UNIVERSITE KASDI MERBAH OUARGLA

Faculté des Mathématiques et des Sciences de la Matière

N° d'ordre :
N° de série :

DEPARTEMENT DES MATHEMATIQUES

MASTER

Spécialité : Mathématiques

Option : Géométrie et Algèbre

Par : Sidali Youmbai

Thème

Groupes morphiques

Soutenu publiquement le : 25/05/2017

Devant le jury composé de :

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

Dédicaces

Aucune dédicace ne saurait exprimer mon respect, ma gratitude, et ma considération pour les sacrifices de :

Kennouzi Milouda

Zaatra abdel malek

Je vous remercie pour tout le soutien, et tous les conseils, et pour m'avoir aidé à traverser des moments difficiles.

Que ce modeste travail soit l'exaucement du fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez.

Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

Remerciements

Je remercie tout d'abord Dieu tout puissant de m'avoir donné le courage, la force et la patience d'achever ce modeste travail.

Le seul moyen de se délivrer d'une tentation, c'est d'y céder paraît-il.
Alors j'y cède en disant un grand Merci aux personnes qui ont cru en moi et qui m'ont permis d'arriver au bout de ce mémoire.
Je tiens à exprimer mes plus vifs remerciements à M^{r} **Ben Moussa** qui m'a proposé le thème de ce mémoire.

J'exprime tous mes remerciements à l'ensemble des membres de mon jury : Messieurs Boussaid Mohamed, Youmbai M.Laid, Bahayou Amine et Yassine Gerbouusa.

J'adresse toute ma gratitude à tous mes ami(e)s et à toutes les personnes qui m'ont aidé dans la réalisation de ce travail.

Table des matières

Notations

➤ G désigne en générale un groupe fini.

➤ $End(G)$ est l'ensemble des endomorphismes de G.

➤ On note C_n le groupe cyclique d'ordre n.

➤ Si $\alpha \in End(G)$, l'image $Im(\alpha) = \alpha(G)$ est souvent notée $G\alpha$.

➤ Si H est un sous-groupe d'un groupe K, ou H est un sous-espace d'un espace vectoriel K, nous notons $H \lessdot K$ pour indiquer que H est maximal dans K.

Introduction

Le concept de module morphique a été introduit en 1976 par Gertrude Ehrlich :
Un module sur un anneau est dit morphique si pour toute paire de sous modules N_1, N_2 tels que $M/N_1 \cong N_2$ l'on ait $M/N_2 \cong N_1$, on de manière équivalente si $\varphi \in End(M)$ alors $\ker \varphi \cong coker\varphi$.

Après l'étude des modules et anneaux morphiques, l'extension du concept aux groupes a été proposé :
Si $\varphi \in End(G)$ est tel que $Im\varphi \triangleleft G$ alors $\ker \varphi \cong \dfrac{G}{Im(\varphi)}$.

Dans ce document, nous proposons les notions de base pour l'étude de groupes :
d'abord le sous-groupe, le groupe quotient, et le groupe produit ; ensuite les groupes cycliques, l'action de groupes et la formule des classes ; enfin les p-sous-groupes et les groupes nilpotents.

Cela sera suffisant pour aborder les groupes morphiques et le transfert de la propriété vers le sous-groupe, le groupe quotient et le groupe produit.
L'importance des groupes nilpotents et leurs propriétés et relation avec les p-groupes nous entrainent vers l'étude des p-groupes morphiques.

Chapitre 1

Généralités sur les groupes

Ce chapitre contient l'essentiel du cours du premier semestre M1 sans démonstrations, et a pour but de faciliter la lecture des chapitres suivants.

1.1 Définitions de base

1.1.1 Groupes

Définition 1.1.1 *Un groupe est un ensemble G non vide, muni d'une loi de composition interne telle que :*

i) La loi de composition est associative :
$\forall\ x,y,z \in G$: $(xy)z = x(yz)$.

ii) La loi possède un élément neutre noté e :
$\exists\ e \in G : \forall\ x \in G,\ ex=xe=x$.

iii) Tout élément x de G possède un symétrique (ou inverse) x' :
$\forall x \in G\ \exists x' \in G : xx' = x'x = e$

1.1.2 Sous-groupes

Définition 1.1.2 *Soit G un groupe et $H \subset G$, H est un sous groupe de G si :*

- *H contient l'élément neutre de G : $e \in H$.*

- *H est stable par la loi de composition de G : $x,y \in H \Longrightarrow xy \in H$.*

- *H est stable par inverse : $x \in H \Longrightarrow x^{-1} \in H$.*

Remarque

Soit G un groupe. Une partie H de G est un sous-groupe de G si :

1- H non vide

2- $x,y \in H \Longrightarrow xy^{-1} \in H$

1.1.3 Homomorphismes de groupes

Définition 1.1.3 *Soit G et G' deux groupes, un homomorphisme de groupes (ou simplement homomorphisme) de G dans G' est une application $f : G \to G'$ vérifiant :*

$$\forall\ x,y \in G : f(xy)=f(x)f(y)$$

1) On vérifie alors que :

- *$f(e)=e'$ (e et e' sont les éléments neutres de G et G')*
- *$f(x^{-1})=(f(x))^{-1}$*

2) Soit $f : G \longrightarrow G'$ un homomorphisme de groupes si f est bijective, on dit que f est un isomorphisme de G dans G', dans ce cas G et G' sont dits isomorphes et l'on note $G \cong G'$

3) Un homomorphisme de G dans G est appelé endomorphisme de G

4) Un isomorphisme de G dans G est appelé un automrphisme de G

1.2 Sous-groupes distingués, Groupes quotients

1.2.1 Relation d'équivalence

Définition 1.2.1 *Une relation d'équivalence R_g est dite compatible à gauche avec la loi interne de G, si :*

$$x \equiv y \ (R_g) \Rightarrow \alpha x \equiv \alpha y \ (R_g) \ \forall \ \alpha \in G$$

i) Si R_g existe alors elle est de la forme $x \equiv y \ (R_g) \Leftrightarrow x^{-1}y \in \overline{e}$, ($\overline{e}$ étant la classe de l'élément neutre de G).

ii) $\overline{e}$ est un sous goupe de G.

iii) Reciproquement, H étant un sous groupe de G, la relation définie par :
$x \ \Re \ y \Longleftrightarrow x^{-1}y \in H$ est une relation d'équivalence compatible à gauche avec la loi de groupe.

En résumé Une relation d'équivalence compatible à gauche avec la loi de groupe, est de la forme $x^{-1}y \in H$, H étant un sous groupe quelconque de G.
On peut introduire de même, les relations d'équivalence compatibles à droite et montrer qu'elles sont de la forme $xy^{-1} \in H$, H sous groupe de G.

1.2.2 Classes selon un sous-groupe

R_g (respectivement R_d) étant une relation d'équivalence compatible à gauche (respectivement à droite), H le sous groupe qui la caractérise, $\overline{x_g}$ (respectivement $\overline{x_d}$) la classe d'un élément x modulo R_g (respectivement R_d) alors :

- $\overline{x_g} = \{ \ xy : y \in H \ \} = xH.$
- $\overline{x_d} = \{ \ yx : y \in H \ \} = Hx$
- xH et Hx seront dites classe à gauche et classe à droite modulo H.

- Les classes $\overline{e_g}$ et $\overline{e_d}$ de l'élément neutre e de G sont égales à H
- L'application de H dans xH définie par $z \longmapsto xz$ est une bijection.
- Si $xH \cap yH$ n'est pas vide alors $xH = yH$.
  Ce qui nous permet de déduire :
- Dans un groupe fini, l'ordre (nombre d'éléments) d'un sous groupe quelconque est un diviseur de l'ordre du groupe.
- L'ensemble quotient mod R_g est noté G/R_g ou $(G/H)_g$; ses éléments sont les classes à gauche.
  $(G/H)_g = \{xH, x \in H\}$; de même $(G/H)_d = \{Hx, x \in H\}$.

1.2.3 Cas d'un groupe commutatif

H sous-groupe de G étant donné, $R_g = R_d = \Re$.
Il est alors possible de munir l'ensemble quotient $\dfrac{G}{\Re}$ (noté aussi $\dfrac{G}{H}$) d'une loi :

$$\bar{x} + \bar{y} = \overline{x + y}.$$

Soit f l'application de G dans $\dfrac{G}{H}$ définie par $f(x) = \bar{x}, \forall x \in G$.
f est un homomorphisme surjectif et ainsi $\dfrac{G}{H}$ est un groupe. Il est dit groupe quotient de G par H

1.2.4 Cas d'un groupe non commutatif

Dans ce cas R_g et R_d engendrées par la donnée d'un sous-groupe H sont généralement distinctes. On se propose de choisir convenablement H de sorte qu'elles soient équivalentes (on entend par là, que les classes à gauche et à droite de tout élément x coincident)

- On a alors :
  $\forall x \in G : xH = Hx$; $H = xHx^{-1} = x^{-1}Hx$.
  Un tel sous-groupe est dit distingué dans G et on note dans ce cas $H \triangleleft G$.

- De tels sous-groupes existent toujours.
  ($\{e\}$ et G par exemple).

- Il est alors possible de munir $(G/H)_g = (G/H)_d = G/H$ d'une loi :

$$\bar{x}.\bar{y} = \overline{xy}.$$

  qui en fasse un groupe, G/H est dit groupe quotient de G par H.

- Soit G un groupe et H un sous-groupe de G. les deux propositions suivantes sont équivalentes :

  i) H est un sous-groupe distingué dans G

  ii) Il existe un groupe G' et un homomorphisme $f : G \longrightarrow G'$ tel que $H = \ker(f)$ $= \{x \in G / f(x) = e'\}$.

