MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA

RECHERCHE SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS – SETIF 1

THESE

Présentée à la Faculté des Sciences
Département de Mathématiques

Pour l'obtention du diplôme de

DOCTORAT EN SCIENCES

Option: ALGEBRE

Par

Mr : Yassine GUERBOUSSA

THEME

SUR L'EXISTENCE D'UN AUTOMORPHISME NON INTERIEUR D'ORDRE p D'UN p-GROUPE NON ABELIEN FINI

Soutenu le 12/01/ 2016 devant le Jury composé de :

Naceurdine Bensalem	Pr	Université Sétif 1	Président
Bounabi DAOUD	Pr	Université Sétif 1	Rapporteur
Alireza ABDOLLAHI	Pr	Université d'Ispahan (Iran)	Co-rapporteur
Nadir TRABELSI	Pr	Université Sétif 1	Examinateur
Lemnouar NOUI	Pr	Université de Batna	Examinateur
Abdelhafid BADIS	MC	Université de Khenchla	Examinateur

Table des matières

Je dédie ce travail à la mémoire de mon ami et mon professeur Miloud Reguiat.

Remerciements

Dans les derniers mois de l'année 2010, j'étais en train de chercher un encadreur pour m'inscrire en doctorat. J'étais un peu frustré après des tentatives non fructueuses dans quelques universités ; et enfin j'ai rencontré le Professeur Nadir Trabelssi dans son bureau à Sétif. J'ai compris qu'il était chargé et qu'il ne pouvait pas prendre un autre étudiant en charge, et j'ai compris qu'il va parler à un collègue à mon sujet. Quelques jours après, j'ai reçu un appel téléphonique du Professeur Bounabi Daoud ; je me souviens de notre discussion qu'il m'avait accepté de travailler avec lui. La théorie des groupes est un domaine formidable, que j'ignorais presque totalement, et je pense que ça restera le cas sans la bienveillance des Professeurs Trabelsi et Daoud ; je suis vraiment reconnaissant envers eux.

Je voudrais remercier cordialement mon encadreur le Professeur Daoud Bounabi pour sa flexibilité, sa disponibilité et pour toute l'aide qu'il m'a donné sur tous les niveaux.

Je remercie le Professeur Alireza Abdollahi pour de nombreuses discussions durant la réalisation de ce travail et pour avoir accepté d'être mon co-encadreur.

Je remercie chaleureusement le Professeur Nacerdine Bensalem d'avoir accepté de présider le jury, ainsi que les Professeurs Nadir Trabelsi, Lemnouar Noui et Abdelhafed Badis pour avoir accepté de participer au jury, et pour la lecture attentive de cette thèse.

Plusieurs résultats dans cette thèse sont émergés de ma collaboration avec mes collégues Miloud Reguiat est Mohammed. T. Benmoussa. Je les remercie chaleureusement pour tout le temps qu'on a passé ensemble. Je remercie également tous les membres du département de mathématiques (comprenant Mohammed Benbitour) de l'université de Ouargla.

Je remercie cordialement le Professeur Andrea Caranti qui m'a invité à l'université de Trento pour l'ambiance familiale et professionnelle qu'il m'avait fourni.

Je remercie aussi tous les mathématiciens avec qui j'ai eu l'occasion de discuter la théorie des groupes.

Finalement, je remercie toute ma famille, surtout ma mère et ma femme pour leur soutien.

Notation et terminologie

Soit G un groupe.

Comme règle, p désigne un nombre premier.

$\lceil x \rceil$ le plus petit majorant entier du nombre réel x.

$\mathrm{Aut}(G)$ le groupe d'automorphismes de G. Si $\sigma, \tau \in \mathrm{Aut}(G)$, le produit $\sigma\tau$ est égal au composé $\tau \circ \sigma$. L'image de $x \in G$ par σ sera notée $\sigma(x)$ ou x^σ.

Un automorphisme $\sigma \in \mathrm{Aut}(G)$ est dit intérieur s'il est de la forme $\sigma(x) = g^{-1}xg$, pour un certain $g \in G$. On dit aussi que σ est l'automorphisme intérieur induit par g.

$\mathrm{Inn}(G)$ le groupe des automorphismes intérieurs de G.

$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ est appelé, par abus de langage, le groupe des automorphismes extérieurs de G.

Pour un sous-groupe N de G, $\mathrm{Aut}_N(G)$ désigne le groupe des automorphismes σ de G qui vérifient $x^{-1}\sigma(x) \in N$, pour tout $x \in G$.

$\mathrm{Aut}_z(G)$ désigne $\mathrm{Aut}_{\mathrm{Z}(G)}(G)$. Ceci est par définition le groupes des automorphismes centraux de G.

Pour $x, y \in G$, le commutateur $[x, y]$ est égal à $x^{-1}y^{-1}xy$.

Si $x_1, x_2, \ldots x_n \in G$, $n \in \mathbb{N}^*$, le commutateur (normé à gauche) $[x_1, x_2, \ldots, x_n]$ est défini par récurrence : $[x_1] = x_1$ et $[x_1, x_2, \ldots, x_n] = [[x_1, x_2, \ldots, x_{n-1}], x_n]$.

$[x,_n y] = [x, y, \ldots, y]$, où y apparait n fois.

Pour deux parties non-vides X et Y de G, $[X, Y]$ est le sous-groupe engendré par tous les commutateurs $[x, y]$, $x \in G$ et $y \in G$.

Pour des parties non-vides $X_1, X_2, \ldots X_n$, $n \in \mathbb{N}^*$, $[X_1, X_2, \ldots, X_n]$ est défini par récurrence : $[X_1] = X_1$ et $[X_1, X_2, \ldots, X_n] = [[X_1, X_2, \ldots, X_{n-1}], X_n]$.

$\mathrm{C}_G(X)$ le centralisateur de la partie $X \subseteq G$; c'est à dire l'ensemble des éléments de G qui commutent avec tous les éléments de X.

$\mathrm{Z}(G) = \mathrm{C}_G(G)$ est le centre de G.

$Z_i(G)$ les termes de la suite centrale ascendante de G.

$\gamma_i(G)$ les termes de la suite centrale descendante de G.

$\lambda_i(G)$ les termes de la suite p-centrale descendante de G.

$G^{(i)}$ les termes de la suite dérivée de G.

$\Phi(G)$ le sous-groupe de Frattini de G.

G^n le sous-groupe engendré par les éléments de la forme x^n, $x \in G$.

$\Omega_i(G)$ le sous-groupe engendré par les éléments de G d'ordre divisant p^i (p un nombre premier fixé).

$\Omega(G)$ désigne $\Omega_1(G)$ lorsque $p \geq 3$; et lorsque $p = 2$, $\Omega(G)$ désigne $\Omega_2(G)$.

Tous les anneaux considérés ici sont associatifs, mais pas forcément unitaires.

Pour un anneau A,

A^+ désigne le groupe additif de A.

A° désigne le groupe adjoint de A.

Le produit de deux idéaux I et J de A est noté IJ.

Si I est un idéal de A, I^n désigne le produit de n copies de I.

A est dit *nilpotent* si $A^{n+1} = 0$ pour certain $n \in \mathbb{N}$. Dans ce cas, la classe de nilpotence de A est le plus petit n qui vérifie cette propriété.

