UNIVERSITE KASDI MERBAH
OUARGLA

Faculté des mathématiques et sciences de la matiére

DEPARTEMENT DE MATHEMATIQUES

master

Spécialité: Mathématiques

Option: Algéber et Géométrie

Par: CHABANI CHOUAIB

Théme

p-GROUPES ET COCLASSE : UNE INTRODUCTION

Version de: 6 juin 2016

Devant le jury composé de:

Mohammed BOUSSAID	Dr UKMO université - Ouargla	president
Mohammed T BENMOUSSA	Dr UKMO université - Ouargla	examinateur
Mohammed l YOUMBAI	Dr UKMO université - Ouargla	examinateur
Mohammed A BAHAYOU	Dr UKMO université - Ouargla	examinateur
Yassine GUERBOUSSA	Dr UKMO université - Ouargla	rapporteur

Dedicase

Je dédie ce mémoire à :

· Mes parents :

Ma mère, qui a oeuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon père, qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi.

Mes frères et soeurs qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité.

Mes professeurs de l'UKMO qui doivent voir dans ce travail la fierté d'un savoir bien acquis.

Remerciement

En premier lieu , je tient a témoigner ma reconnaissance à dieu tout puissant , de m'avoir donnée la possibilité de terminer ce travail .

Je tient a exprimer mon profond respect , et de reconnaissance à mon encadreur de mémoire , **Mr : Yassine GUERBOUSSA** , pour ces conseils , et son encouragement durant la période de la préparation et la rédaction de ce mémoire .

Je remercier sincérement les membres du jury : **Mr.Mohammed BOUSSAID** , d'avoir accepté la présidence du jury . Aussi je remercier vivement , les professeurs : **Mr.Mohammed T BENMOUSSA** d'avoir accepté l'examinateur de ce travail . **Dr.Mohammed A BAHAYOU** d'avoir accepté l'examinateur de ce travail. **Mohammed l YOUMBAI** d'avoir accepté l'examinateur de ce travail . Je les remercier énormément pour l'attention qu'ils ont accordé a ce travail . Il est important pour moi de remercier ma famille : mon pére , ma mére , mon frére et mes soeurs , qui ont toujours été une source inépuisable d'encouragement . Il est important pour moi de remercier tous mes enseignants d'université de KASDI Merbah - Ouargla . Un grand merci a mes collégues pour le soutien qui m'ont donnés .

Introduction.

Rien n'est plus simple qu'un groupe cyclique simple ; c'est à dire un groupe d'ordre premier p. Les p-groupes sont les groupes finis dont la suite de composition contient seulement le groupe simple $\mathbb{Z}_p$.

Dans les débuts de la théorie des groupes, Hölder avait proposé un programme pour traiter les groupes finis :

1. Déterminer tous les groupes simples finis.

2. Pour deux groupes finis donnés, trouver tous les extensions du premier groupe par le deuxième.

La première étape est achevée (en principe) en 2004 ! La classification des groupes simple finis est considéré comme le plus grand achèvement en mathématique dans le siècle précédent ; la démonstration est comprise entre 10000 et 15000 de pages, et est la contribution de plus de 100 mathématiciens.

Pour la deuxième étape, on doit d'abord élaborer le problème avec les groupes construit avec les groupes simples les plus simples ! C'est à dire les p-groupes comme on a déjà mentionné. On sait maintenant que la classification des p-groupes est impossible ; tout simplement le nombre de p-groupes d'ordre p^n augmente dramatiquement avec n.

La théorie de coclasse est une façon pour contourner le problème de classification des p-groupes. La coclasse d'un groupe d'ordre p^n est de classe de nilpotent c est définie comme $n - c$. Dans cette théorie on considère la coclasse comme le premier invariant pour la classification. Cette approche est est commencée par la publication de cinq conjectures par C. Leedham-Green et M. F. Newman, et est inspiré par le travail de N. Blackburn sur les groupes de classe maximale (de coclasse 1).

Ce mémoire est organisé comme suit :

Le premier chapitre commence par les trois théorèmes de Sylow. Ces théorèmes doivent illustrer le rôle des p-groupes dans l'étude des groupes finis. Dans la deuxième section, on montre que les groupes nilpotent finis sont plus ou moins des p-groupes, et la dernière section contient quelques résultats classiques sur les p-groupes.

Le deuxième chapitre est consacré au p-groupes puissants. Ces groupes jouent un rôle décisif dans la démonstration des conjectures de coclasse. On a mentionné brièvement la relation entre les groupes puissants est les groupes analytiques p-adiques.

Les conjectures de coclasse sont discutés dans le dernier chapitre. Quelques implications entre ces conjectures sont prouvées, et une esquisse de la démonstration de la conjecture A qui implique tous les autres, est discutée dans la dernière section.

Table des matières

Chapitre 1

p-groupes finis

Soit p un nombre premier.

Définition 1.0.1. *On appelle p-groupe tout groupe G dont l'ordre de tout élément est une puissance de p.*

Proposition 1.0.1. *Soit G un groupe fini. Alors G est un p-groupe si et seulement si l'ordre de* **G** *est une puissance de p.*

Démonstration. Si l'ordre de G n'est pas une puissance de p alors il existe q premier tel que q divise $|G|$ donc G contient un élément x d'ordre q . On à $x^q = x^{p^k} = 1$. D'après le théorème de Bézout, on peut trouver $a, b \in \mathbb{Z}$ telle que $aq + bp^k = 1$. Donc $x^1 = x^{aq+bp^k} = (x^q)^a(x^{p^k})^b = 1$ contradiction.

Inversement, supposons que $|G| = p^n$ si $x \in G$; alors l'ordre de x est égal à $|\langle x\rangle|$ qui divise p^n par le théorème de lagrange. ■

Dans la suite par un p-groupe on entend toujours un p-groupe fini.

Les p-groupes jouent un rôle central dans la théorie des groupes finis, au moins à cause des théorèmes de Sylow.

1.1 Les théorèmes de Sylow

Soit **G** un groupe fini d'ordre $n = p^r m$, où p ne divise pas m. Un p-sous groupe de Sylow de G est simplement un sous-groupe de G d'ordre p^r.

L'ensemble des p-sous-groupes de Sylow de G sera noté $\mathbf{Syl}_p(\mathbf{G})$. On remarquera qu'un sous-groupe de **G** est un p-Sylow si et seulement s'il est un p-groupe d'indice premier à p. En particulier, si **G** est un p-groupe, il posséde un unique p-Sylow : à savoir **G** lui-même.

Théorème 1. *Soit G un groupe fini. Si p divise $|G|$ alors $\mathbf{Syl}_p(G) \neq \emptyset$.*

Le théorème précédent étant le premier théorème de Sylow. Le deuxième étant

Théorème 2. *Soit G un groupe fini tel que p divise $|G|$. Alors tous les éléments de $\mathbf{Syl}_p(G)$ sont conjugués.*

Le troisième théorème de Sylow stipule

Théorème 3. *Soit G un groupe d'ordre $n = p^r m$, avec m premier à p, et soit n_p le cardinal de $\mathbf{Syl}_p(\mathbf{G})$; alors n_p divise m, et $n_p \equiv 1 \mod p$.*

Pour une démonstration de ces théorèmes classiques voir par exemple [8]

1.2 Groupes nilpotents finis et p-groups

Si x, y sont deux éléments d'un groupe G, alors le commutateur $[x, y]$ est défini par $[x, y] = x^{-1}y^{-1}xy$.

Si on a n éléments $x_1, ..., x_n \in G$, on peut définir $[x_1, ..., x_n]$ par récurrence,

$$[x_1] = x_1 \text{ et } [x_1, ..., x_n] = [[x_1, ..., x_{n-1}], x_n].$$

Définition 1.2.1. *Soit G un groupe. Le $n^{éme}$ terme de la suite centrale descendante $\gamma_n(G)$ de G est défini comme le sous-groupe engendré par tous les commutateurs $[x_1, ..., x_k], k \geq n$.*

On obtient alors une suite décroissante de sous-groupes normaux :

$$... \leq \gamma_n(G) \leq ... \leq \gamma_2(G) \leq \gamma_1(G).$$

Définition 1.2.2. *Un groupe $\mathbf{G}$ est dit nilpotent s'il existe un nombre naturel $n \geq 0$ tel que $\gamma_{n+1}(G) = 1$. Dans ce cas, le plus petit nombre naturel $n \geq 0$ tel que $\gamma_{n+1}(G) = 1$ est appelé la classe de nilpotence de $\mathbf{G}$. On dit aussi que $\mathbf{G}$ est nilpotent de classe n.*

La suite central ascendante de G est définie par réccurence :
$Z_0(G) = 1$ et $Z_{n+1}(G) = \{x \in G | [x, y] \in Z_n(G) \forall y \in G\}$.
Ce n'est pas difficile de montrer que G est nilpotent si et seulement si $Z_n(G) = G$, pour certain n. Si G est de classe c, alors c est le plus petit entier vérifiant $Z_c(G) = G$.