1.3 Groupes cycliques

Définition 1.3.1 *Soit G un groupe, $a \in G$ et $m \in \mathbb{Z}$.*
Si $m > 0$ on note a^m l'élément $(a.a.a...)$, m fois.
Si $m < 0$ on note a^m l'élément $(a^{-1}.a^{-1}.a^{-1}...)$, $-m$ fois.
Si $m = 0$: $a^0 = e$ (l'élément neutre de G).
Ainsi se trouvent définis tous les éléments a^n, $n \in \mathbb{Z}$, comme on peut vérifier les règles de calcul usuelles telles que : $a^{n+m}=a^n.a^m$ et $(a^n)^m = a^{nm}$, pour tous les éléments m, n de $\mathbb{Z}$.
On dit qu'un groupe G est cyclique (ou monogène) s'il existe un élément $a \in G$ tel que $G = \{ a^m, m \in \mathbb{Z} \}$; a est dit générateur du groupe cyclique G.
Soit G un groupe ; l'ordre d'un élément a de G est le plus petit entier positif n tel que $a^n = e$

Proposition 1.3.2 *si G est un groupe cyclique, alors :*
ou bien G est isomorphe au groupe additif $\mathbb{Z}$ ou bien G est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Définition 1.3.3 *Un groupe G est dit homocyclique s'il est le produit direct de groupes cycliques isomorphes.*

1.4 Produit de groupes

Définition 1.4.1 *Soit $(A_i)_{i\in I}$ une famille d'ensembles, chacun d'eux étant muni d'une loi de composition.*
On appelle loi produit des lois des A_i, la loi sur $\prod A_i$ $(i \in I)$ telle que :
$(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i b_i)_{i\in I}$

Proposition 1.4.2 *Si les $(A_i)_{i\in I}$ sont des groupes, alors $\prod A_i$ $(i \in I)$ l'est aussi.*
De plus, pour tout i, la projection d'indice i $p_i : \prod A_i \longrightarrow A_i$ est une homomorphisme de groupes.

Proposition 1.4.3 *Soit $(G_i)_{i\in I}$ une famille de groupes et pour tout i, $p_i : \prod G_i \longrightarrow G_i$ la projection d'indice i. Alors pour tout groupe H, et toute famille $(g_i)_{i\in I}$ d'homomorphismes de groupes ($g_i : H \longrightarrow G_i$), il existe un unique homomorphisme $h : H \longrightarrow \prod G_i$ tel que $g_i = p_i \circ h$, $\forall\, i \in I$.*

Proposition 1.4.4 *Soit G un groupe, H et K deux sous groupes de G tels que : $G = HK$, $H \cap K = \{e\}$, $\forall\, x \in H$, $\forall\, y \in K : xy = yx$, alors l'application $(x, y) \longmapsto xy$ est un isomorphisme de $H \times K$ dans G*

Proposition 1.4.5 *Soit G un groupe, $H_1, H_2, H_3, ..., H_n$, une suite finie de sous groupes de G tel que :*

i) $G = H_1H_2...H_n$

ii) $\forall\, i \in [1, n] : H_i \cap (H_1...H_{i-1}.H_{i+1}...H_n) = \{e\}$

iii) $\forall\, (i, j) \in [1, n] \times [1, n], i \neq j : \forall\, x \in H_i, \forall\, y \in H_j : xy = yx.$

Alors l'application $(x_1, ..., x_n) \longmapsto x_1...x_n$ *est un isomorphisme de* $H_1 \times H_2 \times ... \times H_n$ *dans* G.

Preuve. Par récurrence sur n :

■

1.5 Normalisateur

Définition 1.5.1 *Soit* G *un groupe et* S *une partie de* G. *On appelle normalisateur de* S *l'ensemble* $G_S = \{x \in G : xSx^{-1} = S\}$.

Proposition 1.5.2 *Soit* G *un groupe,* S *une partie de* G ; *l'ensemble* G_S *est un sous groupe de* G.

Proposition 1.5.3 *Soit* H *et* K *deux sous groupes de* G *tels que* $K \subset G_H$ *alors :*

- $KH = HK$
- KH *est un sous groupe de* G
- H *est distingué dans* KH $(H \triangleleft KH)$

Remarque 1.5.4 $(\forall t \in KH,\ tHt^{-1} \subset H) \Rightarrow (\forall t^{-1} \in KH,\ H \subset t^{-1}Ht)$, t, t^{-1} *étant arbitraire dans* KH *on en déduit que :* $(\forall t \in KH,\ tHt^{-1} \subset H) \Leftrightarrow (\forall t \in KH, tHt^{-1} = H)$

Proposition 1.5.5 *Soit* G *un groupe,* H *et* K *deux sous-groupes de* G *tels que* $K \subset G_H$, *alors :*

i) $K \cap H$ *est distingué dans* K

ii) $\dfrac{K}{k \cap H} \simeq \dfrac{KH}{H}$

1.6 Opération d'un groupe sur un ensemble

Définition 1.6.1 *Soit G un groupe et S un ensemble. On appelle opération de G sur S toute application de $G \times S$ dans S : $(x, s) \longmapsto x.s$ vérifiant :*

- $x.(y.s) = (xy).s \ \forall x, y \in G ; \forall s \in S$.
- $e.s = s \ \forall s \in S$.

On dit aussi que S est un G-ensemble.

Proposition 1.6.2 *Si G opère sur S, on a :*

i) $\forall x \in G$, $T_x : S \longrightarrow S \ / \ T_x(s) = x.s$ *est un permutation de S.*

ii) l'application $x \mapsto T_x$ est un homomorphisme de groupe de G dans le groupe $P(S)$ des permutations de S.

Réciproquement, si $f : G \longrightarrow P(S)$ est un homomorphisme de groupe,
$(x, s) \longmapsto x.s = f(x)(s)$ définit une opération de G sur S.

Exemples :

1) Opération naturelle de $P(S)$ sur S : si $x \in P(S)$ et $s \in S$, $x.s = x(s)$..

2) Opération par automorphisme intérieur ou par conjugaison : si G est un groupe, $(x, s) \longmapsto x.s = xsx^{-1}$ est une opération de G sur G.

   Remarques : Si G est un groupe, l'application $h_x : G \longrightarrow G$ définie par :
   $h_x(y) = xyx^{-1}$ est un isomorphisme de G dans G dit automorphisme intérieur de G.

3) Opération d'un groupe G sur l'ensemble S des parties de G :

$$(x, A) \longmapsto Ax^{-1}.$$

4) Si G opère sur T, alors G opère sur $\mathscr{P}(T)$:

$$(x, A) \longmapsto x.A = \{x.y/y \in A\}$$

5) Opération par conjugaison d'un groupe G sur l'ensemble des sous-groupes de G :

$$(x, H) \longmapsto xHx^{-1}$$

Remarque :

Deux parties A et B de G sont conjuguées, s'il existe x dans G tel que $xAx^{-1} = B$.

6) Opération par translation à gauche de G sur G :

$(x, y) \longmapsto x.y = xy$ (produit d'éléments de G).

7) Soit G un groupe, $(x, y) \mapsto yx^{-1}$ est une opération de G sur G.

Définition 1.6.3 *Soit S un G-ensemble, alors :*

Si $x \in G$, $s \in S$ et $(x.s) = s$, on dit que s est invariant de x (ou que s est fixe par x).

Si $\forall x \in G$ $x.s = s$ alors s est dit invariant de G.

Exemple :

Soit E l'ensemble des sous-groupes de G. G opère par conjugaison sur E.

$H \in E$ est distingué dans G, si c'est un invariant pour cette opération.

Proposition 1.6.4 *Si G opère sur S, et $s \in S$; l'ensemble G_s formé des éléments x de G tel que $x.s = s$ est appelé groupe d'isotropie de s ou stabilisateur de s ou fixateur de s.*

Exemple : Si H est un sous-groupe de G :

G_H = Normalisateur de $H = \{x \in G/\ x.H = H\} = \{x \in G/xHx^{-1} = H\}$. Nous avons bien entendu considéré l'opération par conjugaison d'un groupe sur l'ensemble des sous-groupes.

Définition 1.6.5 *Si G opère sur S et $s \in S$, on appelle orbite de s ou trajectoire de s l'ensemble $Gs = \{x.s; x \in G\}$.*
un ensemble K est appelé orbite si c'est l'orbite de l'un de ses éléments.
On dit que G opère transitivement sur S, si S est une orbite. Dans ce cas, on dit que S est un G-ensemble homogène.

Exemple :

1) G opère transitivement sur G par translation.

   $G = \{x.s, x \in G\} = Gs$ pour un s quelconque.

2) Si H est un sous-groupe de G, G opère transitivement par translation à gauche sur $(\frac{G}{H})_g$. $(\frac{G}{H})_g = \{xyH, x \in G\}$ pour yH quelconque.

3) G n'opère pas transitivement sur G par conjugaison sauf si $G = \{e\}$.

   remarque :

   $\{e\}$ est une orbite et e n'appartient à aucune autre orbite.

4) Si G opère sur S et si $s \in S$, alors G opère transitivement sur l'orbite Gs comme suit :

   $G \times Gs \longrightarrow Gs$

   $(x, y.s) \longmapsto xy.s$

Définition 1.6.6 *Si S et T sont deux G-ensembles, on appelle homomorphisme de G-ensembles de S dans T, une application $f : S \longrightarrow T$ telle que :*
$f(x.s) = x.f(s); \forall x \in G, \forall s \in S$.
Si f est bijective, f est dite isomorphisme de G-ensembles.

Proposition 1.6.7 *Soit S un G-ensemble homogène, $s \in S$ et G_s le groupe d'isotrope de s, alors $(\frac{G}{G_s})_g$ est un G-ensemble homogène (lorsque G opère par translation à gauche) et $\frac{G}{G_s}$ et S sont des G-ensembles isomorhes.*

Preuve. Soit $f : (\frac{G}{G_s})_g \longrightarrow S$ définie par $f(xG_s) = x.s$

1) f est bien définie.

2) f est un homomorphisme de G-ensembles.

3) f est injective.

4) f est surjective.

■

Proposition 1.6.8 *Si G opère sur S, S est la réunion disjointe de ses orbites.*

Remarque 1.6.9 *On dit qu'une famille $(x_i)_{i\in I}$ d'éléments de S est une famille d'éléments représentatifs des orbites de S, si pour chaque orbite K, il existe $i \in I$ unique tel que $x_i \in K$.*
On dit qu'une partie H de S est un ensemble d'éléments représentatifs des orbites, si pour chaque orbite K, on a : card$(H \cap K) = 1$.
La proposition précédente s'écrit :
$S = \cup Gx_i(i \in I)$ *Union disjointe*
$(x_i)_{i\in I}$ *famille d'éléments représentatifs des orbites.*

Corollaire 1.6.10 *1) Card(S) $= \sum(G : G_{x_i})$. $(x_i)_{i\in I}$ famille d'éléments représentatifs des orbites.*
En effet, si G opère sur S, alors G opère transitivement sur toute orbite Gx_i,et Gx_i et $(\frac{G}{Gx_i})_g$ sont des G-ensembles isomorphes. Le résultat s'en suit.