On écrit $\Omega_i(A)$ au lieu de $\Omega_i(A^+)$.

$\mathfrak{A}(A)$ désigne l'annihlateur de A, qui est l'ensemble des éléments $x \in A$ tels que $xA = Ax = 0$.

Chapitre 0

Introduction

Dans cette thèse, la lettre p désigne un nombre premier. Un *p-groupe* est un groupe G dans lequel l'ordre de tout élément est une puissance de p. Si G est fini, cela revient à dire que l'ordre de G est une puissance de p.

Désormais, par un p-groupe on entend un p-groupe fini.

Les p-groupes occupent une place centrale dans la théorie des groupes finis. Le célèbre théorème de Sylow affirme l'existence des p-sous-groupes d'ordre maximal dans tout groupe fini ; en d'autre terme, si G est un groupe d'ordre $p^n m$, où $n, m \in \mathbb{N}$, et m n'est pas divisible par p, alors G contient un sous-groupe d'ordre p^n (p-sous groupe de Sylow). Une autre propriété qui n'est pas moins importante est que G opère transitivement sur l'ensemble de ses p-sous-groupes de Sylow. Aussi, la structure d'un groupe fini est intimement liée au plongement de ses p-sous-groupes : l'analyse p-locale, ou encore l'étude des normalisateurs des p-sous groupes non-triviaux, a joué un rôle décisif dans la classification des groupes simples finis. De plus, plusieurs problèmes sur les groupes finis peuvent être réduis à des questions sur les p-groupes, comme montrent par exemple le problème restreint de Burnside (voir [42]), ou le problème d'énumérations des groupes finis (voir [65]).

Ci-dessus, on a exprimé une tradition qui considère les p-groupes en premier lieu comme un moyen d'étudier les autres groupes. La théorie des p-groupes est concernée par les p-groupes, plutôt, pour eux mêmes. Le problème fondamental dans cette théorie, ainsi que dans la théorie des groupes finis en général, est de produire une classification de tous les p-groupes. Le nombre $f(p, m)$ des p-groupes d'un ordre donné p^m, vérifie d'après un résultat de G. Higman et C. Sims (voir [15]),

$$f(p, m) = p^{\frac{2}{27}m^3 + O(m^{8/3})}.$$

Ceci implique que le nombre des p-groupes d'ordre donné est très grand (en revanche, il y a au plus deux groupes simples d'ordre donné !). Ce phénomène rend la classification des p-groupes au sens classique (pratiquement) impossible, et donc notre attention doit se diriger vers des problèmes plus parti-

culiers, afin de mettre un ordre dans l'univers des p-groupes (de la meilleure façon possible).

Les efforts continus pour comprendre les p-groupes, ont produit des théories particulières, et bien élaborées, de quelques familles de p-groupes, comme la théorie des *p-groupes réguliers* (voir [41] ou aussi [11, §7]), la théorie des *p-groupes puissants* (*powerful p-groups*) (voir [25] et [11, §26]), et la théorie des *p-groupes de classe maximale* (voir [58] et [11, §9]). Cette dernière a motivé le développement de *la théorie de coclasse* (voir [58]).

La *coclasse* d'un p-groupe d'ordre p^n et de classe c est égale à $n - c$. Le plus fort entre les théorèmes de coclasse affirme qu'il existe un entier $f(p, r)$, tel que tout p-groupe de coclasse r possède un sous-group normal de class au plus 2 est d'indice au plus $f(p, r)$. La notion de coclasse peut être étendue naturellement au pro-p groupes ; on dit qu'un pro-p groupe (toujours supposé infini) G est de coclasse r, s'il existe $n \in \mathbb{N}$, tel que $G/\gamma_i(G)$ est un p-groupe (fini) de coclasse r, pour tout $i \geq n$. Il revient au même de dire que G est une limite projective de p-groupes de coclasse r. Le théorème précédent implique que tout pro-p groupe de coclasse r est résoluble. En effet, on a $G^{(f(p,r)+2)} \leq \gamma_i(G)$, pour tout i suffisamment grand, ainsi $G^{(f(p,r)+2)} \leq \cap_i \gamma_i(G) = 1$. Donc G est résoluble de longueur dérivée au plus $f(p, r) + 2$ (cette borne peut être améliorée sensiblement). Ce dernier résultat implique qu'il y a seulement un nombre fini (à un isomorphisme près) de pro-p groupes de coclasse r (voir [58]).

Pour p et r fixés, on peut considérer les p-groupes de coclasse r (à isomorphismes près) comme les sommets d'un graphe orienté $\Gamma(p, r)$: il y a un arc $H \to K$, entre les deux sommets H et K, s'il existe un épimorphisme de H dans K, dont le noyau est d'ordre p. Maintenant, pour chaque chemin infini dans $\Gamma(p, r)$

$$... \to H_i \to ... \to H_2 \to H_1$$

on a le pro-p groupe de coclasse r, $\varprojlim H_n$. Inversement un pro-p groupe G de coclasse r détermine un chemin infini

$$... \to G/\gamma_{t+i}(G) \to ... \to G/\gamma_{t+1}(G) \to G/\gamma_t(G)$$

dans $\Gamma(p, r)$, où t est un entier positif suffisamment grand. Donc le dernier résultat mentionné dans le paragraphe précédent revient à dire que le graphe $\Gamma(p, r)$ contient seulement un nombre fini de chemins infinis.

Des résultats plus récents suggèrent que les graphes $\Gamma(p, r)$ possèdent certains types de périodicité. La théorie souhaite de réduire la classification des p-groupes pour chaque coclasse à un nombre fini de calculs, et en fait, ceci est démontré pour les 2-groupes ; mais ces calculs restent non-effectifs pour les 2-groupes les plus abordables. De plus il semble, dans ce contexte, que les p-groupes les plus accessibles sont ceux qui ont une petite coclasse ; mais la classification des p-groupes de coclasse 1 (ou les p-groupes de classe

maximale) n'est achevée que pour $p = 2, 3$ (avant le développement de la théorie de coclasse).

Il semble que les méthodes actuelles ne sont pas assez confortables pour aborder le grand nombre de problèmes sur les p-groupes. La théorie continue à comprendre de plus en plus des méthodes provenant des autres disciplines, algèbres de Lie, pro-p groupes, théorie des nombres, géométrie algébrique, algèbre homologique, analyse complexe, théorie des modèles, informatique...