La proposition suivante montre que la class des groupes nilpotents est assez large.

Proposition 1.2.1. *Tout p-groupe est nilpotent .*

Montrons d'abord

Lemme 1.2.1. *Soient p un nombre premier et G un p-groupe fini opérant sur un ensemble fini X. Alors*

$$|X| \equiv |X^G| \mod p$$

où X^G désigne l'ensemble des éléments $x \in X$ tels que $gx = x$ pour tout élément g de G.

Démonstration. On sait que le nombre d'éléments d'une orbite divise toujours l'ordre de G. Puisque G est un p-groupe, il en résulte que le cardinal d'une orbite non réduite à un élément, est de la forme p^n avec $n > 0$. Comme X est réunion disjointe des G-orbites, la réunion des orbites non-triviales a donc un cardinal divisible par p. Comme la réunion des orbites réduites à un élément est l'ensemble des points fixes, l'énoncé en résulte. ■

Lemme 1.2.2. *Le centre d'un p-groupe non-trivial est non-trivial.*

Démonstration. Faisons opérer G sur son ensemble sous-jacent par conjugaison. Les éléments de G fixés par cette action sont exactement les éléments du centre de G. D'aprés le lemme précédent p divise $|Z(G)|$, mais $|Z(G)| \neq 0$, car $Z(G)$ contient l'élément neutre. Le résultat est immédiat maintenant. ■

Démonstration proposition 1.2. D'après le lemme qui précède, le centre $Z(G)$ n'est pas réduit à l'élément neutre, donc si $G/Z(G)$ n'est pas trivial, alors son centre $Z_2(G)/Z(G) \neq 1$. L'itération de cet opération, implique qu'il existe un entier n tel que $Z_n(G) = G$, ce qui revient à dire que G est nilpotent. ■

Théorème 4. *Si G est un groupe nilpotent fini alors G est produit direct de p-groupes :*

$$G \backsimeq P_1 \times ... \times P_k$$

où P_i est le p_i-Sylow de G, et les p_i sont les diviseurs premiers de $|G|$.

Montrons d'abord

Proposition 1.2.2. *Si G est un groupe nilpotent fini, et $H < G$; alors $H < N_G(H)$; où $N_G(H) = \{g \in G | g^{-1}Hg = H\}$.*

Démonstration. Si $Z_k(G) \subseteq H$, pour tout k, alors $H = G$, ce qui n'est pas le cas, donc soit n le plus petit entier qui vérifie $Z_n \nsubseteq H$. Ainsi, $Z_{n-1}(G) \subseteq H$. Soit $x \in Z_n(G) - H$, on à $[x, h] \in Z_{n-1}(G) \subseteq H$ pour tout $h \in H$. D'où $h \in N_G(H) - H$. ■

Corollaire 1.2.1. *Dans un groupe nilpotent tout sous-groupe maximal est normal.*

En effet, soit $M \leqslant G$. On à $M < N_G(M)$, et comme M est maximal $N_G(M) = G$; donc $M \lhd G$.

Proposition 1.2.3. *Dans un groupe nilpotent tout sous-groupe de Sylow est normal.*

Rappelons d'abord l'argument de Frattini : si $H \lhd G$, et $P \in \mathbf{Syl}_P(H)$, alors $G = HN_G(P)$.

En effet, soit $g \in G$; alors $P^g \subseteq H^g = H$ donc $P^g \in \mathbf{Syl}_P(H)$. D'où, par le deuxième théorème de Sylow, $\exists h \in H$ tel que $P^g = P^h$ donc $P^{gh^{-1}} = P$; par suite $gh^{-1} \in N_G(P)$, donc $g \in HN_G(P)$.

Démonstration de la Proposition 1.2.3. Soit $P \in \mathbf{Syl}(G)$. Si $P \ntriangleleft G$, alors $N_G(P) < G$. Soit M un sous-groupe maximal de G tel que $N_G(P) \leq M$. Par corollaire 1.2.1, $M \lhd G$ et $P \in \mathbf{Syl}_p(M)$; donc par l'argument de Frattini $G = M; N_G(P) = M$ contradiction . D'ou $P \lhd G$.

■

Démonstration du Théorème 4. Soient $p_1, ..., p_k$ les diviseurs premiers de $|G|$. Chaqu'un deux donne un p_i-Sylow P_i. Montrons que $G = P_1 \times P_2 \times ... \times P_s$, ou d'une façon équivalente que

$$G = P_1P_2...P_s \text{ et } P_i \cap \langle P_j, j \neq i \rangle = 1$$

Soit $x \in G$. Posons $|G| = n = p_1^{\alpha_1}...p_s^{\alpha_s}$. soit $n_i = n/p_i^{\alpha_i}$ et ainsi, $PGCD(n_1...n_s) = 1$.

En effet, si q divise tous les n_i alors q divise $p_2^{\alpha_2}...p_s^{\alpha_s}$ donc $p_i = q$, pour certain i.

Mais q divise $n_i = n/p_i^{\alpha_i}$. contradiction.

D'après Bézout, $\exists m_1, m_2, ..., m_s \in \mathbb{Z}$ tels que $m_1n_1 + m_2n_2 + ... + m_sn_s = 1$. D'où

$$x = x^1 = x^{m_1n_1}x^{m_2n_2}...x^{m_sn_s}$$

mais $(x^{m_in_i})^{p_i^{\alpha_i}} = (x^{m_i})^n = 1$; donc $x^{m_in_i} \in P_i$. Il résulte que $x \in P_1 \dots P_n$.

Maintenant, si $x \in P_i \cap \langle P_j, j \neq i \rangle$, alors $x^{p_i^{\alpha_i}} = 1$, d'autre part, $x = x_1 x_2 ... x_{i-1} x_{i+1} ... x_s$, où $x_k \in P_k$. Donc

$$x^{p_i^{\alpha_i}} = x_1^{p_i^{\alpha_i}} \dots x_s^{p_i^{\alpha_i}} = 1,$$

d'où $x_j = 1$, pour tout $j \neq i$; ainsi $x = 1$.

■

1.3 Un peu de folklore sur les p-groups

C'est impossible de couvrir d'une façon raisonnable tous les résultats significatifs sur les p-groupes dans un livre (l'essai [1, 2, 3] est loin d'être exhaustive ou compréhensive). Donc on ne peut ici que représenter des résultats assez classiques et d'une manière assez sélective.

Définition 1.3.1. *Soit* $\mathbf{G}$ *un groupe. Le sous-groupe de Frattini de* $\mathbf{G}$ *qu'on note* $\Phi(\mathbf{G})$*, est défini comme l'intersection de tous les sous-groupes maximaux de* G*.*

Dans le cas ou G ne contient aucun sous-groupe maximal, on pose $\Phi(\mathbf{G}) = G$.

Soit G un groupe et $x \in G$. On dit que x est un élément non-générateur de G, si pour toute partie S de G : $S \cup \{x\}$ engendre G si est seulement si S engendre G.