2 Cas de l'opération par conjugaison de G sur S (Formule des classes).
CardG $= \sum(G : G_x)$
H ensemble d'éléments représentatifs des orbites.
l'orbite $Gx = \{yxy^{-1}, y \in G$ est appelée classe de conjugaison de x.

Remarque 1.6.11 *La classe de conjugaison de x a un seul élément, si et seulement si x est un élément de centre de G.*

La formule des classes peut donc s'écrire :

$$(G:1) = (Z:1) + \sum (G:G_x)/x \in D.$$

D ensemble d'éléments représentatifs des orbites de cardinal supérieur à 1.

1.7 Théorèmes de sylow et p-groupes

1.7.1 théorème de sylow

Définition 1.7.1 *Un groupe fini G est appelé un p-groupe (avec p nombre premier) si $(G:1)$ est une puissance de p.*
Si H est un groupe et K un sous-groupe de H et si K est un p-groupe, on dit que K est un p-sous-groupe.
On dit que K est un p-groupe de sylow de H si :

1) $(H:1) = p^n m$ *avec p ne divise pas m.*

2) $(K:1) = p^n$.

Proposition 1.7.2 ***(Théorème de burnside).***
Le centre d'un p-groupe non trivial n'est jamais trivial.

Proposition 1.7.3 ***(Petits p-groupes).***
Tout p-groupe d'ordre p ou p^2 est abélien.

Théorème 1.7.4 *Si G est un groupe fini d'ordre $p^n m$ (p premier), p ne divise pas m, alors :*

i) *Tout p-groupe de G est inclus dans un p-sous-groupe de sylow de G.*

ii) *Deux p-sous-groupes de sylow sont toujours conjugués.*

iii) *Si s est le nombre de p-sous-groupes de sylow de G, on a :*
$s \equiv 1 \ (p)$ *et* $s \mid (G:1)$.

1.7.2 Sous-groupes distingués dans les p-groupes

Proposition 1.7.5 ***(Réciproque du théorème de Lagrange pour les p-groupes).***
Soit G un groupe d'ordre p^α. Pour tout $\beta \leq \alpha$, G contient un sous-groupe distingué d'ordre p^β.

Définition 1.7.6 ***(Sous groupe maximal).***
Un sous-groupe M de G est dit maximal si c'est un sous-groupe propre, tel que M et G soient les seuls sous groupes de G contenant M.

Proposition 1.7.7 ***(Sous-groupes maximaux d'un p-groupe).***
Tout sous-groupe maximal d'un p-groupe d'ordre p^α est d'ordre $p^{\alpha-1}$ et est distingué.

1.8 Groupes nilpotents

Définition 1.8.1 ***(Groupes nilpotents).***
Rappelons que pour deux sous-groupes H et K de G, on note $[H, K]$ la clôture normale dans G de l'ensemble des éléments $hkh^{-1}k^{-1}$ où $h \in H$ et $k \in K$.
La suite centrale descendante $(C_n(G))_{n\in\mathbb{N}}$ d'un groupe G est définie ainsi : $C_0(G) = G$ et pour tout $n \geq 1$, $C_n(G) = [G, C_{n-1}(G)]$.
Un groupe G est dit nilpotent s'il existe un entier m tel que $C_m(G) = \{1_G\}$.
Le plus petit indice m satisfaisant cette condition est appelé l'indice de nilpotence de G.

Proposition 1.8.2 *Les p-groupes sont nilpotents.*

Corollaire 1.8.3 *Tout produit direct de p-groupes est nilpotent.*

Théorème 1.8.4 ***(Structure des groupes nilpotents).***
Un groupe nilpotent est produit direct de ses p-sylow.

1.9 Théorème de Frattini

Définition 1.9.1 ***(Eléments mous d'un groupe).***
Un élément d'un groupe est dit mou si pour toute partie $S \subset G$ telle que S et cet élément engendrent le groupe, S engendre le groupe.

Exemples :

L'élément neutre est toujours un élément mou. Par exemple $\mathbb{Z}$ ne contient aucun élément mou autre que 0. Puisque pour tout $m \in \mathbb{Z}$, on peut choisir n premier à m et différent de ± 1. Alors m et n engendrent $\mathbb{Z}$, mais m tout seul n'engendre pas $\mathbb{Z}$.

Proposition 1.9.2 ***:***

(i) L'ensemble Φ des éléments mous d'un groupe est un sous-groupe.

(ii) Φ est même un sous-groupe caractéristique.

(iii) Φ est l'intersection de tout les sous-groupes maximaux.

Définition 1.9.3 ***(Sous-groupe de Frattini).***
Le sous-groupe de tous les éléments mous d'un groupe G est apellé le sous groupe de Frattini et est noté $\Phi(G)$.

Théorème 1.9.4 ***(Théorème de Frattini).***
Le quotient d'un p-groupe par le sous-groupe de Frattini est un $\mathbb{F}_p$-espace vectoriel.

1.10 Quelques groupes classiques

1.10.1 Le groupe diédral

Proposition 1.10.1 *Soit $n \geq 1$, alors il existe un et un seul groupe, à isomorphisme près, engendré par deux éléments τ, σ avec $\tau \neq \sigma$, $o(\tau) = n$, $o(\sigma) = 2$ et $\sigma\tau\sigma^{-1} = \tau^{-1}$.*

Ce groupe est réalisé par le sous-groupe suivant de $O_2(\mathbb{R})$.

Soit $M := \left\{ \begin{bmatrix} cos2\pi\frac{k}{n} & -sin2\pi\frac{k}{n} \\ sin2\pi\frac{k}{n} & cos2\pi\frac{k}{n} \end{bmatrix} \begin{bmatrix} cos2\pi\frac{k}{n} & sin2\pi\frac{k}{n} \\ sin2\pi\frac{k}{n} & -cos2\pi\frac{k}{n} \end{bmatrix} 0 \leq k < n \right\}$.

Soient

$$t := \left[\begin{array}{cc} cos2\pi\frac{k}{n} & -sin2\pi\frac{k}{n} \\ sin2\pi\frac{k}{n} & cos2\pi\frac{k}{n} \end{array} \right]$$

$$s := \left[\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right]$$

alors $o(t) = n$, $o(s) = 2$, $sts^{-1} = t^{-1}$.

Un tel groupe s'appelle le groupe diédral d'ordre $2n$ *et se note* D_n.

2. *Les groupes* D_1 *et* D_2 *sont abéliens. Si* $n \geq 3$ *est impair, on a centre* $D_n = \{I_2\}$ *; si* $n = 2m \geq 4$ *est pair on a centre* $D_n = \{I_2, \tau\}$ *où* $\tau = t^m$.

3. *Soit* G *un groupe fini non commutatif engendré par* a, b, *avec* $o(a) = o(b) = 2$, *soit* $n = o(ab)$, *alors on a* $o(G) = 2n$, $n \geq 3$ *et* G *est isomorphe à* D_n.

3. *Soit* $K = \kappa_2$ *le sous-groupe cyclique d'ordre* 2 *de* D_n *engendré par* s, $H = \kappa_n$ *le sous-groupe cyclique d'ordre* n *de* D_n *engendré par* t, *alors* D_n *est produit semi-direct de* K *par* H

1.10.2 Le groupe quaternionnien d'ordre 8

Soit les matrices de $Gl_2(\mathbb{C})$,

$$A = \left[\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right]$$

$$B = \left[\begin{array}{cc} i & 0 \\ 0 & -i \end{array} \right]$$

alors :

$\mathbb{H}_8 := \{\pm I_2, \pm A, \pm B, \pm AB\}$ est un sous-groupe de $Gl_2(\mathbb{C})$ d'ordre 8.

On a $A^2 = B^2 = (AB)^2 = -I_2$, $AB = -BA =$

$$\left[\begin{array}{cc} 0 & -i \\ i & 0 \end{array} \right]$$

Le centre de $\mathbb{H}_8$ est $\{\pm I_2\}$, $\mathbb{H}_8$ n'est pas commutatif et tout élément de $\mathbb{H}_8 -$ centre$\mathbb{H}_8$ est d'ordre 4.

Le groupe $\mathbb{H}_8$ s'appelle le groupe quaternionien d'ordre 8.

Proposition 1.10.2 *Soit G un groupe non commutatif d'ordre 8. Alors G est isomorphe au groupe diédral D_4 ou au groupe quaternionien $\mathbb{H}_8$. Ces deux groupes ne sont pas isomorphes.*

Chapitre 2

Groupes Morphiques

Le deuxième chapitre est consacré d'abord aux définitions des morphismes morphiques et des groupes morphiques. Ensuite à l'étude de certains classes de groupes morphiques.

2.1 Endomorphismes morphiques

Définition 2.1.1 *Soit* $\alpha \in End(G)$.
On dit que α *est normal si* $G\alpha \lhd G$.
On dit que α *est morphique si et seulement si* α *est normal et* $\dfrac{G}{G\alpha} \cong ker(\alpha)$.

Proposition 2.1.2 *Soit* G *un groupe et* $\alpha \in end(G)$ *; les assertions suivantes sont équivalentes :*

1) α *est morphique.*

2) $\exists \beta \in end(G)$ *avec* $ker(\alpha) = G\beta$ *et* $G\alpha = ker(\beta)$.

3) $\exists \beta \in end(G)$ *avec* $ker(\alpha) \cong G\beta$ *et* $G\alpha = ker(\beta)$.

Preuve. 1) $\longrightarrow$ 2) si $\sigma : \dfrac{G}{G\alpha} \longrightarrow ker(\alpha)$ est un isomorphisme, définissons $\beta : G \longrightarrow G$ par $\beta(g) = \sigma(gG\alpha)$, alors $\beta \in end(G)$, $G\beta = \sigma(\dfrac{G}{G\alpha}) = ker(\alpha), ker(\beta) = G\alpha$ car σ et injectif

2) $\longrightarrow$ 3) évident.