Il est commun de considérer les groupes comme des mesures de symétrie. Dans un sens étroit, si G est un groupe qui opère sur un ensemble X, et $S \subset X$, les symétries de S sont les éléments de G qui laissent S invariant. Dans un sens plus large, dans une catégorie quelconque, nous avons la notion d'*isomorphisme* ; et si X est un objet de cette catégorie, les isomorphismes de X dans lui-même forment un groupe, qui est naturellement le groupe de symétrie de l'objet mathématique X. De ce point de vue, le groupe d'automorphismes d'un groupe ambiant G, est le groupe de symétrie de G ; ainsi l'étude des automorphismes des groupes n'est que l'étude des *"symétries des symétries"*. Regardant la littérature, on peut distinguer plusieurs aspects dans l'étude des automorphismes des p-groupes, et voici une description de certains de ces aspects :

Dans [26], B. Eick, C. R. Leedham-Green, et E. A. O'Brien ont élaboré un algorithme pour calculer le groupe d'automorphismes d'un p-groupe donné G ; cet algorithme est implémenté par B. Eick et E. A. O'Brien dans le package AutPGrp de GAP (voir [28]). Pour plus d'informations sur d'autres travaux dans ce contexte algorithmique, le lecteur est référé à l'introduction de [26]. La thèse de G. Helleloid ([44]), contient un survol sur les automorphismes des p-groupes, dans lesques on peut trouver une description détallée des automorphismes de certaines familles de p-groupes, comprenant principalement les p-groupes extra-spéciaux (voir aussi [78]), et les sous-groupes unipotents maximaux des groupes de Chevalley. Plus récemment, il y a eu des tentatives pour déterminer toutes les structures possibles de $\mathrm{Aut}(G)$ lorsque G est minimal non-abélien, c-à-d, lorsque G n'est pas abélien mais tous ses sous-groupes propres sont abéliens. Lorsque G est produit direct de groupes, J. N. S. Bidwell a trouvé une méthode pour décrire $\mathrm{Aut}(G)$ en fonction des groupes d'automorphismes des facteurs directs de G (voir [14]).

Un autre aspect consiste à étudier les restrictions sur la structure d'un p-groupe ayant un automorphisme ou un groupe d'automorphismes de certain type. Cet aspect comprend :

• La théorie des p-automorphismes ayant peu de points fixes (voir [54]). Un résultat typique dans cette branche est le suivant (voir [54, Theorem 12.15]) :

Théorème. *Il existe deux fonctions $h(p, m, n)$ et $k(p, n)$ tels que : si G*

est un p-groupe possédant un automorphisme d'ordre p^n qui fixe exactement p^m point dans G ; alors G contient un sous-groupe caractéristique N qui vérifie $|G : N| \leq h(p, m, n)$, et la longueur dérivée de N ne dépasse pas $k(p, n)$.

• L'étude des p-groupes G avec un p-automorphisme qui a un ordre assez grand relativement à l'ordre de G (voir [11, §33], et [61]). Dans ce cadre, nous avons un problème posé par Y. Berkovich dans le Kourovka Notebook :

Problème 1. (voir [63, Problem 15.32]) *Supposons qu'un p-groupe G d'ordre p^m possède un automorphisme d'ordre p^{m-k}. Est -il vrai que si m est suffisamment grand par rapport à k, alors G posséde un sous-groupe cyclique d'indice p^k ?*

• Le problème de classification des p-groupes avec un groupe d'automorphismes abélien. Une restriction qui résulte immédiatement est que la classe d'un tel groupe est au plus 2. Le lecteur est référé à [51] et [19], pour plus de résultats et de références.

• L'étude des p'-automorphismes des p-groupes. Pour une exposition des résultats classiques dans ce thème le lecteur est référé à [31, §5.3]. Le problème suivant représente une direction de recherche plus moderne.

Problème 2. (voir [62, Question 9]) *Est-ce que pour presque tous les p-groupes, le groupe d'automorphismes est un p-groupe ?*

Le terme *"presque tous"* peut être interprété comme suit : soient $g(p^n)$ le nombre des p-groupes d'ordres au plus p^n, et $h(p^n)$ le nombre des p-groupes qui ont un ordre au plus p^n et pour chacun d'eux le groupe d'automorphismes est un p-groupe ; est ce que pour tout nombre premier p, $\lim_{n\to\infty} \frac{h(p^n)}{g(p^n)} = 1$?

Cette question est liée au problème de détermination de la proportion des groupes finis qui sont nilpotents (voir [62, Question 1]).

Dans le cadre du Problème 2, G. T. Helleloid et U. Martin ont démontré que la réponse est positive pour une version plus faible du problème (voir [43]). Notons que ce résultat est annoncé sans démonstration par U. Martin en 1986 ; et cette version est utilisée par H. W. Henn et S. Priddy pour démontrer que, dans un sens, presque tous les groupes finis sont p-nilpotents (voir [45]).

D'autre part, un effort considérable est consacré à l'étude des p-automorphismes non-intérieurs des p-groupes. Certainement, le résultat le plus célèbre dans ce contexte est celui de W. Gaschütz (voir [30]), qui affirme que tout p-groupe non simple possède un p-automorphisme non-intérieur ; ce qui revient à dire que p divise l'ordre de $\mathrm{Out}(G)$. Donc si G est un p-groupe d'ordre supérieur à p, $\mathrm{Out}(G)$ contient un p-sous-groupe de Sylow non-trivial. Un raffinement

de ce résultat, due à P. Schmid (voir [68]), montre que $\mathrm{Out}(G)$ contient des p-sous-groupes normaux, si G n'est pas élémentaire abélien ou extra-spécial.

Y. Berkovich a proposé un autre raffinement du résultat de Gaschütz :

Conjecture (Berkovich). *Si G est un p-groupe non-simple, alors G admet un automorphisme non-intérieur d'ordre p.*

Cela forme le plus ancien problème sur les p-groupes dans le Kourovka Notebook, après le problème de Burnside pour les groupes d'exposant au plus 100 [63, Problems 4.2 and 4.13]. Cette conjecture fait l'objet de cette thèse, et on va la discuter avec plus de détail ultérieurement.

Voici une autre conjecture dans le cadre des automorphismes non-intérieurs, qui a duré longtemps :

Conjecture de divisibilité. *Si G est un p-groupe d'ordre au moins p^3, alors l'ordre de $\mathrm{Z}(G)$ divise celui de $\mathrm{Out}(G)$.*

Cette conjecture, en d'autre termes, stipule que l'ordre de G divise l'ordre de son groupe d'automorphismes, lorsque $|G| \geq p^3$. Pendant la rédaction de cette introduction, J. González-Sánchez et A. Jaikin-Zapirain ont construit des contres exemples de cette dernière conjecture. La preuve est surprenante, et combine des résultats sur les dérivations de certaines algèbres de Lie sur $\mathbb{Q}$, avec la cohomologie continue des pro-p groupes (voir [34]).

Encore dans le contexte des automorphismes non-intérieurs, M.J. Curran et D.J. Mc Caughan ont caractérisé les p-groupes G, pour lesquels $\mathrm{Aut}_z(G) = \mathrm{Inn}(G)$, où $\mathrm{Aut}_z(G)$ est le groupe des automorphismes centraux de G. Pour cela, il faut et il suffit que G' soit cyclique et que $\mathrm{Z}(G)$ et G' coïncident (voir [22]).

Un automorphisme σ d'un groupe G est dit *quasi-intérieur* si x et $\sigma(x)$ sont conjugués dans G, pour tout $x \in G$. Les automorphismes quasi-intérieurs de G forment un sous-groupe de $\mathrm{Aut}(G)$; il est noté $\mathrm{Aut}_c(G)$; il contient évidement $\mathrm{Inn}(G)$; on peut ainsi définir le groupe $\mathrm{Out}_c(G) = \mathrm{Aut}_c(G)/\mathrm{Inn}(G)$. La détermination des p-groupes (ou les groupes en général) qui ont la propriété $\mathrm{Out}_c(G) = 1$ est un problème important, qui est encore lié à d'autres disciplines ; le lecteur peut se référer à [81] pour plus de détails et de références.