Proposition 1.3.1. *L'ensemble des éléments non-générateurs d'un groupe fini* G *coïncide avec le sous-groupe de Frattini.*

Démonstration. Soit d'abord $x \in \mathbf{G}$ un élément non-générateur. Pour tout sous-groupe maximal $\mathbf{H} < \mathbf{G}$, si l'on a $x \notin \mathbf{H}$, on aurait $\langle \mathbf{H}, x \rangle = G$, et ainsi $\mathbf{H} = \mathbf{G}$, ce qui est absurde. Donc x appartient à tous les sous-groupes maximaux de G, d'où $x \in \Phi(G)$. Soit maintenant $x \in \Phi(G)$. Soit S une partie de $\mathbf{G}$ telle que $\langle S, x \rangle = \mathbf{G}$. Si $\langle S \rangle < \mathbf{G}$; alors comme G est fini, il existe un sous-groupe maximal H de G tel que $\langle S \rangle \leq H$. Mais $x \in H$, donc $G = \langle \mathbf{S}, x \rangle \leq \mathbf{G}$, contradiction. ■

Proposition 1.3.2. *Si* G *est un* p*-groupe, alors* $\Phi(G) = G'G^p$*.*

Démonstration. Soit M un sous-groupe maximal de G. D'après Corollaire 1.2.1, M est normal, et ainsi G/M est un groupe nilpotent simple, d'où $G/M \cong \mathbb{Z}_p$. Ceci implique que M contient G' et

G^p, et ainsi $G'G^p$. Comme ceci est vrai pour tout sous-groupe maximal M, on a $G^{'}G^p \leq \Phi(G)$. D'autre part, $G/G^{'}G^p$ est un groupe abélien d'exposant p, donc on peut le considérer comme un espace vectoriel sur le corps $\mathbb{Z}_p$. Les sous-groupes maximaux de G correspondent au hyperplans de cet espace, mais l'intersection de hyperplans dans un espace vectoriel est trivial ; d'où $\cap_M M \leq G'G^p$, où M parcourt l'ensemble des sous-groupes maximaux de G. Ceci achève la démonstration. ■

Le théorème suivant est connu sous le nom du **Théorème de la base de Burnside**.

Théorème 5. *Soit G un p-groupe, et soit $d(G)$ la dimension de l'espace $G/\Phi(G)$ sur $\mathbb{Z}_p$. Alors*

1. *une partie $X = \{x_1, ..., x_n\}$ engendre G si seulement si $\{\bar{x}_1, \bar{x}_2, ..., \bar{x}_n\}$ engendre $G/\Phi(G)$.*
2. *Toute partie génératrice minimale de G contient exactement $d(G)$ éléments.*

Démonstration. Si X est partie génératrice de G, alors $\bar{X}$ engendre tout quotient G/N, et en particulier $\bar{X}$ engendre $G/\Phi(G)$. Inversement, si $\bar{X} = \{\bar{x}_1, ..., \bar{x}_n\}$ engendre $G/\Phi(G)$, alors $G = \langle X, \Phi(G)\rangle$, et d'après Proposition 1.3.1, on a $G = \langle X\rangle$. Ceci montre 1).

D'autre part, Soit $X = \{x_1, ..., x_n\}$ une partie génératrice minimale de G, donc $\bar{X} = \{\bar{x}_1, ..., \bar{x}_n\}$ engendre $G/\Phi(G)$ qui est un espace vectoriel de dimension $d(G) = d$. On à $\bar{X}$ est minimal ; sinon on peut trouver $Y \subsetneq X$, tel que $\langle \bar{Y}\rangle = G/\Phi(G)$. Ceci implique $\langle Y\rangle = G$ par Proposition 1.3.1 ; mais ceci contredit la minimalité de X. D'où $\bar{X}$ est une base de l'espace $G/\Phi(G)$; par suite $|\bar{X}| = n = d(G)$.

■

Théorème 6 (Philip Hall)**.** *Soit G un p-groupe d'ordre p^n et soit $d = d(G)$.*

1. *Soit $S = \{\delta \in Aut(G), x^{-1}\delta(x) \in \Phi(G), \forall x \in G\}$; alors S est un p-groupe d'ordre au plus $|\Phi(x)|^d = p^{(n-d)d}$.*
2. *$|Aut(G)| \leq p^{(n-d)d}|GL(d,p)|$; et ainsi*

$$|Aut(G)| \leq p^{(n-d)d}(p^d - 1)(p^d - p)...(p^d - p^{d-1}).$$

3. *L'ordre d'un p-sous-groupe de Sylow de $Aut(G)$ est au plus $p^{\binom{n}{2}} = p^{n\frac{(n-1)}{2}}$.*

Démonstration. 1. Si $\delta \in Aut(G)$ considérons

$$\begin{array}{c} \tilde{\delta} : \frac{G}{\Phi(G)} \longrightarrow \frac{G}{\Phi(G)} \\ \bar{x} \longrightarrow \overline{\delta(x)} \end{array}$$

La relation $\tilde{\delta}$ définit un automorphisme de $\frac{G}{\Phi(G)}$. En effet, $\tilde{\delta}$ est bien défini, car si $\bar{x} = \bar{y}$, alors $x^{-1}y \in \Phi(G)$, alors $\delta(x)^{-1}\delta(y) \in \Phi(G)$. D'où $\overline{\delta(x)} = \overline{\delta(y)}$. Le fait que $\tilde{\delta}$ est un homomorphisme est immédiat. Soit maintenant δ^{-1} l'inverse de δ. On a pour tout $\bar{x} \in G/\Phi(G)$,

$$\tilde{\delta^{-1}} \circ \tilde{\delta}(\bar{x}) = \tilde{\delta}^{-1}(\overline{\delta(\bar{x})}) = \overline{\delta}^{-1}(\delta(x)) = \bar{x}.$$

Donc $\tilde{\delta} \in Aut(G/\Phi(G))$. Nous avons ainsi un homomorphisme de groupe

$$Aut(G) \longrightarrow Aut(G/\Phi(G))$$
$$\delta \longrightarrow \tilde{\delta}$$

Le noyau de cet homomorphisme étant l'ensemble des automorphismes δ de G, tels que $\tilde{\delta} = 1_{G\Phi(G)}$, c'est à dire $\tilde{\delta}(\bar{x}) = \bar{x}$, pour tout $\bar{x} \in G\Phi(G)$. Ceci est équivalent à $x^{-1}\delta(x) \in \Phi(x)$, pour tout $x \in G$. D'où le noyau de l'homomorphisme précédent coïncide avec S, ce qui montre que S est un sous-groupe de $Aut(G)$.

Montrons que $|S|$ divise $|\Phi(G)|^d$, et donc S est un p-groupe.

Fixons $\{x_1, ..., x_d\}$ une partie génératrice de G, et soit $B = \{(y_1, y_2, ..., y_d) \in G \,|\, y_i \equiv x_i \mod \Phi(G)\}$. Considérons l'action :

$$S \times B \longrightarrow B$$

$$(\delta, (y_1, ..., y_d)) \longrightarrow (\delta(y_1), ..., \delta(y_d))$$

Cette action est bien définie, en effet $(y_1, ..., y_d) \in B$, pour chaque i , $y_i = x_i f_i$ pour certain $f_i \in \Phi(G)$.

$$\delta(y_i) = \delta(x_i)\delta(f_i) = x_i^{'} \underbrace{f_i^{'}\delta(f_i)}_{\in \Phi(G)}, \text{ avec } f_i^{'} \in \Phi(G)$$

D'où $\delta(y_i) = x_i \mod \Phi(G)$, pour tout i.

Cette action est libre puisque si

$$(y_1, ..., y_d) = (\delta(y_1), ..., \delta(y_d))$$

alors $y_i = \delta(y_i)$, pour tout i. D'après le théorème de la base de Burnside $\{y_1, ..., y_d\}$ engendre G puisque

$$\{\bar{y}_1, ..., \bar{y}_d\} = \{\bar{x}_1, ..., \bar{x}_d\} \mod \Phi(G).$$

Mais ceci montre que δ coïncide avec l'identité sur un système générateur de G. Par suite $\delta = 1_G$.

Il résulte que pour chaque S-orbite O_i dans B, on a $|O_i| = |S|$. Donc $|B| = \sum |S| = |S|^k$, k nombre d'orbites ; mais $B = \{(x_1 f_1, ..., x_d f_d), f_i \in \Phi(G)\}$. Ainsi

$$|B| = |\Phi(G)|^d = p^{(n-d)d}.$$

2. L'ordre d'un p-Sylow dans $Aut(G)$ divise $p^{d(n-d)+\binom{d}{2}}$. En effet, on a $G/\Phi(G)$ est un espace vectoriel de dimension d sur $\mathbb{F}_p$. D'où $Aut(G/\Phi(G)) = GL(d,p)$. On a

$$\begin{aligned} |Aut(G)| &= p^{(n-d)d}|GL(d,p)| = p^{(n-d)d}(p^d-1)(p^d-p)...(p^d-p^{d-1}) \\ &= p^{(n-d)d}p^{\binom{d}{2}}(p^d-1)(p^{d-1}-1)...(p-1). \end{aligned}$$

Donc la plus grande puissance de p divisant $|Aut(G)$ est $p^{(n-d)d+\binom{d}{2}}$.