3) $\longrightarrow$ 1) β étant donnée comme dans 3), alors $G\alpha = ker(\beta) \triangleleft G$ et $\dfrac{G}{G\alpha} = \dfrac{G}{ker(\beta)} \cong G\beta \cong ker(\alpha)$. ■

Proposition 2.1.3 *:*

- *Tout automorphisme de G est morphique.*

- *L'endomorphisme trivial θ défini par $g\theta = 1$ $\forall g \in G$ est morphique.*

- *Soit $G = H \times K$ et la projection $\sigma \in End(G)$ définie par $(h,k)\sigma = (h,1)$, alors σ est morphique car $G\sigma = H \times 1 \triangleleft G$ et $\dfrac{G}{G\sigma} \cong 1 \times K = ker(\sigma)$.*

- *Considérons les groupes $C_2 =< a >$, $C_4 =< b >$ et $G = C_2 \times C_4$.*
  Soit $\sigma : C_2 \longrightarrow C_4$ définie par $\sigma(a^k) = b^{2k}$, et définissons α et β dans $end(G)$ par $\alpha(x,y) = (1, \sigma(x))$ et $\beta(x,y) = (1,y)$.
  On a : $G\beta = 1 \times C_4 = ker(\alpha)$ et $ker(\beta) = C_2 \times 1 \cong 1 \times (C_2)\sigma = G\alpha$.
  α n'est pas morphique car $\dfrac{G}{G\alpha} \cong C_2 \times C_2$ tandis que $ker(\alpha) \cong C_4$.
  Maintenant on définit $\theta : C_4 \longrightarrow C_2$ par $\theta(b^k) = a^k$. Puis nous définissons $\pi : G \longrightarrow G$ et $\gamma : G \longrightarrow G$ par $\pi(x,y) = (x,1)$ et $\gamma(x,y) = (\theta(y), \sigma(x))$, alors $\dfrac{G}{G\pi} \cong C_4 \cong \ker(\pi)$ et $\dfrac{G}{G\gamma} \cong C_2 \cong \ker(\gamma)$ donc π et γ sont morphiques, mais $\pi\gamma = \alpha$ n'est pas morphique.

- *Le composition d'endomorphismes morphiques n'est pas nécessairement un endomorphisme morphique. (voir ce qui précède)*

- *Si $\alpha \in End(G)$ est morphique alors α est injectif si et seulement si α est surjectif.*
  Puissque $\dfrac{G}{G\alpha} \cong ker(\alpha)$ alors évidemment $ker(\alpha) = 1$ si et seulement si $G\alpha = G$.

- *Si $\alpha \in End(G)$ est morphique, alors pour tout automorphisme σ de G $\sigma\alpha$ et $\alpha\sigma$ le sont aussi.*

2.2 Groupes morphiques

Définition 2.2.1 *Un groupe G est dit morphique si pour tout couple N_1, N_2 de sous groupes distingués de G, les deux conditions $\dfrac{G}{N_2} \cong N_1$ et $\dfrac{G}{N_1} \cong N_2$ sont équivalentes.*

Proposition 2.2.2 *Soit G un groupe.*
Les assertions suivantes sont équivalentes :

1- G est morphique.

2- Tout endomorphisme normal de G est morphique.

3- Si $K \lhd G$ est tel que $\dfrac{G}{K} \cong N \lhd G$, alors $\dfrac{G}{N} \cong K$.

4- Si $K \lhd G$, $K \neq 1$, est tel que $\dfrac{G}{K} \cong N \lhd G$ alors $\dfrac{G}{N} \cong K$.

Exemples :

- C_n est morphique pour tout $n \geq 1$ mais le groupe cyclique infini C_∞ n'est pas morphique.
  En effet, pour tout endomorphisme normal α de C_n on a $\dfrac{C_n}{\ker(\alpha)} \cong (C_n)\alpha$, et le groupe $\dfrac{C_n}{(C_n)\alpha}$ et $\ker(\alpha)$ sont cycliques de même ordre, donc isomorphes.
  $C_\infty =< a >$ n'est pas morphique par (2.1.3) car l'endomorphisme $a^k \longrightarrow a^{2k}$ est injectif mais non surjectif.

- $C_2 \times C_4$ n'est pas morphique puisque l'endomorphisme α défini dans (2.1.3) est normal mais n'est pas morphique.

- Soit G un groupe morphique et $K \lhd G$ alors :

  1- Si $K \cong G$ alors $K = G$.

  2- Si $\dfrac{G}{K} \cong G$ alors $K = 1$.

En effet si $K \cong G$ alors $\dfrac{G}{1} \cong K$ donc $\dfrac{G}{K} \cong 1$ et $G = K$.
Si $\dfrac{G}{K} \cong G$ alors $\dfrac{G}{G} \cong K$ donc $K = 1$.

- Tout groupe simple est morphique.

2.3 Groupes uni-série morphiques

Définition 2.3.1 *On dit que G est un groupe uni-série si son réseau de sous groupes distingués est de la forme $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_n = 1$.*
Définissons alors la hauteur uni-série de ses sous groupes distingués par $1_G(G_k) = n - k$. $0 \leq k \leq n$.
Les propriétés suivantes sont alors vérifiées :

1) Si G est uni-série, $K \triangleleft G$ et $H \triangleleft G$ alors $1_G(K) = 1_G(H)$ si est seulement si $H = K$.

2) Si G est uni-série et $K \triangleleft G$ ($K = G_k$ par exemple) alors G/K est uni-série avec $G_0/K \supset G_1/K \supset ... \supset G_k/K = 1$ pour réseau normal, et donc $1_{G/K}(G/K) = k$ et $1_G(K) + 1_{G/K}(G/K) = n$

3) Un sous groupe normal de G peut ne pas être uni-série (considérer $A_4 \supset K_4 \supset 1$ avec $K_4 \cong C_2 \times C_2$).

Proposition 2.3.2 *Soit G un groupe uni-série avec réseau de sous groupes distingués $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_n = 1$, alors :*

1- Si $H \triangleleft G$ est aussi uni-série alors $1_G(H) = 1_H(H)$

2- En particulier si $G_i \cong G/G_k$ alors $i = n - k$.

Preuve. Si $H \triangleleft G$ est aussi uni-série alors $1_G(H) = 1_H(H)$.
Nous montrons d'abord le résultat suivant : si $K \triangleleft H$ alors $K \triangleleft G$.
Soit $H = H_0 \supset H_1 \supset ... \supset H_m = 1$ le réseau de sous groupes normaux de H, tel que $K = H_k$ pour un certain k, soit $g \in G$ et $h \in H$; puisque $H \triangleleft G$, alors $gh = h'g$ pour un

certain $h' \in H$, et $K^g = g^{-1}Kg$, on a $(K^g)^h = K^{h'g} = (K^{h'})^g = K^g$.
Puisque $K \lhd H$, donc $K^g \lhd H$ pour tout $g \in G$, donc $H = H^g \supset H_1^g \supset ... \supset H_m^g = 1$ est aussi une chaine de sous groupes normaux de H. Puisque H est uni-série, il s'ensuit que $H_i^g = H_i$ pour tout i, donc $H_i \lhd G$ pour tout i car $g \in G$ est arbitraire.
En particulier, $K \lhd G$ comme préconisé.
Maintenant supposons que $H = G_k$, alors la chaine $H = G_k \supset G_{k+1} \supset ... \supset G_n = 1$ se compose de sous-groupes normaux de H, et il s'en suit que

$$H = G_k \supset G_{k+1} \supset ... \supset G_n = 1$$

et

$$H = H_0 \supset H_1 \supset ... \supset H_m = 1$$

représentent le réseau de sous-groupes normaux de H, donc $m = n-k$ et $H_i = G_{k+i}$ pour tout $i = 0, 1, ..., n-k$.
En particulier $1_G(H) = n - k = m = 1_H(H)$.
Si $G_i \cong \dfrac{G}{G_k}$ alors $i = n - k$; en effet :
si $G_i \cong \dfrac{G}{G_k}$ alors G_i est uni-série ; nous obtenons donc $k = 1(G/G_k) = 1_G(G_i) = n - i$ donc $i = n - k$.

■

On peut maintenant caractériser les groupes uni-série morphiques.

Théorème 2.3.3 *Soit G un groupe uni-série, et soit $G = G_0 \supset G_1 \supset ... \supset G_n = 1$ son réseau des sous groupes normaux.*
Les assertions suivantes sont équivalentes :

1- G est morphique.

2- Si $\dfrac{G}{G_k} \cong G_{n-k}$ $k = 1, 2, ..., n,$ alors $\dfrac{G}{G_{n-k}} \cong G_k$.

Preuve.
(1) $\Rightarrow$ (2), supposons que $\dfrac{G}{G_k} \cong G_{n-k}$, puisque $G_{n-k} \lhd G$, on a $\dfrac{G}{G_{n-k}} \cong G_k$ par (1).
(2) $\Rightarrow$ (1), soit $\alpha \in end(G)$ normal, on écrit $ker(\alpha) = G_k$ et $Im(\alpha) = G_i$.

Donc $G_i \cong G/G_k$, alors $i = n - k$ par (2.3.2) d'où $G_k \cong G/G_i$ par (2), ce qui prouve que α est morphique. ■

Corollaire 2.3.4 *Si G possède un réseau normal $G \supset S \supset 1$ alors G est morphique.*
En effet pour $G_0 = G$ et $G_1 = S$, $G_2 = 1$, supposons que $G/G_k \cong G_{2-k}$, si $k = 0, 2$ alors $G/G_{2-k} \cong G_k$ est clair, si $k = 1$ alors $G/S \cong S$ donc $G/G_{2-k} = G/S \cong S = G_k$.

Exemple :

Le groupe diédral D_3 est morphique.