Problème 5. (voir aussi [62, Question 10]) *Quels sont les p-groupes avec seulement des automorphismes quasi-intérieurs ?*

Concernant la conjecture de Berkovich, H. Liebeck a démontré dans [60] que tout p-groupe G, p impair, de classe 2 possède un automorphisme non-intérieur d'ordre p, qui peut être choisi de telle façon qu'il fixe tous les éléments de $\Phi(G)$. La situation avec $p = 2$ est un peu différente ; le groupe G

défini par la présentation

$$G = \langle a, b \,|\, a^4 = [a, b, b],\, b^8 = [a, b] \rangle$$

est un groupe d'ordre 128 et de classe 2 et est tel que tout automorphisme d'ordre 2 de G qui fixe les éléments de $\Phi(G)$ est intérieur. L'exemple précédent a été établi par Liebeck. A. Abdollahi ([2]) a construit un groupe analogue, d'ordre 64 ; ce groupe possède la présentation :

$$\langle a, b \,|\, a^4 = b^4,\, b^{16} = 1,\, b^4 = [b, a] \rangle.$$

Une preuve de la conjecture pour les 2-groupes de classe 2 n'a été établie qu'en 2006 par Abdollahi (voir [3]).

Schmid a montré dans [67], que si G est p-groupe régulier, alors les groupes de cohomologie de Tate $\hat{H}^n(G/N, \mathrm{Z}(N))$ sont tous non nuls lorsque G/N n'est pas cyclique (N est un sous-groupe normal de G). Plus tard, Deaconescu et Silberberg ont observé dans [23] que le résultat de Schmid confirme en particulier la conjecture de Berkovich pour les p-groupes réguliers.

Aussi, dans [23], Deaconescu et Silberberg ont réduit la conjecture aux p-groupes G satisfaisant la condition $\mathrm{C}_G(\mathrm{Z}(\Phi(G))) = \Phi(G)$. Plus récemment, M. Ghoraishi a amélioré cette réduction en démontrant que la conjecture est vraie lorsque la propriété $H \leq \mathrm{C}_G(H) = \Phi(G)$ n'est pas vérifiée ; où H est l'image réciproque de $\Omega_1(\mathrm{Z}(G/\mathrm{Z}(G)))$ dans G (voir [31]).

Les p-groupes puissants ressemblent beaucoup aux p-groupes abéliens, et donc c'est raisonnable d'essayer de démontrer la conjecture lorsque $G/\mathrm{Z}(G)$ est puissant (au lieu d'être abélien). Ce cas a été réglé par Abdollahi dans [2].

Dans [5], la conjecture est démontrée pour les p-groupes de classe 3. En vertu de la validité de la conjecture pour les p-groupes réguliers, il suffit dans ce cas de considérer seulement $p = 2, 3$.

La conjecture est aussi confirmée dans d'autres cas particuliers, pour lesquels le lecteur est référé à [32], [71], [72], et [52].

Nos résultats peuvent être réparties en deux types. Le premier comprend les résultats liés directement à la conjecture de Berkovich ; et le deuxième type comprend des résultats qu'on a développés pendant notre investigation de la conjecture, et qui sont motivés par elle. Les résultats principaux du premier type sont :

Théorème A (voir [10]). *Soient G un p-groupe semi-abélien et N un sous-groupe normal de G tel que G/N ne soit pas cyclique ou un quaternion généralisé. Alors $\hat{H}^n(G/N, \mathrm{Z}(N)) \neq 0$, pour tout entier n ; où $\hat{H}^n(G/N, \mathrm{Z}(N))$ désignent les groupes de cohomologie de Tate.*

Un p-groupe G est dit *semi-abélien* s'il satisfait

$$(xy^{-1})^p = 1 \Leftrightarrow x^p = y^p$$

pour tout $x, y \in G$. Ces groupes sont traités dans la section 1.2.

Théorème B (voir [10])**.** *Soit G un p-groupe semi-abélien. Alors G possède un automorphisme non-intérieur d'ordre p, qui fixe tous les éléments de $\Phi(G)$.*

D'après un résultat de Xu (voir Théorème 1.3.5), tout p-groupe G satisfaisant $\Omega(\gamma_{p-1}(G)) \leq \mathrm{Z}(G)$ est fortement semi-abélien (voir Définition 1.2.1). D'où

Corollaire C. *Si G est un p-groupe vérifiant $\Omega(\gamma_{p-1}(G)) \leq \mathrm{Z}(G)$, alors G possède un automorphisme non-intérieur d'ordre p, qui fixe tous les éléments de $\Phi(G)$.*

Tout p-groupe régulier est fortement semi-abélien (voir Proposition 1.3.2). Donc

Corollaire D. *Si G est un p-groupe régulier, alors G possède un automorphisme non-intérieur d'ordre p, qui fixe tous les éléments de $\Phi(G)$.*

Comme nous avons mentionné, Corollaire D doit être attribué à P. Schmid, M. Deaconescu et G. Silberberg.

Théorème E. *Soit G un p-groupe. Si G est p-central de hauteur $p-2$ ou p^2-central de hauteur $p-1$; alors G est fortement semi-abélien.*

Corollaire F. *Soit G un p-groupe. Si G est p-central de hauteur $p-2$ ou p^2-central de hauteur $p-1$; alors G possède un automorphisme non-intérieur d'ordre p, qui fixe tous les éléments de $\Phi(G)$.*

Le théorème suivant est démontré d'abord par l'auteur et M. Reguiat pour $p \geq 3$, et complété pour $p = 2$ par A. Abdollahi, M. Ghoraishi et B. Wilkens. Le résultat sous la forme ci-dessous est publié dans [4].

Théorème G. *Soit G un p-groupe de coclasse 2. Alors G possède un automorphisme non-intérieur d'ordre p.*

Notons que, dans ce cas, on peut choisir notre automorphisme de telle façon qu'il opère trivialement sur le centre.

Abdollahi a démontré dans [2, Corollary 2.3] que si tous les automorphismes centraux d'ordre p d'un p-groupe G sont intérieurs, alors $\mathrm{d}(\frac{Z_2(G)}{\mathrm{Z}(G)}) = \mathrm{d}(G)\,\mathrm{d}(\mathrm{Z}(G))$ (ce résultat a été aussi établi par Attar dans [71, Theorem]). Le théorème suivant caractérise la classe des p-groupes ($p \geq 3$) pour lesquels tous les automorphismes centraux d'ordre p sont intérieurs.

Théorème H. *Soit G un p-groupe, p impair. Alors G possède un automorphisme central non-intérieur d'ordre p si, et seulement si,* $\mathrm{d}(\frac{Z_2(G)}{\mathrm{Z}(G)}) \neq \mathrm{d}(G)\,\mathrm{d}(\mathrm{Z}(G))$.

Notons que ce théorème (en fait, une seule implication) implique que tout p-groupe de classe maximale vérifie la conjecture de Berkovich.