3. Montrons que

$$(n-d)d + \frac{d^2-d}{2} \leq \frac{n(n-1)}{2}$$

Cet inégalité équivaut

$$n(n-1) - (n-d)d - (d^2-d) \geq 0$$

ou encore

$$n(n-1) - 2nd + 2d^2 - d^2 + d \geq 0$$

ou aussi

$$n^2 - n - 2nd + d^2 + d \geq 0$$

ou

$$n^2 - (2d-1)n + d^2 + d \geq 0.$$

Mais, $\Delta = (2d+1)^2 - 4(d^2+d) = 1$, ce qui implique (en calculant les racines) que notre inégalité est vraie pour tout n naturel.

■

Théorème 7. *Un p-groupe G d'ordre p^n contient un sous-groupe normal abélien d'ordre p^k,avec $n \leqslant \frac{k(k+1)}{2}$*

Démonstration. Soit A sous-groupe abélien normal maximal dans G.

$$P : G \longrightarrow Aut(A)$$

$$g \longrightarrow P_g : a \longrightarrow a^g = gag^{-1}.$$

le noyau de ce morphisme étant $g \in G; P_g(a) = a, \forall a \in A.$; donc $\ker P = C_G(A)$.

On a $C_G(A) = A$, sinon $C_G(A)/A$ contient un élément de $\bar{x}$ dans le centre de G/A ; et ceci implique que $B = A\langle x\rangle$ est un sous-groupe abélien normal contenant A strictement ; ce qui contredit le fait que A est maximal. Donc

$$G/\ker P \hookrightarrow Aut(A),$$

ou

$$G/A \hookrightarrow Aut(A).$$

On a alors $|G/A| \leq$ l'ordre d'un p-Sylow de $Aut(A)$. Si $\mid A \mid = p^k$, alors d'après Théorème 6,

$$p^{n-k} \leqslant p^{\binom{k}{2}}$$

donc

$$p^n \leqslant p^{\frac{k(k-1)}{2}+\frac{2k}{2}} = p^{\frac{k(k+1)}{k}}$$

d'où

$$n \leqslant \frac{k(k+1)}{2}.$$

■

Corollaire 1.3.1. *Un p-groupe G d'ordre p^n contient un sous-groupe abélien normal d'ordre $\geqslant p^{-1+\frac{\sqrt{1+8n}}{2}} \sim p^{\sqrt{2n}}$.*

En effet, supposons que tous sous-groupe abélien normal est d'ordre $< p^{\frac{\sqrt{1+8n}-1}{2}}$.
Si A est un sous-groupe abélien normal maximal de G alors :
$\mid A \mid = p^k < p^{\frac{\sqrt{1+8n}-1}{2}}$,donc $k < \frac{\sqrt{1+8n}}{2} - 1$
mais d'après le théorème précédent on à :

$$n \leqslant \frac{k(k+1)}{2} < \frac{1}{2}((\frac{\sqrt{1+8n}-1}{2})(\frac{\sqrt{1+8n}+1}{2}))$$

$$n < \frac{1}{8}((\sqrt{1+8n}-1)(\sqrt{1+8n}+1))$$

$$n < \frac{1}{8}(1+8n-1) \Rightarrow n < n$$

contradiction.

Chapitre 2

p-GROUPES PUISSANTS

2.1 p-Groupes puissants finis

L'étude systématique des p-groupes puissants est commencée par Avinoam Mann et Alex Lubotzky dans [7] ; mais plusieurs résultats sur ces groupes sont déjà connus dans la littérature, et on peut les trouver dans les traveaux de Lazard, Arganbright, King, et autres (voir la bibliographie de [7]). Cette famille a trouvé plusieurs applications en théorie des p-groupes et pro-p groupes. Par exemple, elle joue un rôle fondamental dans la démonstration des conjectures de coclasse, et ceci est la raison pour laquelle on a choisi de traiter ces groupes. Pour simplifier l'exposition on suppose dans la suite que $p > 2$.

Définition 2.1.1. *Soit G est un p-groupe et $N \lhd G$. On dit que N est puissamment plongé dans G, si $[N, G] \leq N^p$ (si $p = 2$ on exige $[N, G] \leq N^4$).*

On dit que G est puissant s'il est puissamment plongé dans lui même.

On note $N\, p.e\, G$ si N est puissamment plongé dans G ($p.e$ est tiré de "powerfully embedded").

Proposition 2.1.1. *Si N, M sont puissamment plongé dans G , alors $[N, G]$, $N^p, [N, M]$, etNM sont puissamment plongés dans G.*

Démonstration. On va montrer que N^p $p.e$ G ; les autres cas sont similaires (voir [7, 4]).

En essayant de prouver qu'un certain sous-groupe N est puissamment plongé, on peut supposer que $[N, G, G] = 1$; car si

$$[N, G]/[N, G, G] \leq N^p[N, G, G]/[N, G, G]$$

alors $[N,G] \leq N^p[N,G,G]$ et cela implique $[N,G] \leq N^p[N,G,G,\ldots,G]$ où G apparait autant que fois qu'on veut ; et la nilpotence de G montre que le terme $[N,G,G,\ldots,G]$ devient éventuellement trivial.

Pour $[N,G]$, on peut supposer que $[N,G,G,G] = 1$. Donc $[N,G,G] \leq Z(G)$. On doit montrer $[N^p,G] \leq [N,G]^p$. Une façon de le faire est de monter que pour $x,y \in G$, l'application $\varphi : n \longrightarrow [[n,x],y]$ est un homomorphisme de $N \longrightarrow Z(G)$. On a

$$\begin{aligned}\phi(n_1n_2) &= [[n_1n_2,x],y]\\ &= [[n_1,x][n_1,x,n_2][n_2,x],y]\\ &= [[n_1,x],y]^{[n_1,x,n_2][n_2,x]}[[n_1,x,n_2][n_2,x],y]\\ &= [n_1,x,y][n_2,x,y].\end{aligned}$$

En développant $[n^p,x]$, on obtient le résultat désiré. On a donc

$$[N,G,G] \leq [N^p,G] \leq [N,G]^p$$

ce qui revient à dire que N est puissamment plongé dans G.

■

Proposition 2.1.2. *Dans un p-groupe puissant, les éléments x^{p^n}, $x \in G$ forment un sous-groupe.*

Démonstration. Voir [7] . ■

Théorème 8. *Si G est un groupe puissant alors $d(H) \leq d(G)$ pour tout $H \leq G$. avec $d(H)$ désigne le nombre minimal de générateurs de G.*

Démonstration. Voir [7] . ■

Définition 2.1.2. *Pour tout p-groupe G, et tout $d > 0$, on définit $V(G,d)$ comme l'intersection des noyaux de tous les homomorphismes de G dans $GL(d,p)$.*

Proposition 2.1.3. *(i) Si $N \lhd G$, alors $V(G,d)N/N \leq V(G/N,d)$.*

(ii) $V(G,d)$ est un sous-groupe charactéristique de G.

(iii) *Si* $N \lhd G$ *et* $d(N) \leq d$, *alors* $[N, V(G,d)] \leq \Phi(N)$. *Si en outre* $N \leq V(G,d)$, *alors* $\Phi(N) = [N, V(G,d)]N^p$.

(iv) *Soit* U *le* p*-Sylow de* $GL(d,p)$ *constitué de tous les matrices uni-triangulaires supérieures ; alors* $V(G,d)$ *est l'intersection des noyaux de tous les homomorphismes de* G *dans* U.

(v) *Les sous-groupes* $\gamma_d(G)$ *et* $\Pi_i(G)$ *pour* $p^i \geq d$ *sont tous deux contenus dans* $V(G,d)$.