Preuve. :

Le réseau normal de D_3 est $D_3 \supset A \supset 1$ où A est le sous groupe normal d'indice 2. ■

Proposition 2.3.5 *Le groupe symétrique S_n est morphique pour tout $n \geq 1$.*

Preuve. $S_1 = 1$ est morphique, $S_2 \cong C_2$ est morphique, $S_3 \cong D_3$ est morphique, et S_n est morphique pour $n \geq 5$ par le corollaire précédent car son réseau normal est $S_n \supset A_n \supset 1$. Finalement si $S_4 \supset A_4 \supset K_4 \supset 1$ désigne le réseau des sous groupes normaux de S_4 alors S_4 est morphique par le théorème (2.3.3) car $S_4/A_4 \ncong K_4$ et $S_4/K_4 \ncong A_4$. ■

Théorème 2.3.6 *Un groupe abélien engendré par un nombre fini d'éléments est morphique si et seulement s'il est fini et toute composant p-primaire possède la forme $(C_{p^k})^n$ pour un certain $n \geq 0$ et $k \geq 0$.*

Ainsi les groupes abéliens $(C_{p^k})^n$ sont morphiques pour tout p premier et k entier $k \geq 0$. Notons que $C_4 \times C_4$ est morphique mais son sous groupe $C_2 \times C_4$ n'est pas morphique. Le groupe diédral $D_2 \cong C_2 \times C_2$ est morphique par le théorème 2.3.6, cependant pour les groupes diédral supérieurs, la situation est comme ce qui suit :

Proposition 2.3.7 *Si $n \in Z$, $n > 2$, le groupe diédral D_n est morphique si et seulement si n est impair.*

Preuve. Soit $G = D_n = \{1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1}\}$ ou $a^n = b^2 = 1$ et $aba = b$, on écrit $A =< a > \lhd G$.

Si $K \triangleleft G$ et n est impair, alors soit $K \subseteq A$ ou bien $K = G$.

Si $K \nsubseteq A$ il existe $x = ba^m \in K$, on vérifie que $a^2 = axa^{-1}x^{-1}$ alors $a^2 \in K$.

Puisque 2 et $n =\mid a \mid$ sont relativement premier, il s'en suit que $a \in K$, d'où $b \in K$, alors $K = G$.

Supposons d'abord que n est impair, et montrons que G est morphique, en montrons que tout endomorphisme est soit trivial ou bien un automorphisme.

Supposons par contre que $\alpha \neq \theta$ et $\alpha \notin aut(G)$, alors $ker(\alpha) \subseteq A$ et $G\alpha \subseteq A$, donc $\mid ker(\alpha) \mid$ et $\mid G\alpha \mid$ sont impairs, mais alors |G| $= \mid ker(\alpha) \mid = \mid G\alpha \mid$ est impair (Contradiction).

Si $n = 2m$, montrons que D_n n'est pas morphique.

Soit $N = \langle a^m \rangle$, alors N et A sont des sous groupes normaux de G, puisque $G/A \cong C_2 \cong N$ mais $G/N \cong D_m \ncong A$, il s'en suit que G n'est pas morphique par le proposition 2.2.2. ■

Proposition 2.3.8 *Aucun des groupes de quaternion Q_{4n} n'est morphique.*

Preuve. Notons $G = Q_{4n} = \langle a, b \,/ a^{2n} = 1, a^n = b^2, aba = b \rangle$, et soit $A = \langle a \rangle$ et $N = \langle a^n \rangle$; alors $A \triangleleft G$ et $N \triangleleft G$.

Nous avons $G/A \cong C_2 \cong N$ mais $G/N \ncong A$, en effet si $n = 2$ $G/N \cong C_2 \times C_2 \ncong A$ alors que si $n > 2$ alors $G/N = \langle aN, bN \rangle \cong D_n \ncong A$ car A est abélien. ■

2.4 Groupes Fortement Morphiques

Proposition 2.4.1 ***(Importante)***

Les assertions suivantes sont équivalentes pour un groupe morphique :

(1) Tout sous groupe normal de G est isomorphe à une image de G.

(2) Toute image de G est isomorphe à un sous groupe de G.

Preuve. (1) $\Rightarrow$ (2) : l'image $\dfrac{G}{K}$ de G étant donnée, soit $\dfrac{G}{N} \cong K$ par (1) pour $N \triangleleft G$. Comme G est morphique, $\dfrac{G}{K} \cong N$ par 2.2.2.

(2) $\Rightarrow$ (1) : Si $K \triangleleft G$ alors $\dfrac{G}{K} \cong N$ pour certain $N \triangleleft G$ par (2), $\dfrac{G}{N} \cong K$ par 2.2.2.

■

Définition 2.4.2 *Soit G un groupe, G est dit fortement morphique s'il est morphique et si les conditions de* (2.4.1) *sont vérifiées.*

Il est clair que tout groupe simple est fortement morphique.
D_3 est morphique mais n'est pas fortement morphique : si $A \triangleleft D_3$ est le sous groupe cyclique d'ordre 3 alors $D_3/A \cong C_2$, mais D_3 n'a pas de tel sous groupe normal.
De la même manière A_4 est morphique mais n'est pas fortement morphique.
Il est clair que le groupe cyclique fini C_n est aussi fortement morphique (si $K \triangleleft C_n$ alors C_n/K est cyclique et son ordre divise n).

Théorème 2.4.3 *Un groupe abélien fini est fortement morphique si et seulement s'il est morphique.*

Preuve. Si G est morphique, il suffit par 2.4.1 de montrer que toute image G/K s'injecte dans G. Par le théorème de décomposition primaire, on peut supposer que G est un p-groupe (p est premier), mais dans ce cas là le théorème est bien connu.
Voir par exemple B.Baumslag et B.Chandler (Theory and problems of groups theory, Schawms ouline series, Mcgraw-hill 1968). ∎

Théorème 2.4.4 *Soit G un groupe fortement morphique, si $K \triangleleft G$ et $K_1 \triangleleft G$ alors :*
$G/K \cong G/K_1$ si et seulement si $K \cong K_1$.

Preuve. Soit $G/K \cong G/K_1$.
Puisque G est fortement morphique, soit $G/K \cong N \cong G/K_1$ où $N \triangleleft G$, il s'en suit par 2.2.2 que $K \cong G/N \cong K_1$ car G est morphique.
Réciproquement, soit $K \cong K_1$.
Puisque G est fortement morphique, soit $G/K \cong N$ et $G/K_1 \cong N_1$ où N et N_1 sont normaux dans G, alors $G/N \cong K \cong K_1 \cong G/N_1$ par 2.2.2, alors $N \cong N_1$, d'où :
$G/K \cong G/K_1$. ∎

Théorème 2.4.5 *Soit G un groupe uni-série, et $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_n = 1$ son réseau de sous groupes normaux. Les assertions suivantes sont équivalentes :*

(1) G est fortement morphique.

(2) Tout sous groupe normal de G est isomorphe à une image de G.

(3) $G/G_k \cong G_{n-k}$ pour tout $k = 1, 2, ..., n$.

(4) Toute image de G est isomorphe à un sous groupe normal de G.

Preuve.
(1) $\Rightarrow$ (2) par la définition d'un groupe fortement morphique.
(2) $\Rightarrow$ (3) par 2, il existe $N \triangleleft G$ tel que $G/G_k \cong N$, posons $N = G_i$ alors $G/G_k \cong G_i$, alors $i = n - k$.
(3) $\Rightarrow$ (4) G/N étant donné, $N \triangleleft G$, soit $N = G_k$, puisque G est uni-série ; appliquons (3).
(4) $\Rightarrow$ (1) par 2.4.1, il suffit de montrer que G est morphique, par 2.3.3 il est suffisant de montrer que $G/G_k \cong G_{n-k} \Rightarrow G/G_{n-k} \cong G_k$ mais $G/G_{n-k} \cong G_i$ pour un certain i par (4), alors $i = n - (n - k) = k$ par 2.3.2. ■

Corollaire 2.4.6 *Tout groupe simple est fortement morphique.*

Corollaire 2.4.7 *Supposons que $G \supset S \supset 1$ sont les seuls sous groupes normaux de G, alors G est fortement morphique si et seulement si $G/S \cong S$.*

Conséquence : A_4 et S_n pour $n \geq 5$, sont tous uni-série morphiques de hauteur 2 mais ne sont pas fortement morphiques.

2.5 Produit direct

Proposition 2.5.1 *Si $P = G \times H$ est morphique, alors G et H sont aussi morphiques.*

Preuve. $\alpha \in end(G)$ étant donné, avec $G\alpha \triangleleft G$, définissons $\overline{\alpha} \in end(P)$ par : $(g,h)\overline{\alpha} = (g\alpha, h)$, alors $ker(\overline{\alpha}) = ker(\alpha) \times 1$ et $P\overline{\alpha} = G\alpha \times H \triangleleft P$ donc $\frac{G}{G\alpha} \cong \frac{G \times H}{G\alpha \times H} = \frac{P}{P\overline{\alpha}} \cong ker(\overline{\alpha}) = ker(\alpha) \times 1 \cong ker(\alpha)$. ■

Définition 2.5.2 *Un groupe G est dit hamiltonien s'il est non abélien et tout sous groupe est normal.*

Proposition 2.5.3 *aucun groupe hamiltonien n'est morphique.*

Preuve. Tout groupe hamiltonien possède le groupe quaternion Q_8 comme un facteur direct, par (2.5.1), il suffit de montrer que Q_8 n'est pas morphique.
$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ ou $i^2 = j^2 = k^2 = ijk = -1$.
Si $C = \{1, -1\}$ alors $\dfrac{Q_8}{\langle i \rangle} = C_2 \cong C$ mais $\dfrac{Q_8}{C} \cong C_2 \times C_2 \ncong \langle i \rangle$. ■

Proposition 2.5.4 *Soit $G = G_1 \times G_2 \times ... \times G_n$ où $hom(G_i, G_j) = \{\theta\}$ pour tout $i \neq j$. alors G est morphique si et seulement si G_i est morphique pour tout i*

Preuve. Si G est morphique alors les G_i le sont aussi par (2.5.1).
Réciproquement, supposons que les G_i sont morphique.
Si $\alpha \in end(G)$ alors, puisque $Hom(G_i, G_j) = \theta$ pour $i \neq j$,il existe $\alpha_i \in end(G_i$ tel que $\langle g_1, ..., g_n \rangle \alpha = \langle g_1 \alpha_1, ..., g_n \alpha_n \rangle$ pour tout $\langle g_1, ..., g_n \rangle \in G$; ainsi $ker(\alpha) = \Pi_{i=1}^n ker(\alpha_i)$ et $Im(\alpha) = \Pi_{i=1}^n Im(\alpha_i)$, donc G est morphique car :

$$\frac{G}{Im(\alpha)} = \frac{\Pi_{i=1}^n G_i}{\Pi_{i=1}^n Im(\alpha_i)} \cong \Pi_{i=1}^n \frac{G_i}{Im(\alpha_i)} \cong \Pi_{i=1}^n ker(\alpha_i) = ker(\alpha).$$