Les résultats du deuxième type concernent essentiellement la classe des anneaux (i, p^j, k)-nuls. Ces anneaux sont émergés de notre étude des automorphismes centraux des p-groupes. D'abord on a observé qu'il est possible d'associer un anneau à tout groupe d'automorphisme $\mathrm{Aut}_A(G)$, où A est un sous-groupe abélien normal du groupe G, de telle façon que $\mathrm{Aut}_A(G)$ soit isomorphe au groupe adjoint de cet anneau (on a découvert ultérieurement que cette relation a été déjà établie par H. Laue dans [57]). Pour $A = \mathrm{Z}(G)$, $\mathrm{Aut}_A(G)$ est le groupe d'automorphismes centraux de G, et son anneau associé n'est autre que $\mathrm{Hom}(G, \mathrm{Z}(G))$ muni de de l'addition usuelle et la composition des applications comme multiplication. Lorsque G est un p-groupe vérifiant $\mathrm{Z}(G) \leq \Phi(G)$, tout homomorphisme $h : G \longrightarrow \mathrm{Z}(G)$, qui vérifie $ph = 0$ est nul sur $\Phi(G)$, et donc il est nul sur l'image de tout homomorphisme de G dans $\mathrm{Z}(G)$; ceci revient à dire que h est un annihilateur à droite de l'anneau $\mathrm{Hom}(G, \mathrm{Z}(G))$. On est ramené alors à introduire la notion d'anneaux $(1, p, 0)$-nuls (p-nuls à droite suivant la terminologie de [40]), et ainsi, dualement, la notion d'anneaux $(0, p, 1)$-nuls (p-nuls à gauche). Plus généralement on est ramené à définir les anneaux (i, p^j, k)-nuls.

Soient A un anneau et $i, j, k \in \mathbb{N}$. On dit que A est *(i, p^j, k)-nul*, si pour tout $x \in A$ tel que $p^j x = 0$, et pour tous $x_1, x_2, .., x_{i+k} \in A$, on a $x_1 \dots x_i x x_{i+1} \dots x_{i+k} = 0$ (voir Définition 2.1.4).

Lorsque i, j, k sont arbitraires, on recouvre au moins les p-anneaux finis nilpotents qui forment une classe d'anneaux assez sauvage. En revanche, lorsque $i + k$ est petit par rapport à p, on obtient une classe d'anneaux avec plusieurs propriétés intéressantes. La propriété la plus remarquable d'un anneau dans cette dernière classe est que la p-structure de son groupe adjoint est sévèrement contrôlée par celle de son groupe additif :

Théorème A'. *Soit A un p-anneau fini. Supposons que A est (i, p^j, k)-nul, où $i + k \leq p - 2$ et $j \geq 1$ ou bien $i + k \leq p - 1$ et $j \geq 2$. Alors $\Omega_{\{n\}}(A^\circ) = \Omega_n(A^+)$, pour tout $n \geq 1$. En particulier on a $\Omega_{\{n\}}(A^\circ) = \Omega_n(A^\circ)$, pour tout $n \geq 1$.*

Une fois $i+k = p-1$ avec aucune condition sur j, ou en général $i+k = p$, le théorème précédent devient faux ; donc il ne peut pas être amélioré dans un sens.

Théorème B'. *Soient A un p-anneau fini et H un sous-groupe de A°. Supposons que A est (i, p^j, k)-nul, où $i + k \leq p - 2$ et $j \geq 1$ ou bien $i + k \leq p - 1$ et $j \geq 2$. Alors $|H : H^p| \leq |\Omega_1(H)|$.*

Il est conjecturé par O. Dickenshied (voir [24]) que pour tout p-anneau nilpotent fini A, on a $r(A^\circ) \leq \epsilon r(A^+)$, où $\epsilon = 1$ si $p \geq 3$ et $\epsilon = 2$ si $p = 2$. Le Théorème B' confirme alors cette conjecture pour les anneaux dans son énoncé.

Le résultat suivant est démontré par O. Dickenshied pour les p-anneaux nilpotents finis (voir [24]).

Corollaire C'. *Soient A un p-anneau fini, et P un p-sous-groupe de Sylow de A°. Alors $r(P) \leq \epsilon r(A^+)$, où $\epsilon = 2$ si $p \geq 3$ et $\epsilon = 3$ si $p = 2$.*

Le résultat suivant réfute la conjecture de Dickenshied.

Théorème D'. *Pour tout entier positif m, il existe un p-anneau nilpotent fini A tel que $r(A^\circ) - r(A^+) \geq m$.*

Notons que l'auteur et Andrea Caranti ont proposé une conjecture plus fine que celle de Dieckenshied ; cette conjecture alternative est démontrée dans les cas critiques où celle de Dickenshied est fausse ; ce travail n'est pas encore soumis.

Les p-anneaux (i, p^j, k)-nuls interviennent dans plusieurs cas lorsque on étudie les automorphismes de p-groupes. Par exemple ils interviennent dans la démonstration du théorème H, ci-dessus. Le troisième et le quatrième chapitre contiennent plusieurs autres applications ; citons par exemple :

Proposition E'. *Soient G un p-groupe et A un sous-groupe normal abélien de G qui vérifie $A \leq G'G^{2p}$. Si $A \leq Z_k(G)$, alors l'anneau $\mathrm{Der}(G, A)$ est $(k, p, 0)$-nul.*

Comme conséquence, on a :

Théorème F'. *Soit G un p-groupe et A un sous-groupe normal abélien de G qui vérifie $A \leq G'G^{2p}$ et $A \leq Z_k(G)$. Si $p \geq 3$ et $k = p - 2$, ou $p = 2$ et $k = 1$, alors*

(i) *pour tout $n \geq 1$, on a $\Omega_n(\mathrm{Aut}_A(G)) = \Omega_{\{n\}}(\mathrm{Aut}_A(G)) = \mathrm{Aut}_{A_i}(G)$, où A_i désigne $\Omega_n(A)$;*

(ii) *pour tout sous-groupe P de $\mathrm{Aut}_A(G)$, on a $|P : P^p| \leq |\Omega_1(P)|$.*

En essayant d'obtenir un dual de la Proposition E' (le cas où $\mathrm{Der}(G, A)$ est $(0, p, k)$-nul), on avait constaté que le résultat désiré s'obtiendra sans supposer que A est abélien. On était ramené à introduire la notion de *"action p-centrale sur un groupe"*; cette notion est traitée dans [38], et on a décidé de ne pas la discuter dans cette thèse. L'un des résultats prouvé dans [38] est utilisé dans la section 2.3.3, pour démontrer :

Théorème G'. *Soit G un p-groupe de rang k, avec $p \geq 3$. Alors tout p-sous-groupe de $\mathrm{Aut}(G)$ peut être engendré par $\frac{5}{4}k^2$ éléments.*

Ce dernier donne une amélioration remarquable de la borne sur le p-rang de $\mathrm{Aut}(G)$, obtenue par D. Segal et A. Shalev (voir [73]), et celle obtenue par l'auteur et B. Daoud dans [39].

Théorème H'. *Soient G un p-groupe, $p \geq 3$, et $P = \mathrm{Aut}_{S_1}(G)\,\mathrm{Inn}(G)$, où S_1 est le sous-groupe des éléments d'ordre au plus p dans $(G^{2p}G') \cap \mathrm{Z}(G)$. Soit p^t le plus petit entre $\exp(G/G')$ et $\exp(\mathrm{Z}(G))$. Alors l'exposant de $\mathrm{C}_{\mathrm{Aut(G)}}(P)$ divise $p^t(p-1)$; et en particulier l'exposant de $\mathrm{Z}(\mathrm{Aut(G)})$ divise $p^t(p-1)$.*

Finalement, voici une brève description de la structure de cette thèse :

Dans le premier chapitre on discute les p-groupes semi-abéliens. La première section traite les propriétés de base des groupes nilpotents dont on a besoin ; ces résultats sont en principe bien connus dans la littérature. Dans la deuxième section on introduit la notion des p-groupes semi-abéliens et fortement semi-abéliens, qui est due à Mingyao Xu. La relation de ces groupes avec d'autres familles de p-groupe est discutée dans la troisième section, où on a aussi établi Théorème E. Ce chapitre se termine par une réponse d'une question posée par Mingyao Xu.

