_2 est normal dans H_1 et H_1/H_2 est abélien, donc $D(H_1)$ est inclus dans H_2.

Comme $D(G)$ est inclus dans $H_1, D^2(G) = D(D(G))$ est inclus dans $D(H_1)$ d'où dans H_2.

En répétant le même procédé pour $i = 3, ..., n$, on trouve $D^n(G)$ inclus dans $H_n = \{1\}$ et par conséquent $D^n(G) = \{1\}$. ■

Théorème 3.2.1 [11].

Soient G un groupe et H un sous-groupe distingué de G. Si G/H est résoluble de classe p et H résoluble de classe q, G est résoluble de classe $\leq p + q$.

Preuve. [11].

Soit π l'homomorphisme canonique de G sur G/H. Nous avons $\pi(D^p(G)) = D^p(\pi(G)) = D^p(G/H)$. Par définition de $p, D^p(G/H) = 1$, donc $\pi(D^p(G)) = 1$, c'est-à-dire que $D^p(G) \subseteq$

H. Dès lors, $D^q(D^p(G)) \subseteq D^q(H)$, autrement dit $D^{p+q}(G) \subseteq \{1\}$, donc G est bien résoluble de classe $\leq p+q$. ■

Remarque 3.2.2 .

G peut être résoluble de classe $< p+q$. Prendre par exemple pour G le produit direct d'un groupe commutatif non trivial H par un groupe commutatif non trivial K. Alors G, H et G/H (qui est isomorphe à K) sont tous trois résolubles de classe 1.

Théorème 3.2.2 [2].

Soient G un groupe et n un nombre naturel. Les trois conditions suivantes sont équivalentes :

1) G est résoluble de classe $\leq n$;

2) il existe une suite de composition $G = G_0 \supseteq G_1 \supseteq ... \supseteq G_n = 1$ où tous les G_i sont distingués dans G et dont tous les quotients sont commutatifs;

Preuve. [2].

$1 \Rightarrow 2$. Il suffit évidemment de prendre G_i égal à $D^i(G)$.

Prouvons que 2 entraîne 1. Dans l'hypothèse 2, $D^i(G) \subseteq G^i$ pour tout i. C'est vrai en particulier pour $i = n$, donc $D^i(G) = 1$, donc G est résoluble de classe $\leq n$, ce qui prouve 1). ■

Théorème 3.2.3 [11].

Tout groupe cyclique est résoluble.

Preuve. [11].

Car un groupe cyclique est abélien. ■

Corollaire 3.2.1 .

Tout groupe quotient d'un groupe résoluble est un groupe résoluble.

Preuve. .

En effet, un groupe quotient de G est une image homomorphe de G par la surjection canonique. ■

Théorème 3.2.4 [7].

Toute image par un homomorphisme d'un groupe résoluble est un groupe résoluble.

Preuve. [7].

Si G est une image homomorphe du groupe résoluble G, alors il existe un homomorphisme surjectif $f : G \to G'$. Si

$\{e\} = H_0 \subseteq H_1 \subseteq ... \subseteq H_n = G$

est une chaîne normale de G à facteurs abéliens, alors la chaîne

$\{e'\} = H'_0 \subseteq H'_1 \subseteq ... \subseteq H'_n = G'$

où $H'_i = f(H_i)$ pour $i = 1, ..., n-1$ est normale et ses facteurs sont des images homomorphes de ceux de la chaîne de G. Il en résulte que la chaîne est une chaîne G' normale à facteurs abélien. Ceci prouve que G' est résoluble. ■

Théorème 3.2.5 [2].

Si $f : G \to G'$ est un homomorphisme injectif et si G' est résoluble, alors G est résoluble.

Preuve. [2].

Si G' est résoluble, alors il possède une chaîne normale

$\{e'\} = H'_0 \subseteq H'_1 \subseteq ... \subseteq H'_n = G'$

à facteurs abéliens. La chaîne

$\{e\} = H_0 \subseteq H_1 \subseteq ... \subseteq H_n = G$

où $H_i = f^{-1}(H'_i)$ pour $i = 1, ..., n$ est une chaîne normale et il existe homomorphisme injectif $v_i : H_{i+1}/H_i \to H'_{i+1}/H'_i$. Il en résulte que les facteurs de la chaîne G de sont tous abéliens, ce qui prouve G que est résoluble. ■

Corollaire 3.2.2 .

Tout sous-groupe K d'un groupe résoluble est un groupe résoluble.

Preuve. .

Il suffit d'appliquer le théorème précédent à l'injection canonique. ■

Théorème 3.2.6 [2].

Si G possède une chaîne normale dont les facteurs sont des groupes résolubles, alors G est résoluble.

Preuve. [2].

Soit $\{e\} = H_0 \subseteq H_1 \subseteq ... \subseteq H_n = G$

une chaîne normale de telle que tous les facteurs $F_i = H_{i+1} \diagup H_i$ sont résolubles. Nous avons démontré que l'on peut utiliser ces chaînes normales des facteurs pour construire une chaîne normale de G dont les facteurs sont isomorphes aux facteurs des différentes chaînes normales des facteurs. Mais les chaînes des F_i peuvent être choisies à facteurs abéliens, il en résulte que les facteurs de la chaîne concaténée sont tous abéliens et G est résoluble. ■

Théorème 3.2.7 [7].