■

Proposition 2.5.5 *Un groupe nilpotent fini G est morphique si et seulement si chaque sous groupe de sylow est morphique.*

Preuve. On a $G \cong S_1 \times S_2 \times ... \times S_n$, où les S_i sont les sous groupes de sylow.
Si G est morphique alors chaque S_i est morphique par 2.5.1 .
Réciproquement, si les S_i sont morphiques, comme on a $hom(S_i, S_j) = \{\theta\}$ pour tout $i \neq j$, alors G est morphique par (2.5.4) . ■

Lemme 2.5.6 *Soit S un groupe non abélien simple, si G est un groupe et $K \triangleleft (S \times G)$ alors soit $K = 1 \times H$ pour un certain $H \triangleleft G$, ou bien $K = S \times H$ pour certain $H \triangleleft G$.*

Preuve. Notons $P = S \times G$, soit $\pi : P \longrightarrow P$ la projection donné par $(s, g)\pi = (s, 1)$ et $S_1 = S \times 1$, si $K \triangleleft P$ alors $K\pi \triangleleft S_1$, $K\pi = 1$ où $K\pi = S_1$ car $S_1 \cong S$ est simple, dans le premier cas, $K \subseteq ker(\pi) = 1 \times G$ alors $K = 1 \times H$ ou $H = \{h \in G|(1, h) \in K\} \triangleleft G$.
Supposons que $K\pi = S_1$, alors si $s \in S$, on a $(s, 1) \in K\pi$, $(s, 1) = (s, k)\pi$ ou $(s, k) \in K$, alors si $t \in S$ est arbitraire, nous obtenons $(tst^{-1}, 1) = (t, 1)(s, k)(t, 1)^{-1}(s, k)^{-1} \in K$ car $K \triangleleft P$, il s'en suit que $S' \times 1 \subseteq K$ ou S' est le sous groupe des commutateurs, mais $S' = S$, car S est simple et non abélien, alors on conclut que $S_1 \subseteq K$, mais alors si on écrit $H = \{h \in G|(1, h) \in K\}$, on a $H \triangleleft G$ et $K = S \times H$.
Si G est abélien, Le lemme est faux. ■

Définition 2.5.7 *On dit que $K_1 \times K_2 \times ... \times K_n$ est un sous groupe standard de $S_1 \times S_2 \times ... \times S_n$ si pour tout i $K_i = \{e\}$ ou $K_i = S_i$.*

Proposition 2.5.8 *Soit G un groupe et $K \triangleleft (S_1 \times S_2 \times ... \times S_n) \times G$, ou chaque S_i est non abélien et simple, alors $K = U \times H$ ou $U \triangleleft (S_1 \times S_2 \times ... \times S_n)$ est standard, and $H \triangleleft G$.*

Preuve. Si $n = 1$ voir le lemme précédent, supposons que $n \geq 1$, $S = S_1 \times S_2 \times ... \times S_n$, alors $K \triangleleft S_1 \times (S \times G)$, alors $K = X \times B$ ou $X \in \{1, S_1\}$ et $B \triangleleft (S \times G)$, alors $B = U' \times H$ ou $U' \triangleleft S$ est standard, et $H \triangleleft G$, ainsi nous avons fini avec $U = X \times U'$. ■

Corollaire 2.5.9 *Soit $G = S_1 \times S_2 \times ... \times S_n$, chaque S_i est non abélien et simple. Alors tout sous groupe normal de G est standard.*

Proposition 2.5.10 *Si $G = S_1 \times S_2 \times ... \times S_n$ et si chaque S_i est non abélien et simple, alors G est fortement morphique.*

Preuve. Montrons d'abord que G est morphique, en effet soit $G/K \cong N$ ou $K \triangleleft G$ et $N \triangleleft G$, alors $K = \Pi_l S_i$ pour un certain $l \in \{1, 2, ..., n\}$ par le corollaire précédent $G/K \cong \Pi_{l'} S_i$ ou l' est la complémentaire de l dans $\{1, 2, ..., n\}$, donc $N \cong \Pi_{l'} S_i$, puisque N est standard il existe $\sigma \in aut(G)$ tel que $N\sigma = \Pi_{l'} S_i$. Ainsi $G/N \cong G\sigma/N\sigma = G/$

$(\Pi_{l'} S_i) \cong \Pi_{l''} S_i = K$.

Finalement, pour montrer que G est fortement morphique, il faut montrer que si $U \triangleleft G$ alors U est isomorphe à une image de G.

Puisque U est standard par le lemme précédente, on a $U = \Pi_l S_i$ pour un certain $l \in \{1, 2, ..., n\}$ alors $G = U \times U'$ ou $U' = \Pi_l S_i$, mais alors $U \cong G/U'$. ■

Corollaire 2.5.11 *Si S est un groupe simple, alors S^n est morphique.*

Preuve. Si S est non abélien, nous utilise alors la proposition précédente, si S est abélien alors S^n est morphique, si $S \cong Z_p$ ou p est premier, alors S^n est un espace vectoriel sur Z_p.

Supposons que $U \triangleleft S^n$, posons $dim(U) = k$ alors $dim(S/U) = n - k$, et S certainement possède un sous espace de dimension $n - k$, alors S^n est fortement morphique. ■

Définition 2.5.12 *Un groupe G est dit caractéristiquement simple s'il n'admet pas des sous groupes caractéristiques.*

Tout groupe caractéristiquement simple fini est un produit fini de groupes simples isomorphes.

Corollaire 2.5.13 *Tout groupe caractéristiquement simple fini est fortement morphique.*

On sait que tout groupe simple est morphique.

Théorème 2.5.14 *Soit $P = S_1 \times S_2 \times ... \times S_n \times G$, (chaque S_i est non abélien et simple), et G morphique avec la condition de chaine descendante sur les sous groupes, si aucun des S_i n'est un sous quotient de G alors P est morphique.*

Preuve. Notons $S = S_1 \times S_2 \times ... \times S_n$, est tel que $\dfrac{G}{K} \cong N \triangleleft P$, il faut montrer que $P/N \cong K$. Par la proposition (2.1.27) on a $K = U \times X$ et $N = V \times Y$ ou U et V sont normaux dans S et standards, $X \triangleleft G$ et $Y \triangleleft G$.

Soit $S = U \times U'$ ou U' est standard. Alors :

$$V \times Y = N \cong \frac{P}{K} = \frac{S \times G}{U \times X} \cong \frac{S}{U} \times \frac{G}{X} \cong U' \times \frac{G}{X}.$$

Donc soit :

$$\sigma : V \times Y \longrightarrow U' \times \frac{G}{X} \text{ un isomorphisme.}$$

a) On a aussi $V \cong U'$.

Définissons $\iota : V \longrightarrow V \times Y$ par $v\iota = (v, 1)$, et soit $\pi; U' \times \frac{G}{X} \longrightarrow \frac{G}{X}$ la projection. Alors $V\iota\sigma\pi = 1$ par hypothèse, donc $V\iota\sigma \subseteq ker(\pi) = U' \times 1 \cong U'$. Cela donne lieu à un monomorphisme $\mu : V \longrightarrow U'$, de même soit $v : U' \longrightarrow V$ injectif, alors $\mu v : V \longrightarrow V$ est injectif, mais V vérifie DCC sur les sous groupes, alors μv est un isomorphisme, il s'en suit que $\mu : V \longrightarrow U'$ est aussi un isomorphisme.

b) $\frac{G}{X} \cong Y$.

$\frac{G}{X} \cong Y$.

Définissons $\varepsilon : Y \longrightarrow V \times Y$ par $y\varepsilon = (1, y)$, donc par (2.5.8) $Y\varepsilon\sigma \lhd U' \times \frac{G}{X}$ alors $Y\varepsilon\sigma = U" \times T$ ou $U" \lhd U$ et $T \lhd \frac{G}{X}$, cela implique que $U" \hookrightarrow Y\varepsilon\sigma$ et $U" = 1$ par hypothèse, ainsi $Y\varepsilon\sigma = 1 \times T \cong T \lhd \frac{G}{X}$.

Soit $\lambda : Y \longrightarrow \frac{G}{X}$ injectif, un argument similaire implique qu'il existe un monomorphisme $\mu : \frac{G}{X} \longrightarrow Y$, tel que $\lambda\mu : Y \longrightarrow Y$ et $\mu\lambda : \frac{G}{X} \longrightarrow \frac{G}{X}$ sont injectifs. Puisque Y et $\frac{G}{X}$ hérite la condition de chaine descendante sur les sous groupes, il s'en suit que $\frac{G}{X} \cong Y$.

Puisque G est morphique, on a $X \cong \frac{G}{Y}$ par la proposition b, aussi puisque S est fortement morphique, on a $S/V \cong S/U'$, mais $\frac{P}{N} = \frac{S \times G}{V \times Y} \cong \frac{S}{V} \times \frac{G}{Y} \cong U \times X = K$, Cela prouve que P est morphique.

■

Corollaire 2.5.15 *Soit $P = S_1 \times S_2 \times ... \times S_n \times G$ dont tout S_i est simple et non abélien. Si G est un groupe abélien morphique fini, alors P est morphique.*

Chapitre 3

p-Groupes

Puisque les groupes nilpotents sont produit de p-groupes ; et que l'étude de ces derniers nous informe sur le caractère "morphique" de ces groupes, ce chapitre a été consacré aux p-groupes.

3.1 p-Groupes

Théorème 3.1.1 *Un groupe nilpotent fini G est morphique si et seulement si chaque sous groupe de syllow est morphique.*

Ce théorème montre que la décision pour un groupe nilpotent fini d'être morphique se résume aux cas des p-groupes finis où p est premier. Dans cette section, nous présentons quelques résultats de décision pour qu'un p-groupe soit morphique ; p toujours un entier premier.
2.3.6 montre qu'un p-groupe abélien fini G est morphique si et seulement si $G \cong (C_{p^k})^m$ pour un certain k et m ; le théorème fondamental donne :

Proposition 3.1.2 *Un p-groupe abélien fini G est morphique si et seulement si deux sous* *groupes maximaux quelconques de G sont isomorphes.*

Théorème 3.1.3 *Soit G un groupe morphique fini avec $\mid G \mid= p^n$, alors :*

1- Tout les sous groupes et les images de G d'ordre p^{n-1} sont isomorphes.