Le deuxième chapitre traite les p-anneaux (i, p^j, k)-nuls. Les Théorème A' et Théorème B' sont démontrés dans la première section. Le rang des groupes adjoints d'anneaux et le Théorème D' sont traités dans la section qui suit. On conclut ce chapitre par quelques applications des p-anneaux (i, p^j, k)-nuls ; ceci comprend en particulier une démonstration du Théorème H, et une réponse de deux problèmes posés par Y. Berkovich.

Le troisième chapitre traite quelques applications de la cohomologie des groupes finis aux automorphismes non-intérieurs des p-groupes. Théorème A et Théorème B sont établis dans la troisième section de ce chapitre.

Le dernier chapitre discute en premier lieu le problème de prolongement des endomorphismes d'un quotient central d'un p-groupe G, à G tout entier. Une notion intéressante qui intervient est celle d'un p-groupe pleine par rapport à un sous-groupe maximal ; celle-ci est discutée dans la deuxième section. Ce matériel est utilisé dans la dernière section pour établir le Théorème G.

Chapitre 1

p-Groupes semi-abéliens

1.1 Préliminaires sur les p-groupes

Cette section contient quelques notions de base sur les p-groupes, ou plus généralement sur les groupes nilpotents, qu'on va utiliser ultérieurement. Les résultats les plus standards sont cités sans références.

Soit G un groupe. Le commutateur $[x, y]$ de deux éléments $x, y \in G$, est défini par

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

cette opération peut être itérée pour définir des commutateurs de plusieurs éléments ; si $x_1, x_2, \dots x_n$ sont des éléments de G, $n \in \mathbb{N}^*$, le commutateur (normé à gauche) $[x_1, x_2, \dots, x_n]$ est défini par récurrence

$$[x_1] = x_1$$

$$[x_1, x_2, \dots, x_n] = [[x_1, x_2, \dots, x_{n-1}], x_n].$$

On peut aussi définir le commutateur $[X, Y]$ de deux parties non-vides X et Y de G, comme le sous-groupe engendré par tous les commutateurs $[x, y]$, $x \in X$ et $y \in Y$.

Soit $\gamma_n(G)$ le sous-groupe engendré par tous les commutateurs $[x_1, x_2, \dots, x_k]$, $k \geq n$. Ces sous-groupes sont totalement invariants, et forment une suite

$$\cdots \lhd \gamma_n(G) \lhd \cdots \lhd \gamma_2(G) \lhd \gamma_1(G) = G$$

qui s'appelle *la suite centrale descendante* de G

Définition 1.1.1. *On dit que G est nilpotent si $\gamma_n(G)$ est trivial à partir d'un certain rang. Dans ce cas, le plus petit entier c qui vérifie $\gamma_{c+1}(G) = 1$ est appelé la classe de nilpotence de G.*

On peut également définir les sous-groupes $\gamma_n(G)$ par récurrence :

$$\gamma_1(G) = G \quad \text{et} \quad \gamma_{n+1}(G) = [\gamma_n(G), G].$$

L'équivalence entre les deux définitions des $\gamma_n(G)$ résulte de ces deux identités (distributivité des commutateurs) :

$$[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z] \tag{1.1}$$

$$[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z] \tag{1.2}$$

Nous avons en particulier, $[\gamma_n(G), \gamma_1(G)] \leq \gamma_{n+1}(G)$, pour tout n. Cette propriété peut être encore généralisée.

Proposition 1.1.2. *Sous les notations ci-dessus, nous avons* $[\gamma_n(G), \gamma_m(G)] \leq \gamma_{n+m}(G)$*, pour tous* $n, m \in \mathbb{N}^*$.

Cette généralisation est possible grâce au Lemme de trois sous-groupes, qui résulte de l'identité de Hall-Witt :

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

Proposition 1.1.3. *(Lemme de trois sous-groupes) Soient X, Y et Z trois sous-groupes de G, et N un sous-groupe normal dans G. Si N contient deux des trois sous-groupes $[[X, Y], Z]$, $[[Y, Z], X]$ et $[[Z, X], Y]$, alors il contient le troisième.*

Soient $i, j \in \mathbb{N}^*$; en vertu de Proposition 1.1.2, on a une application bien définie

$$\gamma_i(G)/\gamma_{i+1}(G) \times \gamma_j(G)/\gamma_{j+1}(G) \longrightarrow \gamma_{i+j}(G)/\gamma_{i+j+1}(G)$$

$$(x\gamma_{i+1}(G), y\gamma_{j+1}(G)) \mapsto [x, y]\gamma_{i+j+1}(G)$$

Il en résulte des identités (1.1) et (1.2) que cette application est $\mathbb{Z}$-bilinéaire, donc elle induit un homomorphisme de groupe abélien

$$\gamma_i(G)/\gamma_{i+1}(G) \otimes \gamma_j(G)/\gamma_{j+1}(G) \longrightarrow \gamma_{i+j}(G)/\gamma_{i+j+1}(G)$$

où le produit tensoriel est pris sur $\mathbb{Z}$.

Le cas où $i = 1$, a une importance particulière.

Proposition 1.1.4 ([59, 1.2.11])**.** *Soient G un groupe et j un entier positif. Alors l'application définie par*

$$xG' \otimes y\gamma_{j+1}(G) \mapsto [x, y]\gamma_{j+2}(G)$$

est un homomorphisme surjectif de $G/G' \otimes \gamma_j(G)/\gamma_{j+1}(G)$ dans $\gamma_{j+1}(G)/\gamma_{j+2}(G)$.

Ce résultat implique que l'abélianisé G/G' de G, a une grande influence sur les autres facteurs de la suite centrale descendante ; et en particulier sur G tout entier lorsqu'il est nilpotent.

Corollaire 1.1.5. *Supposons que G/G' est de type fini et d'exposant égal à m ; alors*

1. *L'exposant de $\gamma_i(G)/\gamma_{i+1}(G)$ divise m pour tout $i \geq 1$. De plus si G est nilpotent de classe c, alors l'exposant de G divise m^c.*
2. *Pour tout $i \geq 1$, $\gamma_i(G)/\gamma_{i+1}(G)$ est de type fini. De plus si G est nilpotent, alors tout sous-groupe de G est de type fini.*

Notons que le groupe additif (gradué) $L(G) = \bigoplus_{i\geq 1} \gamma_i(G)/\gamma_{i+1}(G)$, peut être muni d'une multiplication définie sur ses éléments homogènes par

$$[x_i\gamma_{i+1}(G), y_j\gamma_{j+1}(G)] = [x_i, y_j]\gamma_{i+j+1}(G),$$

cette multiplication est $\mathbb{Z}$-bilinéaire, qui vérifie $[x, x] = 0$, et l'identité de Jacobi

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0,$$

pour tous $x, y, z \in L(G)$. L'identité de Jacobi résulte exactement de l'identité de Hall-Witt (le lecteur doit constater la ressemblance entre les deux). Donc $L(G)$ a une structure d'une algèbre de Lie sur $\mathbb{Z}$ (ou aussi anneau de Lie). Cette construction (ou ses variantes) permet de réduire quelques problèmes sur les groupes à des problèmes sur les algèbres de Lie. Cette méthodologie a abouti à la solution du problème restreint de Burnside (voir [76]) ; le lecteur est référé à [54] pour d'autres applications.