Démonstration. Voir [6]

■

Théorème 9. *Soit* G *un* p*-groupe fini,* d *un entier positif, et* $N \lhd G$ *avec* $d(N) \leq d$.

(i) *Pour* p *impair, si* $N \leq V(G,d)$, *alors* $Np.eV(G,d)$.

(ii) *Pour* $p = 2$ *impair, si* $N \leq V(G,d)^2$, *alors* $Np.eV(G,d)^2$.

Démonstration. (i) Pour p impair supposons que G est un groupe avec $N \lhd G$ pour lequel le résultat est faux et supposons que $|N|$ est minimal pour ces propriétés. Soit $V = V(G,d)$. Alors $d(N) \leq d$ et $N \leq V$ et$[N,V] \not\leq N^p$. Alors Proposition 2.1.3 (iii) donne $\Phi(N) = [N,V]N^p > N^p$. En particulier, N n'est pas abélien. Soit L un sous-groupe normal de G tel que $N^p \leq L < \Phi(N)$ et $|\Phi(N) : L| = p$. Maintenant, par Proposition 2.1.3 (i) $N/L \leq V(G/L,d)$ et $[N/L, V(G/L,d)] \not\leq (N/L)^p$. Il résulte de la minimalité de $|N|$ que $L = \langle 1\rangle$ et donc $|N| \leq p^{d+1}$ et $N^p = \langle 1\rangle$. Soit M un sous-groupe maximal de N avec $M \lhd G$. Alors $|M| \leq p^d$ et ainsi $d(M) \leq d$ et maintenant la minimalité de $|N|$ implique que $[M,V] \leq M^p \leq N^p = \langle 1\rangle$. Donc M est au centre de N. Comme N/M est cyclique, il suit que N est abélien, donnant une contradiction.

(ii) Pour $p = 2$, on suppose également que G est un 2-groupe avec $N \lhd G$ pour lequel le résultat est faux et $|N|$ est minime. Soit $V = V(G,d)$. Alors $d(N) \leq d$, et $N \leq V^2$ et $[N,V^2] \not\leq N^4$. Soit L un sous-groupe normal de G tel que $N^4 \leq L < [N,V^2]N^4$ et $|[N,V^2]N^4 : L| = 2$. Encore une fois la minimalité de $|N|$ implique que $L = \langle 1\rangle$. Maintenant $N^4 = \langle 1\rangle$ et $[N,V^2]$ est d'ordre 2 et est central dans G. Aussi donc, en utilisant Proposition 2.1.3 (iii) donne $[N,V] \leq \Phi(N) = N^2$. Il en résulte que $[N,V,N] \leq [N^2,N] \leq [N^2,V^2] \leq [N,V^2]^2[N,V^2,V^2] = \langle 1\rangle$. Par conséquence, $[N,V]^2 \leq (N^2)^2 \leq N^4[N^2,N] = \langle 1\rangle$. Ces deux résultats impliquent

$$[N,V^2] \leq [N,V]^2[N,V,V] \leq [N^2,V] \leq [N,V]^2[N,V,N] = \langle 1\rangle,$$

contradiction.

2.2 Pro-p-groupes et groupe analytiques p-adiques

2.2.1 Pro-p-groupe de type fini

Définition 2.2.1. *On appelle pro-p-groupe tout groupe topologique compact G, dont les sous-groupes normaux d'indice égal à une puissance de p forment un système fondamental de voisinage de l'identité.*

On peut voir que les pro-p-groupes sont exactement les limites projectives des p-groupes finis. On réfère le lecteur à [4] ou encore à la thèse de Fètimi [5] pour une exposition détaillée.

Si X est un partie d'un pro-p-groupe, alors on note $\langle X\rangle$ le sous-groupe fermé engendré par X ; c-à-d, $\langle X\rangle$ est l'intersection de tous les sous-groupes fermés contenant X.

On dit que G est de type fini s'il existe une partie finie X de G telle que $G = \langle X\rangle$. On définit

$$d(G) = \min\{|X|, X \subseteq G, \langle X\rangle = G\}.$$

Proposition 2.2.1. *Soit G pro-p-groupe. Alors $d(G) = \dim G/\Phi(G)$, où $G/\Phi(G)$ est vu comme un espace vectoriel sur $\mathbb{Z}_p$, et $\Phi(G)$ est défini comme l'intersection des sous-groupes ouverts maximaux de G.*

Le fait que $G/\Phi(G)$ est un espace vectoriel sur $\mathbb{Z}_p$ est justifié par le résultat suivant.

Proposition 2.2.2. *Soit G un pro-p-groupe. Alors $\Phi(G) = \overline{G^pG'}$, où $\overline{G^pG'}$ désigne l'adhérence du sous-groupe G^pG'.*

Démonstration. Soit M un sous-groupe maximal ouvert de G. Comme G est compact, M est d'indice fini dans G. Pour n'importe quel sous-groupe ouvert normal N de G, tel que $N \leq M$, on a M/N est un sous-groupe maximal du p-groupe fini G/N. D'où d'après le résultat correspondant pour les p-groupes fini $M/N \lhd G/N$; ainsi $M \lhd G$ et $|G : M| = p$. Il en résultat que $G'G^p \leq M$, et comme M est fermé (car c'est le complémentaire de $\bigsqcup_{g_i \notin M} g_iM$) on a $G'G^p \leq M$.

Inversement, soit $\overline{G} = G/\overline{G^pG'}$. Comme $\overline{G}$ est un pro-p-groupe (effectivement, tout quotient d'un pro-p-groupe par un sous-groupe normal fermé est un pro-p-groupe), l'intersection des sous-groupes ouverts d'indice une puissance de p est égal à 1. Pour un tel sous-groupe $\overline{N}$, $\overline{G}/\overline{N}$ est un p-groupe fini abélien d'exposant p, d'où $\Phi(\overline{G})/\overline{N}$, c-à-d $\Phi(\overline{G}) \leq N$, et ainsi

$\Phi(\overline{G}) \leq \cap\overline{N} = 1$, donc l'intersection des sous-groupes maximaux de G contenant $\overline{G^pG'}$ est égal à $\overline{G^pG'}$. Ainsi $\Phi(G)/\overline{G^pG'}$.

■

Démonstration proposition 2.2.1. Comme le procède pour les groupes finis, une partie $X \subseteq G$, vérifie $\langle X \rangle = G$ si et seulement si $\langle X, \Phi(G) \rangle = G$.

Mais cette dernière revient à dire que l'image de X dans $G/\Phi(G)$ engendre $G/\Phi(G)$. Maintenant X est génératrice minimale de G si et seulement si sa image $\overline{X}$ est génératrice minimale de $G/\Phi(G)$; si on démontre que $G/\Phi(G)$ est fini, alors $\overline{X}$ est un base de $G/\Phi(G)$ est notre résultat découle.

Montrons que $G/\Phi(G)$ est fini. On sait que l'ordre d'un groupe abélien engendré par d'éléments et d'exposant p ne peut pas dépasser p^d. Ainsi pour tout sous-groupe ouvert $N/\Phi(G)$ de $G/\Phi(G)$ on a $|G : N| \leq p^d$. Il en résulte que $|G : \cap N| \leq p^d$ et ainsi $|G : \Phi(G)| \leq p^d$. ■

2.2.2 Pro-p-groupes puissants

Définition 2.2.2. *Soit G pro-p-groupe et N un sous-groupe ouvert de G. On dit que N est puissamment plongé dans G et on note $Np.eG$ si $[N, G] \leq \overline{N^p}$, ou $[N, G] \leq \overline{N^4}$ pour $p = 2$. Le groupe G est dit puissant si $Gp.eG$.*

Notons que $Np.eG$ si et seulement si $NH/Hp.eG/H$, pour tout sous-groupe ouvert H de G. Il résulte.

Proposition 2.2.3. *Un pro-p-groupe G est puissant si et seulement s'il est limite projective d'un système projectif de p-groupes puissants avec des morphismes surjectifs.*

Théorème 10. *Soit G un pro-p-groupe puissant, de type fini, et H un sous-groupe fermé de G. Alors $d(H) \leq d(G)$.*

Démonstration. Soit N un sous-groupe ouvert de G. Alors HN/N est un sous-groupe du p-groupe puissant G/N ; d'où $d(HN/N) \leq d(G/N) \leq d(G)$. Mais $HN/N \simeq H/H \cap N$; et $\sqcap(H \cap N) = 1$.