2- G/G' est morphique.

Preuve. 1 : Soit M un sous groupe maximal de G, puisque G est un p-groupe, on a $M \lhd G$ et $\mid M \mid= p^{n-1}$, et puisque $Z = Z(G) \neq 1$, fixons $z_0 \in Z$ avec $\mid z_0 \mid= p$, alors $G/M \cong C_p \cong \langle z_0 \rangle \lhd G$, puisque G est morphique $M \cong G/\langle z_0 \rangle$, maintenant soit F une image de G avec $\mid F \mid= p^{n-1}$, alors $F \cong G/N$ ou N est normal dans G et $\mid N \mid= p$, d'où $G/M \cong C_p \cong N$ et comme G est morphique $M \cong G/N \cong F$, d'où 1.
2 : Soit M/G' et N/G' des sous groupes maximaux de G/G', par 1 soit $\sigma : M \longrightarrow N$ un isomorphisme. Alors σ induit un isomorphisme $M/G' \longrightarrow N/G'$, alors G/G' est morphique par 3.1.2. ■
Notons que tous les sous groupes maximaux du groupe des quaternions Q_8 sont isomorphes à C_4, mais Q_8 n'est pas morphique.
D'ailleurs ni D_4 ni Q_8 ne sont morphiques par la proposition suivante :

Proposition 3.1.4 *Soit G un groupe avec $\mid G \mid= p^n, n \geq 3$, et supposons que G possède un sous groupe cyclique d'ordre p^{n-1}, alors G est morphique si et seulement s'il est cyclique.*

Preuve. Si G est cyclique alors il est morphique (évident).
Réciproquement supposons que $A = \langle a \rangle \subseteq G$ d'ordre p^{n-1} alors $A \lhd G$ et $G/A \cong C_p \cong \langle z \rangle \lhd G$ pour un certain $z \in Z(G)$ d'ordre p, comme G est morphique, on a $G/\langle z \rangle \cong A \cong C_{p^{n-1}}$ ce qui implique que G est abélien et donc $G \cong C_{p^{n-1}} \times C_p$ ou $G = C_{p^n}$ mais $C_{p^{n-1}} \times C_p$ n'est pas morphique par 2.3.6 car $n-1 \geq 2$, ainsi $G \cong C_{p^n}$ est cyclique. ■
Notons que si $n = 2$ dans la proposition précédente, alors G est abélien d'ordre p^2, il s'en suit que $G \cong C_{p^2}$, et les deux sont morphiques. Rappelons qu'un groupe est d'exposant fini si les ordres des éléments de G sont bornés ; l'exposant de G ($exp(G)$) est le plus petit multiple commun des ordres des éléments de G.

Définition 3.1.5 *Un groupe G est dit élémentaire abélien s'il est abélien d'exposant p, pour un p premier.*

Proposition 3.1.6 *Soit G un groupe tel que $\mid G \mid = p^3$.*
Les assertions suivantes sont équivalentes :

1) G est morphique.

2) G est ou bien cyclique, ou bien élémentaire abélien, ou bien non abélien d'exposant p.
De plus, dans ce cas on a :

* *Si $p = 2$ alors G est cyclique ou élémentaire abélien.*

* *Si $p > 2$ alors G est soit cyclique, soit élémentaire abélien, ou bien $G = \langle a, b, c \mid a^p = b^p = c^p = 1, [a, b] = c, ac = ca, bc = cb \rangle$.*

Preuve. 1) $\Rightarrow$ 2) : Si $exp(G) = p^3$ alors G est cyclique, si $exp(G) = p^2$ alors G possède un sous groupe cyclique d'ordre p^2 et aussi G est cyclique par 1) et 2.3.6. Si $exp(G) = p$ alors 2) est évident.
2) $\Rightarrow$ 1) : Puisque les groupes cycliques sont morphiques, nous pouvons supposer que $exp(G) = p$. Si $K \lhd G$ est tel que $G/K \cong N \lhd G$ nous devons montrer $G/N \cong K$. Puisque K et G/K sont d'exposant p, alors deux cas sont possibles :
si $\mid K \mid = p$ alors $\mid N \mid = p^2$, il s'en suit que $G/N \cong C_p \cong K$.
si $\mid K \mid = p^2$ alors $\mid N \mid = p$, il s'en suit que $G/N \cong C_p \times C_p \cong K$.
Pour le reste : si $p = 2$ alors G est abélien car D_4 et Q_8 ne sont pas morphiques, d'où G est cyclique ou élémentaire abélien par 2).
Si $p > 2$ et si G est abélien, alors il est cyclique ou élémentaire abélien, sinon on peut vérifier que $G' = Z(G)$ est le seul sous groupe normal d'ordre p dans G.
Maintenant G/G' a le type (p, p) car $exp(G) = p$, et $G = \langle a, b, G' \rangle$. On note $c = [a, b]\rangle$, alors $c \neq 1$ puisque G n'est pas abélien. D'où $G' = \langle c \rangle$ car $exp(G) = p$, et donc $G = \langle a, b, c \rangle$. Puisque $c \in Z(G)$, nous obtenons le résultat préconisé.

Soit maintenant G un groupe morphique avec $\mid G \mid = p^4$, si G est abélien alors il est isomorphe à un des $C_{p^4}, C_{p^2} \times C_{p^2}$ ou $C_p \times C_p \times C_p \times C_p$ (2.3.6). ■

Étonnamment il n'y a pas de groupe non abélien morphique d'ordre p^4.

Proposition 3.1.7 *Si p est premier, tout groupe morphique d'ordre p^4 est abélien.*

Preuve. Supposons que G est un groupe non abélien morphique avec $\mid G \mid = p^4$.

Soit A un sous groupe normal de G tel que $\mid A \mid = p^3$, alors tout sous groupe et toute image de G d'ordre p^3 est abélien (3.1.3).

En particulier, si $z \in Z(G)$ d'ordre p, alors $G/\langle z \rangle$ est abélien, d'où $G' \subseteq \langle z \rangle \subseteq Z(G)$, puisque $G' \neq 1$ (G est non abélien), on a $G' =< z >$, donc $G/\langle z \rangle$ est morphique, et a le type (p, p, p), et on a $G = \langle a, b, c, G' \rangle$.

Puisque G est non abélien, on peut supposer que $ab \neq ba$, ainsi $\langle a, b \rangle$ est un sous groupe non abélien propre de G, alors $\mid \langle a, b \rangle \mid = p^3$. (Contradiction) ■

Définition 3.1.8 *Un p-groupe fini G est dit élémentaire abélien morphique ou simplement ea-morphique si :*

Soit N un sous-groupe normal de G, tel que N est élémentaire abélien ou $\dfrac{G}{N}$ est élémentaire abélien, alors il existe un épimorphisme $\phi : G \longrightarrow N$ tel que $\dfrac{G}{N} \cong \ker(\phi)$.

Définition 3.1.9 *On dit qu'un groupe G est s.auto-dual si tout sous groupe de G est isomorphe à un quotient de G, q.auto-dual si tout quotient de G est isomorphe à un sous groupe de G, auto-dual s'il est à la fois s.auto-dual et q.auto-dual.*

Conjecture

Les seuls p-groupes morphiques finis sont les groupes abéliens, les groupes homocycliques, et les groupes non abéliens d'ordre p^3 et d'exposant p (p premier).

Théorème 3.1.10 *Soit G un p-groupe morphique fini, alors :*

1) tout sous groupe de G est l'image homomorphique de G.

2) toute image homomorphique de G est isomorphe à un sous groupe normal de G.

Le dernier résultat montre qu'un p-groupe morphique fini appartient à la classe des groupes auto-duals.

Théorème 3.1.11 *Soit G un p-groupe morphique fini.*
Si G peut être engendré par deux éléments alors :
G est abélien et homocyclique ou bien
p est impair et G est isomorphe à un groupe d'ordre p^3 d'exposant p.

Théorème 3.1.12 *Soit G un p-groupe auto-dual fini. Alors :*

1. *G est abélien, ou*
2. *p est impair, et G est le produit direct du groupe non abélien d'ordre p^3 d'exposant p, par un groupe élémentaire abélien.*

Théorème 3.1.13 *Soit G un p-groupe non abélien ea-morphique. Alors G est engendré par deux éléments.*

Résultat
Les p-groupes morphiques finis sont des groupes ea-morphiques.

3.2 Triplets morphiques

Le but de ce qui suit est la démonstration du théorème suivant :

Théorème 3.2.1 *Soit G un p-groupe ea-morphique fini et non abélien alors G est engendré par deux éléments.*

Lemme 3.2.2 *Si N un sous groupe normal de G alors :*
$(\dfrac{G}{N})' \cong \dfrac{G'}{G' \cap N}$.

Preuve. Soit $G \neq \{1\}$ un p-groupe ea-morphique fini, avec nombre minimal de générateurs d ie, $\mid \dfrac{G}{\Phi(G)} \mid = p^d$. Soit N un sous groupe d'ordre p normal de G, alors pour tout sous groupe maximal M de G, on a $\dfrac{G}{M} \cong N$ donc aussi $\dfrac{G}{N} \cong M$.

■

On particulier nous obtenons :

Lemme 3.2.3 *Dans un p-groupe morphique fini, tous les sous groupes maximaux sont isomorphes.*

A partir de maintenant nous supposerons G non abélien et prendrons $N \leq G'$. Puisque $M \cong \frac{G}{N}$, alors par le lemme précédent :
$|M'| = |\frac{G'}{N}| = \frac{|G'|}{p}$, donc aussi :
$|\frac{G'}{M'}| = p$.
Considérons le sous groupe caractéristique K de G défini par :
$K = \cap\{M' : M < G\}$. $\frac{G'}{K}$ est isomorphe à un sous groupe de $\prod_{M<G} \frac{G'}{M'}$, donc il est élémentaire abélien.
Considérons l'application :

$$\beta : \frac{G}{\Phi(G)} \times \frac{G}{\Phi(G)} \longrightarrow \frac{G'}{K}$$
$$\text{donneé par } (a\Phi(G), b\Phi(G)) \longrightarrow [a,b]K.$$

β est bien définie, comme on a :

Lemme 3.2.4 $[G, \Phi(G)] \leq K$. *on particulier,* $\Phi(G)' \leq K$.