Le dual de la suite centrale descendante est *la suite centrale ascendante*. Cette suite est définie par récurrence :

$$Z_0(G) = 1 \quad \text{et} \quad Z_{n+1}(G)/Z_n(G) = \mathrm{Z}(G/Z_n(G)).$$

Notons en particulier que $Z_1(G)$ coïncide avec le centre de G.

Proposition 1.1.6. *Soit G un groupe. Alors G est nilpotent si et seulement si $Z_n(G) = G$ pour certain n. De plus si G est de classe c, alors c est le plus petit entier tel que $Z_c(G) = G$.*

Une propriété assez élémentaire mais fondamentale pour les p-groupes, est que le centre d'un p-groupe non-trivial est non-trivial. Un raisonnement simple par récurrence montre que

Proposition 1.1.7. *Tout p-groupe (fini) est nilpotent.*

Le réciproque de la proposition précédente est presque vraie : un groupe nilpotent fini est produit direct de ses sous-groupes de Sylow (voir [66, 5.2.4]).

Ainsi, l'étude des groupes nilpotents finis peut se ramener à celle des p-groupes.

L'influence du centre d'un groupe sur les autres facteurs de la suite centrale ascendante, ressemble à celle de l'abélianisé sur les facteurs de la suite centrale descendante. D'abord, nous avons pour tout entier positif i, un homomorphisme injectif

$$Z_{i+1}(G)/Z_i(G) \longrightarrow \mathrm{Hom}(G, Z_i(G)/Z_{i-1}(G))$$

qui applique $xZ_i(G)$ sur l'homomorphisme $g \mapsto [x,g]Z_{i-1}(G)$. Or l'exposant de $\mathrm{Hom}(G, Z_i(G)/Z_{i-1}(G))$ divise l'exposant de $Z_i(G)/Z_{i-1}(G)$, il en résulte par induction sur i que

Proposition 1.1.8. *Si l'exposant de* $\mathrm{Z}(G)$ *divise* m*, alors l'exposant de* $Z_{i+1}(G)/Z_i(G)$ *divise* m*, pour tout* $i \geq 1$*. De plus si* G *est nilpotent de classe* c*, alors l'exposant de* G *divise* m^c*.*

Soit A un groupe, et supposons que G est un A-groupe, ce qui revient à donner un homomorphisme du groupe A dans le groupe d'automorphismes $\mathrm{Aut}(G)$. On appelle section de G tout quotient H/K, où $H, K \leq G$ et K est normal dans H. On dit que A centralise la section H/K, si $x^{-1}x^{\sigma} = [x,\sigma] \in K$, pour tout $x \in H$ et $\sigma \in A$. Notons dans ce cas que H et K sont invariants par l'action de A.

Par exemple, G est un G-groupe avec l'action induite par conjugaison. Dans ce cas, G centralise tous les facteurs de sa suite centrale ascendante ou descendante.

Plus généralement, si G centralise tous les facteurs d'une suite

$$1 = N_{r+1} \lhd N_r \lhd \cdots \lhd N_1 = G$$

on dit que cette suite est centrale dans G. Notons que G possède une suite centrale (de longueur finie) si, et seulement si G est nilpotent. Ceci résulte du fait que $\gamma_i(G) \leq N_i$ (ou aussi $N_{r-i+1} \leq \mathrm{Z}_i(G)$), pour toute suite centrale descendante $(N_i)_{i=1,r+1}$.

Le résultat suivant montre que la situation n'est pas différente si on remplace l'action de G sur lui même par l'action d'un groupe d'automorphismes de G.

Proposition 1.1.9. *Soit* A *un groupe d'automorphismes de* G*, qui centralise tous les facteurs d'une suite normale*

$$1 = N_{r+1} \lhd N_r \lhd \cdots \lhd N_1 = G.$$

Alors A *est nilpotent de classe au plus égale à* $r-1$*.*

Ce résultat est due à Kaloujnine (1953). Un peu plus tard P. Hall (1958) a généralisé ce résultat, en supposant seulement que la suite est sous-normale

(Voir [59, 1.2.7]). Notons aussi que si on a une suite de sous-groupes dans G, les automorphismes qui centralisent cette suite forment un sous-groupe de $\mathrm{Aut}(G)$, qui s'appelle (souvent) le groupe stabilisateur de cette suite ; donc un groupe stabilisateur est toujours nilpotent.

Proposition 1.1.10. *Soit A le groupe stabilisateur d'une suite normale dans G,*

$$1 = N_{r+1} \lhd N_r \lhd \cdots \lhd N_1 = G.$$

Si l'exposant de chaque facteur N_i/N_{i+1} divise un entier positif m, alors l'exposant de A divise m^{r-1}.

Démonstration. Voir [25, 0.7] □

Une variante de la suite centrale descendante est *la suite p-centrale descendante*. Cette suite est définie pour un groupe G, comme suit :

$$\lambda_1(G) = G \quad \text{et} \quad \lambda_{n+1}(G) = [\lambda_n(G), G]\lambda_n(G)^p.$$

Cette suite est particulièrement intéressante pour les p-groupes : si G est fini, alors $\lambda_n(G)$ atteint 1 si et seulement si G est un p-groupe. Dans ce cas le plus petit entier n qui vérifie $\lambda_{n+1}(G) = 1$ s'appelle la longueur p-centrale de G.

Le résultat suivant se démontre facilement par récurrence.

Proposition 1.1.11. *Soient G un p-groupe, et*

$$1 = N_{r+1} \lhd N_r \lhd \cdots \lhd N_1 = G.$$

une suite centrale dans G, dont les facteurs sont d'exposant p. Alors $\lambda_i(G) \leq N_i$, pour tout $i \geq 1$.

Il est important de noter que les termes de la suite p-centrale descendante peuvent être encore définis par :

$$\lambda_n(G) = \lambda_1(G)^{p^{n-1}} \lambda_2(G)^{p^{n-2}} \ldots \lambda_n(G),$$

et qu'ils vérifient la propriété

$$[\lambda_i(G), \lambda_j(G)] \leq \lambda_{i+j}(G), \quad \text{pour } i, j \geq 1.$$

La démonstration de ces deux propriétés, est basée sur la formule de Hall-Petrescu (voir Proposition 1.1.15 ci-dessous), les détails de la démonstration peuvent être trouvés dans [48, Chapter VIII. §1]

Proposition 1.1.12 ([49, Theorem VIII.1.7])**.** *Soient G un groupe et σ un automorphisme de G. Si σ centralise $G/\lambda_2(G)$, alors σ centralise tous les facteurs $\lambda_i(G)/\lambda_{i+1}(G)$, $i \geq 2$.*

Pour un groupe G, le sous-groupe de Frattini $\Phi(G)$ est défini comme l'intersection de tous les sous-groupes maximaux de G. Ce sous-groupe coïncide avec $\lambda_2(G) = G'G^p$ si G est un p-groupe. Donc pour les p-groupes, $G/\Phi(G)$ peut être considéré comme un espace vectoriel sur $\mathbb{Z}_p$. Un résultat classique de Burnside (Voir [66, 5.3.2]) affirme que la dimension de $G/\Phi(G)$ coïncide avec le nombre minimal de générateurs de G, qui est noté $\mathrm{d}(G)$.