Donc on peut trouver N tel que $H \cap N \leq \Phi(H)$. Il en résulte $d(H/\Phi(H)) \leq dG$, mais on a vu que $d(H/\Phi(H)) = dH$. ■

Pour un pro-p-groupe G, on définit $r(G)$ le rang de G comme :

$$r(G) = \{d(H), H \text{ sous-groupe fermé de } G\}$$

On dit que G est de rang fini si $r(G) < \infty$. Le théorème précédent montre que tout pro-p-groupe puissant de type fini est de rang fini . Inversement ...

Théorème 11. *Soit G pro-p-groupe de rang fini, alors G contient un sous-groupe fermé puissant qui soit ouvert.*

Ce théorème peut être démontré en utilisant le dual du théorème 10 dans la section précédente.

Un groupe analytique p-adique est un groupe topologique qui admet une structure de variété sur le corps $\mathbb{Q}_p$ des nombres p-adiques, qui soit compatible avec la loi du groupe.
Il revient au même de dire qu'un groupe est analytique p-adique s'il satisfait les axiomes d'un groupe de Lie en remplaçant $\mathbb{R}$ par $\mathbb{Q}_p$.

M. Lazard a caractérisé ces groupes par le fait qu'il admettent un sous-groupe ouvert H qui satisfait : $H' \leq H^p$ où $H' \leq H^4$ si $p = 2$ et H est de type fini.

Avec le théorie des groupes puissants ceci revient à dire que les groupes analytiques p-adiques sont les groupes virtuellement puissants de type fini. Il en résulte du théorème 11 que :

Théorème 12. *Les pro-p-groupe analytiques p-adiques sont exactement les pro-p-groupes de rang fini.*

Chapitre 3

Les conjectures de coclasse

3.1 Classification des p-groupes

On sait d'après G. Higman et C.Sims que le nombre des p-groupes d'ordre p^n, $f(p^n)$ est donné par la formule asymptotique :

$$f(p^n) = p^{2/27^{n^2}+O(n^{8/3})}$$

Plus concrètement, les travaux récents par Besche, E.O'brien et B.Eick ont montré que

$$f(2^8) = 59092$$

$$f(2^9) = 10494213$$

$$f(2^{10}) = 49487365422$$

Le nombre des p-groupes d'ordre p^n augmente dramatiquement avec n, ce qui rend une approche pour la classification des p-groupes au sens classique impossible.

En 1980, C.Leedham-Green et M.Newman ([6]) on proposé la notion de coclasse comme un invariant pour classifier les p-groupes. Le programme est commencé par cinq conjectures qu'on va annoncer ci-dessous ; ces conjectures sont inspirés par le travail de N.Blackburn sur les p-groupes de classe maximale (qui peut être définis aussi comme les p-groupes de coclasse 1), ainsi que le travail successeur sur ces p-groupes par C.Leedham-Green et S.Mckay.

3.2 Les Conjectures de coclasse

On commence par définir la coclasse d'un p-groupe. Celle-à est égale pour un groupe d'ordre p^n et de classe c à $n-c$.

Conjecture A

Il existe un entier $f(p,r)$, tel que tout p-groupe de coclasse r posséde un sous-groupe normal N de classe au plus 2 et d'indice au plus $f(p,r)$.

Conjecture B

Il existe un entier $g(p,r)$, tel que tout p-groupe de coclasse r est résoluble de longuer dérivée au plus $g(p,r)$.

Proposition 3.2.1. *Conjecture A implique conjecture B.*

Démonstration. Soit G un p-groupe de coclasse r. Donc il existe un sous-groupe normal N de G, tel que $|G/N| \leq f(p,r)$. Ainsi la longueur dérivée de G/N est au plus $f(p,r)$; c-à-d, $(G/N)^{(f(p,r))} = 1$, ou encore $G^{(f(p,r))} \leq N$. Mais N est nilpotent de classe au plus 2, ainsi la longueur dérivée de N est au plus 2, $G^{(f(p,r)+2)} = 1$. Prenons par exemple $g(p,r) = f(p,r)+2$ que G est de longueur dérivée $\leq g(p,r)$. ce qui implique. ■

Pour annoncer la conjecture C, on va étendre la définition de coclasse au pro-p-groupes. Soit G un pro-p-groupe, et $\gamma_n(G)$ sa suite centrale descendante. On dit que G est de coclasse r, s'il existe un $k \in \mathbb{N}^*$, tel que $G/\gamma_n(G)$ soit un p-groupe (fini) de coclasse r, pour tout $n \geq k$.

Conjecture C

Tout pro-p-groupe de coclasse fini est résoluble.

Proposition 3.2.2. *La conjecture B implique Conjecture C.*

Démonstration. Soit G un pro-p-groupe de coclasse r. Si N est un sous-groupe ouvert de G, alors G/N est un p-groupe fini, d'où G/N est nilpotent, ce qui implique que $\gamma_n(G/N) = 1$, pour certain n. Il revient au même de dire que $\gamma_n(G) \leq N$, pour certain N. Comme les sous-groupes ouverts N forment un système fondamental de voisinage de l'identité, on a $\bigcap_n \gamma_n(G) = 1$.

D'autre part, $\exists k > 0$, tel que $G/\gamma_n(G)$ est de coclasse r pour tout $n \geq k$. Par la conjecture B, on a $G^{(g(p,r))} \leq \gamma_n(G)$, pour tout $n \geq k$. Ainsi

$$G^{(g(p,r))} \leq \prod_{n \geq k} \gamma_n(G) = 1. \text{ D'où } G \text{ est résoluble.}$$

■

Conjecture D

Pour tout p et r, il existe seulement un nombre fini de pro-p-groupes de coclasse r.

Conjecture E

Pour tout p et r, il y a seulement un nombre fini de pro-p-groupes résolubles de coclasse r.

Notons que dans cette thése les pro-p-groupes sont toujours supposés infinis.

La conjecture D implique évidement la conjecture E, et en vertu de la conjecture B, si Conjecture E est vraie, alors conjecture D est identique à B.

La conjecture E est démontré par Leedham-Green, S.Mckay et W.Pleskin en 1986, en atilisant la cohomologie, la structure des sous-groupes de Sylow du groupes linéaire général et beaucoup de calculs.

Ce qu'on a démontré ci-dessus montrer que la conjecture A avec ce dernier résultat de Leedham-Green et Al implique toutes les conjectures qui restent ; donc tout revient à prouver la conjecture A. Il y a au moins trois approcher pour démontrer cette conjecture, dont la plus élémentaires (mais encore assez technique) et la plus effective est celle donné par A.Shalev [9]. Dans la dernière section de ce chapitre le lecteur trouve un sketch pour cette preuve.

3.3 Graphe associé au p-groupes d'une classe donnée

Fixons un nombre premier p, et un entier positif r.

Soit $\Gamma(p,r)$ l'ensemble de tout les p-groupes de coclasse r.(On identifie tous les p-groupes isomorphes, donc $\Gamma(p,r)$ est l'ensemble des classes d'isomorphismes des p-groupes de coclasse r.)

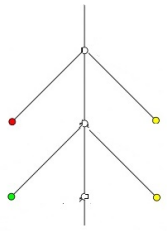
Définissons une structure de graphe sur $\Gamma(p,r)$ comme suit : Les sommets du graphe sont les éléments de $\Gamma(p,r)$, et si H, K sont deux sommet, il y a une arrête orientée (ou un arc) $H \longrightarrow K$ s'il existe un épimorphisme de H dans K dont le noyau est d'ordre p.

Notons ici comme H et K ont la même coclasse, pour tout épimorphisme $\varphi : H \longrightarrow K$, avec $|ker\varphi| = p$ on a $ker\varphi = \gamma_c(H)$, où c est la classe de H.

On a $H/ker\varphi \simeq K$, donc $|H| = p|K|$. Mais $|H| = p^{c+r}$, ainsi $|K| = p^{(c-1)+r}$, mais comme K est de coclasse r, il en résulte que K est de classe $c-1$, d'où $\gamma_c(H/ker\varphi) = 1$ et ainsi $\gamma_c(H) \leq ker\varphi$, et comme $\gamma_c \neq 1$, on a $\gamma_c(H) = ker\varphi$.