Preuve. $(\frac{G}{M'})' = \frac{G'}{M'}$ est d'ordre p.
D'abord on a $[G, G'] \leq M'$ pour tout $M < G$, donc $[G, G'] \leq K$. de même si $a, b \in G$, alors pour tout $M \lessdot G$ on a :

$$[a, b^p] \equiv [a,b]^p \equiv 1 \text{ (Mod } M').$$

on vient de voir que $[b, [a,b]] \in M'$ et aussi $[G, G^p] \leq K$.
Cela donne aussi que β est bilinéaire, puisque

$$[ab, c] = [a,c].[[a,c],b].[b,c] \equiv [a,c].[b,c],\ ModK.$$

■

Les F_p-espaces vectoriels $V = \dfrac{G}{\Phi(G)}$ et $W = \dfrac{G'}{K}$ avec l'application β satisfont aux définitions suivantes :

Définition 3.2.5 *Soit V, W deux espaces vectoriels sur F_p, et*

$$\beta : V \times V \to W$$
$$(v_1, v_2) \mapsto [v_1, v_2]$$

une application bilinéaire alternée.
Si U_1, U_2 sont deux sous espaces de V, notons $[U_1, U_2]$ pour $\beta(U_1, U_2)$, et U_1' pour $[U_1, U_1]$.
(V, W, β) est dit triplet morphique si les conditions suivantes sont vérifiées :

1) $V' = W$.

2) Pour tout $U \lessdot V$, on a $U' \lessdot W$.

3) $\cap\{U' : U \lessdot V\} = \{0\}$.

La considération seule des triplets morphiques ne suffit pas pour démontrer le théorème, comme il existe des exemples de triplets morphiques non associées avec les p-groupes morphiques finis.

Proposition 3.2.6 *Soit (V, W, β) un triplet morphique.*
Soit $U \lessdot V$ alors il existe un unique $T = \tau(U) \lessdot U$ satisfaisant aux propriétés suivantes :
Pour $S \lessdot V$ il y a est équivalence entre :

1) $U' = S'$ et

2) $S \geq T$.

Preuve. Soit $a \in V \setminus U$. Considérons l'application τ

$$U \longrightarrow W \longrightarrow W/U'$$

définie par $x \mapsto [a,x]+U'$; puisque $W = V' =< a, U >' = [a,U]+U'$, c'est une application linéaire surjective, avec $\dim(W/U') = 1$. Ainsi :
$T = \tau(U) = ket(\tau) = \{x \in U : [a,x] \in U'\}$ est un sous espace maximal de U. Par définition $[a,T] \leq U'$.
On peut voir facilement que T est indépendant du choix de $a \in V \setminus U$. Ainsi si $T \lessdot S \lessdot V$, et $S \neq U$, on peut supposer que $S = [a,T]$. Il s'en suit que $S' = [a,T]+T' \leq U'+T' \leq U'$ et ainsi que $S' = U'$, puisque il sont tous les deux des sous espaces maximaux de W.
Inversement, supposons que $U \neq S \lessdot V$; et $S' = U'$.
Alors $S \cap U \lessdot U$ et si $S =< a, S \cap U >$ alors $a \notin U$, et on a $[a, S \cap U] \leq S' = U'$ tel que $S \cap U = \tau(U)$. ∎

Corollaire 3.2.7 *Pour tout $U \lessdot V$ l'ensemble*

$$\{S \lessdot V : S' = U'\}$$

possède $p+1$ éléments, à savoir les sous espaces S tel que $\tau(U) \lessdot S \lessdot V$.

Preuve.
L'ensemble M des sous espaces maximaux de W a

$$1 + p + ... + p^{e-1}$$

éléments, où $e = \dim(W)$.
Le corollaire implique que le sous ensemble de M

$$\Re = \{Z \lessdot W : Z = U' \text{ pour certain } U \lessdot V\}$$

possède $(1+p+...+p^{d-1}/1+p$ éléments, ainsi d est pair, et

$$\frac{1+p+...+p^{d-1}}{1+p} = 1+p^2+...+p^{d-2}.$$

Il est clair que si $e < d-1$ on a

$$\mid M \mid = 1+p+...+p^{e-1} < 1+p^2+...+p^{d-2} = \mid \Re \mid.$$

Contradiction. ∎

nous venons de montrer le :

Corollaire 3.2.8 *Dans un triplet morphique (V, W, β), on a*

$$dim(W) \geq dim(V) - 1$$

En particulier, dans un p-groupe non abélien ea-morphique fini G avec un nombre minimal des générateurs d on a

$$\mid G'/K \mid \geq p^{d-1}.$$

Nous sommes maintenant en mesure de prouver le théorème principal.

Soit G un p-groupe non abélien ea-morphique fini avec un nombre minimal de générateurs $d > 2$, nous voulons trouver une contradiction.

Par la définition (3.1.8) il existe un épimorphisme $G \longrightarrow \Phi(G)$, et si $E = ker(\Phi)$ puisque $G/E \cong \Phi(G)$, on a aussi $G/\Phi(G) \cong E$ et puisque $\mid G/\Phi(G) \mid = p^d$, E est un sous groupe élémentaire abélien normal de G d'ordre p^d.

Soit

$$p^t = \mid E \cap G' \mid \text{ avec } t \leq d.$$

Puisque $G/E \cong \Phi(G)$ le Lemme (3.2.2) donne :

$$\mid \Phi(G)' \mid = \mid \frac{G'}{E \cap G'} \mid = \frac{\mid G' \mid}{p^t}.$$

Par le Lemme (3.2.4) et le corollaire (3.2.8) nous obtenons

$$\mid E \cap G' \mid = \mid \frac{G'}{\Phi(G)'} \mid = p^t, \text{ pour } t \in \{d, d-1\}.$$

Soit alors L un sous groupe élémentaire abélien normal d'ordre p^{d-1} contenu dans G' (nous prenons L égal $E \cap G'$ s'il est d'ordre p^{d-1} sinon si $E \leq G'$ nous prenons L comme un sous groupe maximal de E qui est normal dans G), et soit

$$\{1\} = L_0 \lessdot L_1 \lessdot L_2 \lessdot ... \lessdot L_{d-1} \leq G'$$

une série des sous groupes, chacun d'eux normal dans G. En particulier, $\mid L_i \mid = p^i$ pour tout i.

Considérons une série arbitraire

$$\Phi(G) = S_0 \lessdot S_1 \lessdot S_2 \lessdot ... \lessdot S_{d-1} \lessdot S_d = G$$

(Nous allons faire un choix plus précis de S_2 plus tard), en particulier chaque S_i est normal dans G ; et $\mid G/S_i \mid= p^{d-i}$ pour tout i. Clairement si $i \geq 1$ on a $G/S_i \cong L_{d-i}$ comme étant deux groupes élémentaires abéliens d'ordre p^{d-i}. Par la définition (2.2.1) on a aussi :

$$G/L_{d-i} \cong S_i, \text{ pour tout } i \geq 1.$$

Pour $i \geq 1$ on a par le Lemme (3.2.2)

$$\mid S_i' \mid=\mid G'/L_{d-i} \mid= \frac{\mid G' \mid}{p^{d-i}},$$

c'est à dire :
$\mid G'/S_i' \mid= p^{d-i}$. ....(3.1).

En particulier, $\mid G'/S_1' \mid= p^{d-1}$. Puisque $S_1 =< a, \Phi(G) >$ pour un certain $a \in G$, le Lemme (3.2.4) implique : $S_1' \leq [< a >, \Phi(G)]\Phi(G)' \leq K$, et par le corollaire (3.2.8) $\mid G'/K \mid= p^{d-1}$ et $S_1' = K$; il s'en suit que $S_i' \geq S_1' = K$ pour tout $i \geq 1$. Nous obtenons de (3.1) :

$$\mid S_i'/K \mid=\mid (G'/K)/(G'/S_i' \mid= p^{i-1} \text{ pour tout } i \geq 1.$$

En particulier $\mid S_2'/K \mid= p$ et $\mid S_3'/K \mid= p^2$. (c'est le seul point où nous utilisons l'hypothèse $d > 2$). Puisque $S_3 =< a, b, c, \Phi(G) >$ pour certains $a, b, c \in G$, le Lemme (3.2.4) donne $S_3' \leq< [a, b], [a, c], [b, c], K >$. Puisque tout élément du carré extérieur d'un espace vectoriel de dimension 3 est un tenseur décomposable, nous pouvons choisir a, b, c tell que $[a, b] \in K$. En choisissant $S_2 =< a, b, \Phi(G) >$ le Lemme (3.2.4) montre que $S_2' \leq K$, une contradiction finale. Finalement nous obtenons une démonstration de la conjecture. Si G est un p-groupe abélien morphique fini, ce n'est pas difficile de voir que G est forcément homocyclique. par le lemme (3.2.3).
Par le théorème (3.1.11), supposons que G est non abélien, puisque les p-groupes morphiques sont ea-morphiques, par le théorème (3.2.1) nous concluons que G est engendré par deux éléments, et par théorème (3.1.12) nous avons ce que nous voulons.

Bibliographie

[1] A. Caranti et C.M. Scoppola, Finit morphic p-Groups. *Journal of Pure and Applied Algebra Volume* 219*, Octobre* 2015*, Pages* $4635 - 4641$.

[2] Cours théorie des groupes, *Master 1.*

[3] Yuanlin Li, W.K.Nicholson, Libo Zan, Morphic groups, *Journal of Pure and Applied Algebra. Volume* 214*,* 2010*, Pages* $1827 - 1834$.

Résumé

Les p-groupes homocycliques finis sont morphiques, ainsi que les groupes non abéliens d'ordre p^3 et d'exposant p.

An, Ding et Zhan ont montré en 2011 que dans la classe des groupes auto-duaux, ce sont les seuls exemples de p-groupes finis morphiques.

Caranti et Scoppolla en 2015 sont arrivés a prouver les mêmes résultats avec moins d'hypothèses.

Les mots-clés : Morphique, homocyclique, élémentaire abélien.

Abstract :
Finit homocyclic p-groups are morphic, and so the non-abelien groups of order p^3 and exposent p.

An, Ding and Zhan proved in 2011 that in the class of self-dual groups, these are the only examples of finit morphic p-groups.

Caranti and Scoppolla were able to prove the same results under a weaker hypothesis

Keywords : Morphic, Homocyclic, elementary abelien.