Soit H des sous-groupes distingué de G. G est résoluble, si et seulement si, H et $G \diagup H$ sont résolubles.

Preuve. [7].

Si G est résoluble, alors H et $G \diagup H$ sont résolubles comme nous l'avons vu. Réciproquement, si H et $G \diagup H$ sont résolubles, alors $\{e\} \subseteq H \subseteq G$

est une chaîne normale de G dont les facteurs $F_1 = H \diagup \{e\} \approx H$ et $F_2 = G \diagup H$ sont résolubles. Il en résulte que G est résoluble. ■

Théorème 3.2.8 [2].

Si G est un groupe résoluble, alors possède une chaîne normale dont les facteurs sont des groupes cycliques d'ordres premiers.

Preuve. [2].

Soit $\{e\} = H_0 \subseteq H_1 \subseteq ... \subseteq H_n = G$

une chaîne normale à facteurs abéliens. Nous supposons que cette chaîne est la plus longue des chaînes normales de G à facteurs abéliens. Si un facteur F_i n'était pas un groupe cyclique d'ordre premier, alors F_i possède un sous-groupe propre et G possède un sous-groupe H tel que$H_i \subseteq H \subseteq H_{i+1}$. H est distingué dans H_{i+1}, car si $x \in H_{i+1}$et $y \in H$, alors $\bar{x}^{-1}\overline{yx} = \overline{y}$ (F_i est abélien). Il en résulte $x^{-1}yxy^{-1} \in H_i \subseteq H$ et $x^{-1}yx = (x^{-1}yxy^{-1})\, y \in H$. D'un autre côté,$H \diagup H_i$ est abélien (sous-groupe de F_i) et $H_{i+1} \diagup H$ est abélien car nous avons

$H_{i+1} \diagup H \simeq (H_{i+1} \diagup H_i) \diagup (H \diagup H_i)$

et $(H_{i+1}/H_i)/(H/H_i)$ est abélien car c'est un quotient du groupe abélien F_i. Ainsi, si nous insérons H entre H_i et H_{i+1} nous obtenons une chaîne normale à facteurs abéliens plus longue que la plus longue des telles chaînes. ■

Proposition 3.2.2 [2].

Soit G un groupe et soit n un entier > 1. Les propriétés suivantes sont équivalentes :

(1) G est résoluble de classe $\leq n$,

(2) Il existe une suite $G = G_0 \supset G_1 \supset ... \supset G_n = \{1\}$ de sous-groupes normaux de G tels que $Gi/Gi+1$ soit abélien pour $0 \leq i \leq n-1$,

(2') Il existe une suite $G = G_0 \supset G_1 \supset ... \supset G_n = \{1\}$ de sous-groupes de G tels que G_i soit normal dans G_{i-1} et que G_{i-1}/G_i soit abélien, pour $1 \leq i \leq n$,

(3) Il existe un sous-groupe abélien A normal dans G tel que G/A soit résoluble de classe $\leq n-1$.

Preuve. [2].

(1) $\Rightarrow$ (2) Posons $G_i = D^iG$ pour tout $i > 0$. Puisque $D(G)$ est stable par tout automorphisme (même non intérieur!) de G, D^iG est normal dans G pour tout i. La suite $(G_i)_{i>0}$ ainsi définie vérifie donc (2).

(2) $\Rightarrow$ (2') est trivial.

(2') $\Rightarrow$ (1) Par récurrence sur k on voit que $D^kG \subset G_k$ pour tout k, d'où $D^nG = \{1\}$.

(1) $\Rightarrow$ (3) On prend $A = D^{n-1}G$.

(3) $\Rightarrow$ (1) D'après l'implication (1) $\Rightarrow$ (2), appliquée à G/A et à $n-1$, il existe une suite $A_0 = G \supset A_1 \supset ... \supset A_{n-1} = A$

de sous-groupes normaux de G telle que la suite des quotients

$G/A \supset A_1/A \supset ... \supset A_{n-1}/A = \{1\}$

vérifie la condition (2). Alors la suite

$G \supset A_1 \supset ... \supset A_{n-1} \supset \{1\}$

vérifie la condition (2) et l'implication (2) $\Rightarrow$ (1) appliquée à G et à n permet de conclure. ■

Remarque 3.2.3 .

Tout sous-groupe (et tout groupe quotient) d'un groupe résoluble de classe $\leq n$ est résoluble de classe $\leq n$.

Corollaire 3.2.3 .

Deux p-Sylow d'un groupe résoluble sont conjugués.

Proposition 3.2.3 [5].

Tout groupe nilpotent est résoluble.

Preuve. [5].