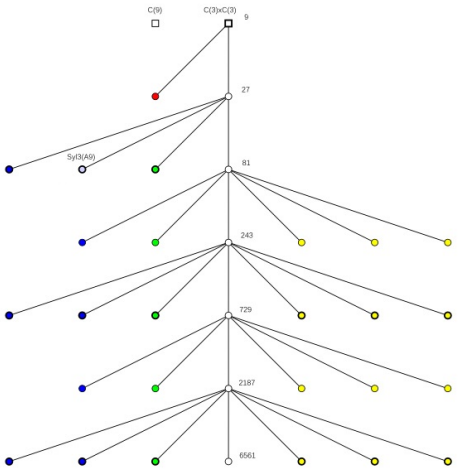
D'après le travail de Blackburn sur les 2-groupes et les 3-groupes de coclasse 1, on peut représenter $\Gamma(2,1)$, et $\Gamma(3,1)$ comme suit :

2-groupes de coclasse 1



où pour chaque n, le sommet "." représente le groupe dihedral D_2n, et les autres sommets sont les groupes Q_{2^n} et SD_{2^n} (Les quaternions généralisés, et les groupes semi-dihedrals).

3-groupes de coclasse 1



Pour l'interprétation de ce graphe, voir par exemple [6].

La conjecture D implique que le graphe $\Gamma(p,r)$ possède seulement un nombre fini de chemins

infinis maximaux. Si on a un chemin infini maximal dans $\Gamma(p,r)$

$$\longrightarrow H_n \longrightarrow ... \longrightarrow H_2 \longrightarrow H_1$$

Alors les H_n avec leurs épimorphismes définissent un système projectif de p-groupe ; donc on peut construire le groupe $\varprojlim H_n$, Pour chaque k, on a un quotient $\varprojlim H_n/\gamma_k \simeq H_k$ qui est un p-groupe de coclasse r, ainsi $\varprojlim H_n$ est un pro-p-groupe de coclasse r.
Inversement, si G est un pro-p-groupe de coclasse r, alors il existe $m \in \mathbb{N}^*$ telle que : $G/\gamma_n(G)$ est un p-groupe de coclasse r pour tout $n \geq m$. Nous avons ainsi une suite de p-groupes

$$... \longrightarrow G/\gamma_{n+i}(G) \longrightarrow ... \longrightarrow G/\gamma_{n+1}(G) \longrightarrow G/\gamma_n(G)$$

qui forme un chemin infini dans le graphe $\Gamma(p,r)$.

3.4 Sketch de la démonstration du conjecture A

On entend ici la preuve donnée par Shalev [9]. Notons que la démonstration pour $p > 2$ est un peu différente de celle pour $p = 2$; mais on ne perd pas des grandes choses si on suppose que p est impair.

I.

Soit G un p-groupe qui opére sur un espace vectoriel V défini sur un corps de caractéristique p. On dit que G opère unisériellement sur V, si pour tout sous-espace G-invariant U de V, on a $\dim(U/[U,G]) = 1$. Cette définition peut être adaptée aisément pour les algèbres de Lie (c-à-d, on suppose que G est une algèbre de Lie qui opère sur V ; dans ce cas l'action doit vérifier $[x,y]v = x(yv) - y(xv), \forall x,y \in G, \forall v \in V$). Idem, si G opère sur un p-groupe fini N, alors on dit que cette action est unisérielle si pour chaque sous-groupe G-invariant H de N, on a $|H : [H,G]| = p$. *Soit G un p-groupe de coclasse r. Alors G opère unisèriellement sur $\gamma_n(G)$, où $n = 2p^{r-1}$. De plus si on pose $k = p^r$, et $d = d(\gamma_k(G))$, alors $\gamma_i(G)^p = \gamma_{i+d}(G)$, pour tout $i \geq k$.*

Si $N \lhd G$, et chaque sous-groupe normal $H \leq N$ est puissamment plongé dans N, c-à-d : $[H,N] \leq H^p$; on dit que H est fortement héréditaire puissant.

L'étape suivante consiste à démontrer

Proposition 3.4.2. *Si G est un p-groupe de coclasse r, et $|G| \geq p^{2p^r+r}$. Alors pour $m = p^{r-1}(p-1)$, le sous-groupe $\gamma_m(G)$ est fortement héréditaire puissant, et $d(\gamma_m) = (p-1)p^s$, pour certain $0 \leq s \leq r-1$.*

Notons que sous les notations de Proposition 3.4.2, il résulte de la proposition 3.4.1, que G opère unisèriellement sur $\gamma_m(G)$ et $\gamma_i(G)^p = \gamma_{i+p}(G)$, pour $i \geq m$.

II. Réduction du problème au algèbres de Lie.

Notons d'abord que si G est p-groupe de coclasse r tel que $|G| < p^{2p^r+r}$, alors conjecture A est vraie pour G. Il suffit par exemple de prendre $N = 1$. Donc désormais, on doit supposer que $|G| \geq p^{2p^r+r}$, ce qui permet d'appliquer Proposition 3.4.2. On va appliquer les notations de cette pro-p.

Si c est la classe de nilpotence de G, alors on a

$$|\gamma_i(G) : \gamma_{i+1}(G)| = p, \text{ pour } m \leq i \leq c.$$

Ceci résulte du fait que $\gamma_m(G)$ est un G-groupe unisériel. Il en résulte que $\gamma_i(G)/\gamma_{i+1}(G)$ est un $\mathbb{F}_p$-espace vectoriel, et ainsi on peut former le $\mathbb{F}_p$-espace vectoriel

$$M = \bigoplus_{i \leq m} M_i, \text{ où } M_i = \gamma_i(G)/\gamma_{i+1}(G).$$

Définissons le degré de commutativité de G comme le plus grand entier satisfaisant

$$[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j+l}(G).$$

pour tous $i, j \geq m$. Si $\gamma_m(G)$ est abélien, on pose $l = \infty$.

Si $l = \infty$, on considére M comme une $\mathbb{F}_p$-algèbre de Lie abélienne (trivial) et si $l < \infty$ on définit un crochet de Lie sur M par :

$$[x\gamma_{i+1}, y\gamma_{j+1}] = [x, y]\gamma_{i+j+l+1}$$

et on étend la définition au éléments non homogènes par bilinèarité.

D'autre part, on a l'algèbre de Lie classique $L = \bigoplus_{i \geq 1} \gamma_i(G)/\gamma_{i+1}(G)$ avec le produit insuel $[x\gamma_{i+1}, y\gamma_{j+1}] = [x, y]\gamma_{i+j+1}$.

Soit $\mathfrak{R}$ le quotient de L par l'idéal pL. Ainsi $\mathfrak{R} = \bigoplus_{i \geq 1} \mathfrak{R}_i$, où $\mathfrak{R}_i = L_i/pL_i$ et $L_i = \gamma_i(G)/\gamma_{i+1}(G)$.

Notons que $\mathfrak{R}_i = M_i$ au moins pour $i \geq m$ proposition 3.4.2 implique que :

(a) L'algèbre de Lie $\mathfrak{R}$ opère sur l'espace vectoriel M, et cette action vérifie

$$M_i\mathfrak{R}_j \subseteq M_{i+j}, \text{ pour } i \geq m \text{ et } j \geq 1.$$

(b) L'action de $\mathfrak{R}$ sur M est unisérielle.

Par proposition 3.4.1, si $x \in \gamma_i(G)$, alors $x^p \in \gamma_{i+d}(G)$, pour tout $i \geq m$. Ainsi nous avons une application

$$\tau : M \longrightarrow M$$

définie sur les éléments homogènes de M par :

$$\tau(x\gamma_{i+1}) = x^p\gamma_{i+d+1}.$$

On doit montrer de résultat suivant :

Proposition 3.4.3. *1)* $\tau : M \longrightarrow M$ *est linéaire.*

2) $\tau(M_i) = M_{i+d}$*, pour* $i \geq m$*.*

3) $[\tau(x), y] = \tau[x, y]$*, pour tous* $x, y \in M$*.*

4) τ *commute avec l'action de* $\mathfrak{R}$*.*

$$\tau(x)y = \tau(xy)$$

(il revient au même de dire que τ *est un homomorphisme de* $\mathfrak{R}$*-module)*

Théorème 13. *Pour avoir la conjecture A, il suffit de montrer que* $2l \geq c - 3m - 3d + 7$*.*

Démonstration. Soit $t = 2(p^r - p^{r-1} - 1) = 2(m-1)$. On a

$$\gamma_3(\gamma_t(G)) = [[\gamma_t, \gamma_t], \gamma_t] = [\gamma_{2t+l}, \gamma_t] = \gamma_{3t+2l}$$

On

$$3t + c - 3m - 3d + 7 = 6m - 6 - c - 3m - 3d - 7 = c + 3m - 3d + 1 \geq c + 1$$

D'où $\gamma_3(\gamma_t(G)) = 1$, ce qui revient à dire que $\gamma_t(G)$ est nilpotent de classe au plus 2, et on a d'autre part $G/\gamma_t(G)$ est nilpotent de classe $t-1$ et de coclasse $\leq r$, ainsi l'ordre de $G/\gamma_t(G)$ ne dépasse pas $p^{(2(p^r-p^{r-1}-1)+r-1)}$. Donc on peut prendre $f(p,r) = p^{(2(p^r-p^{r-1}-1)+r-1)}$ ■

Dans la suite on doit supposer pour l'absurde que

$$2l < c - 3m - 3d + 7.$$

À partir de M et de l'application τ définie dans proposition 3.4.3, on va construire une algèbre de Lie $\widetilde{M}$ qui est libre en tant que $\mathbb{F}_p[\tau]$-module, et qui est de rang d.

D'abord considérons un $\mathbb{F}_p[\tau]$-module libre sur les générateurs $x_m, ..., x_{m+d-1}$ (on peut supposer que chaque $0 \neq x_i \in M_i$, et ainsi $x_m, ..., x_{m+d-1}$ engendre M entant que $\mathbb{F}_p[\tau]$-module .)

Pour chaque $m \leq i, j \leq m + d$, on définit

$$[x_i, x_j] = \lambda_{ij}\tau^n x_k$$

où λ_{ij}, n et k sont définis comme suit :

Si on considère x_i et x_j comme éléments de M, on a $[x_i, x_j] \in M_{i+j+l}$. Notre hypothèse sur l, implique que $i + j + l \leq c$, et ainsi $M_{i+j+l} \neq 1$.

D'où $[x_i, x_j] = \lambda_{ij}x_{i+j+l}$ pour certain $\lambda_{ij} \in \mathbb{F}_p$. D'après proposition 3.4.3, $x_{i+j+l} = \tau^n(x_k)$, pour certains $m \leq k < m + d$ et $n \geq 0$.

Idem on doit regarder $\widetilde{M}$ comme un $\mathfrak{R}_1$-module (à droite comme M). Pour ceci, si $y \in \mathfrak{R}_1$, on pose $x_i y = \mu_i x_{i+1}$, pour certains $m \leq i < m + d - 1$.

et $x_{m+d-1}y = \mu_{m+d-1}\tau(x_m)$ pour des μ_i convenable.

Avec ces définitions on obtient

(i) $\widetilde{M}$ est une algèbre de Lie qui est libre de rang d entant que $\mathbb{F}_p$-module.

(ii) Comme une algèbre de Lie sur $\mathbb{F}_p$, $\widetilde{M} = \bigoplus_{i \geq m} \widetilde{M}_i$, où $\dim_{\mathbb{F}_p} \widetilde{M}_i = 1$, et $[\widetilde{M}_i, \widetilde{M}_j] = \widetilde{M}_{i+j+l}$.

(iii) $\widetilde{M}$ est un $\mathfrak{R}_1$-module unisériel.

(iv) $\tau^n(\widetilde{M}) \subseteq \widetilde{M}'$, en particulier $|\widetilde{M} : \widetilde{M}'| < \infty$.
(ici $\widetilde{M}'$ est l'algèbre dériveé de $\widetilde{M}$)

On considère maintenant le corps des fractions $\mathbb{F}_p(\tau)$ et $\mathbb{F}$ sa clôture algébrique, et on définit $\mathfrak{g} = \widetilde{M} \otimes_{\mathbb{F}_p[\tau]} \mathbb{F}$ et $U = \mathfrak{R}_1 \otimes_{\mathbb{F}_p} \mathbb{F}$.

Conséqunce.

(1) L'algèbre $\mathfrak{g}$ est parfaite ; c-à-d, $L' = L$.

(2) $\mathfrak{g}$ possède une dérivation D telle que : $D^{p-1} = 1$.

III.

L'étape finale consiste à prouver

Théorème 14. *Si* $\mathfrak{g}$ *est une algèbre de Lie de dimension finie sur un corps de caractéristique* p*, et si* $\mathfrak{g}$ *possède une dérivation* D *qui satisfait* $D^{p-1} = 1$ *; alors* $\mathfrak{g}$ *est nilpotent.*

Pour ce théorème on démontre que $\mathfrak{g}$ est gradué par $\mathbb{Z}_p$, ou les composantes homogènes pour cette graduations sont les sous-espaces propres associés à D. Finalement, on utilise une version du théorème d'Engel (on suppose seulement que les éléments homogènes sont nilpotents) pour déduire que $\mathfrak{g}$ est nilpotent.

Conclusion

Il y a une deuxième génération de conjectures de coclasse. D'abord on est loin de bien maitriser le matériel discuté dans ce mémoire ; donc on doit élaborer ce matériel plus attentivement, et après on doit passer à ces conjectures.

Bibliographie

[1] Y. Berkovich, Groups of prime power order, vol. 1, Walter de Gruyter, 2008.

[2] Y. Berkovich and Z. Janko, Groups of prime power order, vol. 2, Walter de Gruyter, 2008.

[3] Y. Berkovich and Z. Janko, Groups of prime power order, vol. 3, Walter de Gruyter, 2011.

[4] J. Dixon, M. du Sautoy, A. Mann, D. Segal, Analytic pro-p Groups, second ed., Cambridge Univ. Press, 1999.

[5] M. Fétimi, Groupes de Shafarevich-Tate, Thèse de Master, UKMO (2016).

[6] C. R. Leedham-Green and S. McKay, The structure of Groups of prime power order, London Math. Soc. Monogr., Oxford University Press, Oxford, 2002.

[7] A. Lubotzky and A. Mann, *Powerful p-groups. I. Finite groups.*, J. Algebra **105**, 484-505 (1987)

[8] D. J. S. Robinson, A Course in the Theory of Groups, 2nd ed. New York : Springer-Verlag, 1995.

[9] A. Shalev (1994) The structure of finite p-groups : effective proof of the coclass conjectures. Invent. Math. 115, 315-345.

[10] A. Shalev and E. I. Zel'manov (1992) Pro-p groups of finite coclass. Math. Proc. Camb. Phil. Soc. Ill , 417-421.

Abstract

This work is a brief introduction to the coclass theory of p-groups. We give a sketch of the proof of the strongest of the coclass conjectures, which is based on the theory of powerful p-groups and Lie methods. Related topics as analytic pro-p-adic and pro-p-groups of finite coclass are also discussed.

Keywords: p-groups, coclass, pro-p groups, Lie algebras.

Résumé

Ce travail est une brève introduction de la théorie de coclasse des p-groupes. On présente une esquisse de la démonstration de la plus forte conjecture basée sur les p-groupes puissants et les méthodes de Lie. Notamment on a discuté des sujets relatifs comme les groupes analytiques p-adiques et les pro-p-groupes de coclasse fini.

Mot clés: p-groupes , coclasse , pro-p-groupe- Algèbre de Lie.

ملخص

هذه المذكرة عبارة عن مقدمة سريعة لنظرية **صف التملم لـ** p– **زمرة** .**وقد قدمنا لمحة عن** برهان اقوى مخمنة في هذه النظرية ، بالإعتماد على p – **زمرة** القوية و طرق "لي".

على غرار ذلك ناقشنا مواضيع مختلفة متعلقة بها مثل الزمرة التحليلية p – أدية **و** p – **زمرة** المميزة **لـ اصناف تملم** منتهية .

كلمات مفتاحية : p – **زمرة** ، **صف التملم** ، p – **زمرة** المميزة ، **جبر لي** .