C'est une conséquence du résultat suivant: pour tout groupe G et pour

tout entier $k \geq 0$, on a l'inclusion $G(k) \leq \gamma_{2k}(G)$. En effet, si G est nilpotent de classe c, en choisissant k tel que $2k > c$, on aura $G(k) = \{1\}$. Montrons donc par récurrence l'inclusion précédente. Pour $k = 0$, le résultat est trivial. Supposons que $G(k) \leq \gamma_{2k}(G)$. On a alors:

$G(k+1) = [G(k), G(k)] \leq [\gamma_{2k}(G), \gamma_{2k}(G)]$. Mais $[\gamma_{2k}(G), \gamma_{2k}(G)] \leq \gamma_{2k} + 2k(G) = \gamma_{2k} + 1(G)$, d'où l'inclusion $G(k+1) \leq \gamma_{2k} + 1(G)$. ■

Remarque 3.2.4 .

Tout groupe resoluble n'est pas en générale nilpotent.

Contre exemple $G = S_3$ resoluble, mais n'est pas nilpotent.

Exemple 3.2.2 .

Pour $n \geq 5, A_n$ et S_n ne sont pas résolubles.

Preuve. .

Soit $n \geq 5$. A_n n'est pas résoluble, puisque $A_n = D_i(A_n)$

pour tout $i \geq 1$. Par conséquent, S_n ne l'est pas non plus,

. Plus précisément, comme tout commutateur est de signature 1, on a $D(S_n) \subseteq A_n$ pour tout n, et l'égalité $A_n = D(A_n)$ entraîne a fortiori $A_n = D(S_n)$. ■

On résulte que :

groupes abélien $\subset$ groupes nilpotent $\subset$ groupes résolubles .

On général on trouve:

groupes abélien $\subset$ groupes nilpotent $\subset$ groupes super résolubles $\subset$ groupes résolubles.

Conclusion Générale

Nous avons présenté dans notre mémoire les plus intéressant propriétés de groupe finie pour définir ce la on à rappelé les définitions et propriétés des groupes ,sous -groupes distinguées, homomorphisme des groupes et quel que divers groupe, (groupe abélien, cyclique, symétrique ,et les p-groupes. . . . .).Pour bien étudier les groupesnilpotents et les groupes résolubles.

Bibliographie

[1] Claude Mutafian, Le défi Algébrique, DURAND, 28600 Luisant, FRANCE, 1975.

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

[3] Francois Dumas, Algéber: Groupes et Anneaux 2, Polycopi´e du cours 2004-2005.

[4] Gabor Wiese et Agnès David, Algèbre 2, Université du Luxembourg, Version du 31 mai 2013.

[5] Gerard Endimioni, Une introduction aux groupes nilpotents, . Cours de DEA 1996/1997 (Université de Provence - France), 1997.

[6] Hitta.Amara, Cours D'algébre et exercices corrigés, OPU 1994.

[7] Jean-Pierre Serre, Groupes finis, Cours à l'Éco le Normale Sup érieure de Jeunes Filles, 1978/1979.

[8] Maarouf Abd Elrahman Samhan et Faoizi Ben Ahmed Saleh Eldaquir, Théorie Des Groupes Arabique, Université de Roi Saoud.

[9] Muriel Galley, Seminaire thématique : Théorie de Galois, 24 mai 2012.

[10] Nicolas JACON, Complement De Théorie Des Groupe, Université de Reims.

[11] perso.wanadoo, Théorie Des Groupes, http://perso.wanadoo.fr/cyd60000theoriedesgroupes@orange.fr

[12] D. Schaub, Elements De La Théorie Des Groupes, Université d'Angers 1997/1998.

ملخـــص

لـقد تطرقنـا فـي بحثنـا هـذا إلـى أهـم خـواص الـزمر المنتهيـة , و لأجـل معـرفة ذلك جيدا ذكـرنا بأهـم التعـاريف و الخـواص الخـاصة بالزمـر و الزمـر الجزئيـة الناظميـة و تمـاثـل الزمـر وتطبيقاتهـا, وذكـرنا أهـم أنـواع الزمـر(الزمـر التبديليـة – الدوريـة – التناظريـة - p زمـرة ....)

و ذلك ليتسنـى لنـا دراسـة الزمـر عديمـة القـوى والزمـر التحليليـة و المقارنـة بينهمـا وإعطـاء أمثلـة مناسبـة.

الكلمات المفتاحية: الزمر- الزمر الجزئية - التشاكل - السلاسل – الزمر عديمة القوى –الزمر التحليلية

Résumé

Nous avons présenté dans notre mémoire les plus intéressant propriétés de groupe finie pour définir ce la on à rappelé les définitions et propriétés des groupes , sous -groupes distinguées, homomorphisme des groupes et quel que divers groupe, (groupe abélien, cyclique ,symétrique et les p-groupes……). Pour bien étudier les groupes nilpotents et les groupes résolubles.

Les mots clée : groupes, sous- groupes, morphisme, série, groupe nilpotent, groupe résoluble.

.

Abstract

We are study in our memory to important properties of fini groups . We are recall the définitions and propretiés of groups , subgroups, normal subgroups , homomorphisme of groups and their applications and setting the divers groups, (abélien group, cyclic group, symétrique group and p-groups…….). Which permit to study the nilpotents and solvables groups.

In finally given exemples and comparison between the nilpotents groups and solvables groups.

Kye words : group, sub-group, homomorphism, nilpotent group, solvable group.