Une des conséquences remarquables du résultat de Burnside est le résultat suivant du à P. Hall (voir [41] ; pour une référence plus récente voir par exemple [66, 5.3.3]).

Proposition 1.1.13. *Soient G un p-groupe, et $\mathrm{Aut}_{\Phi(G)}(G)$ le groupes des automorphismes de G qui centralisent le quotient $G/\Phi(G)$. Alors l'ordre de $\mathrm{Aut}_{\Phi(G)}(G)$ divise $|\Phi(G)|^d$, avec $d = \mathrm{d}(G)$. De plus $\mathrm{Aut}(G)/\mathrm{Aut}_{\Phi(G)}(G)$ est isomorphe à un sous-groupe de $\mathrm{GL}(d, p)$.*

Cela fournit une borne pour l'ordre de $\mathrm{Aut}_{\Phi(G)}(G)$. D'autre part, Proposition 1.1.12 implique que $\mathrm{Aut}_{\Phi(G)}(G)$ est le groupe stabilisateur de la suite p-centrale descendante de G. Il en résulte de Proposition 1.1.9 que

Proposition 1.1.14. *Soit G un p-groupe de longueur p-centrale n. Alors $\mathrm{Aut}_{\Phi(G)}(G)$ est nilpotent de classe au plus $n - 1$.*

Soient G un groupe et $x, y \in G$; par définition du commutateur $[x, y]$, on a $xy = yx[x, y]$. Cette propriété permet de changer l'ordre des symboles dans un produit d'éléments de G, en ajoutant, grossièrement, un commutateur à droite pour chaque permutation. On peut illustrer ceci par l'exemple suivant :

$$(xy)^2 = xyxy = x^2y[y, x]y = x^2y^2[y, x][y, x, y].$$

La même méthodologie mène à une formule plus générale :

Proposition 1.1.15 (Formule de Hall-Petrescu)**.** *Soient x et y deux éléments d'un groupe G, et n un entier positif. Alors*

$$(xy)^n = x^n y^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \dots c_n^{\binom{n}{n}}$$

où $c_i \in \gamma_i(G)$, pour chaque indice i.

Démonstration. Voir par exemple [11, Appendix 1]. □

Il est sous-entendu que chaque c_i dans la formule précédente appartient à $\gamma_i(H)$ où $H = \langle x, y \rangle$ (prendre $G = H$).

Le résultat suivant est l'une des belles conséquences de la formule de Hall-Petrescu ; et est du à G. A. Fernández-Alcober, J. González-Sánchez et A. Jaikin-Zapirain (voir [27, Theorem 2.7]).

Proposition 1.1.16. *Soient G un p-groupe, X une partie de G qui engendre un sous-groupe normal, et i, n deux entiers positifs. Alors*

$$[P_{0,i}\, G]^{p^n} \leq \prod_{j=0}^{n} [P_{n-j,j(p-1)+i}\, G]$$

où $P_j = \langle x^{p^j} \mid x \in X \rangle$.

1.2 p-Groupes semi-abéliens et p-groupes fortement semi-abéliens

Les p-groupes semi-abéliens sont introduits et étudiés par Mingyao Xu (voir[80]), et la plus part de ses travaux sur ce sujet sont en chinois (voir la bibliographie de [80]).

Définition 1.2.1. *Soit G un p-groupe. On dit que G est fortement semi-abélien si pour tous $x, y \in G$, on a*

$$(xy^{-1})^{p^n} = 1 \Leftrightarrow x^{p^n} = y^{p^n} \text{ pour tout entier positif } n.$$

Si on exige la propriété ci-dessus seulement pour $n = 1$, on dit que G est semi-abélien.

Il en résulte que si G est un p-groupe fortement semi-abélien, alors les éléments ayant un ordre divisant p^n forment un sous-groupe, qui coïncide évidement avec $\Omega_n(G)$. Il en résulte aussi que l'application

$$G/\Omega_n(G) \longrightarrow G^{\{p^n\}}$$

qui applique $x\Omega_n(G)$ sur x^{p^n}, est une bijection bien définie. Cette dernière propriété peut être considérée comme une définition alternative des p-groupes fortement semi-abéliens. Cette propriété implique aussi que

$$|G : G^{p^n}| \leq |\Omega_n(G)|, \quad \text{pour tout entier positif } n. \tag{1.3}$$

Le lemme suivant sera utile dans Chapitre 3.

Lemme 1.2.2. *Soit G un p-groupe fortement semi-abélien. Alors*

$$[x^{p^n}, y] = 1 \Leftrightarrow [x, y]^{p^n} = 1$$

pour tous $x, y \in G$ et $n \in \mathbb{N}$.

Démonstration. Supposons que $[x^{p^n}, y] = 1$. On a

$$x^{p^n} = (x^{p^n})^y = (x^y)^{p^n} = (x[x, y])^{p^n},$$

le fait que G est fortement semi-abélien implique

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

Inversement, supposons que $[x,y]^{p^n}$, donc $(x^{-1}x[x,y])^{p^n} = 1$, et encore puisque G est fortement semi-abélien on a

$$x^{p^n} = (x[x,y])^{p^n} = (x^y)^{p^n} = (x^{p^n})^y,$$

ceci montre que $[x^{p^n}, y] = 1$. □

Si G est semi-abélien, on peut adapter (trivialement) la démonstration précédente pour montrer que

$$[x^p, y] = 1 \Leftrightarrow [x,y]^p = 1, \quad \text{pour tout } x, y \in G.$$

Et en fait, cette propriété, qui est plus faible, est suffisante pour notre besoin.

1.3 Relations avec d'autres familles de p-groupes

On peut considérer la théorie des p-groupes réguliers comme la première tentative pour une étude systématique des p-groupes. La théorie des p-groupes réguliers est due à P. Hall ; elles peut être trouvée dans [41], ainsi que dans [11, §7] ou dans [48, Kap III].

Définition 1.3.1. *Un p-groupe G est dit régulier si pour tous $x, y \in G$, il existe $c \in \gamma_2(\langle x, y\rangle)^p$, tel que $(xy)^p = x^p y^p c$.*

Proposition 1.3.2. *Tout p-groupe régulier est fortement semi-abélien.*

Démonstration. Voir [11, Theorem 7.2 (a)]. □

La réciproque du Théorème 1.3.2 n'est pas forcément vraie (voir la section 1.4) ; mais on a le résultat suivant de M. Y. Xu (voir [80, Theorem 1]).

Théorème 1.3.3. *Soit G un p-groupe. Alors G est régulier si, et seulement si, toute section de G est semi-abélienne.*

Pour la commodité du lecteur, on a rassemblé quelques propriétés des p-groupes réguliers dans la proposition suivante.

Proposition 1.3.4. *Soit G un p-groupe.*

(a) *Si G est régulier, alors toute section de G est régulière.*

(b) *Si G est régulier, alors $\exp(\Omega_n(G)) \leq p^n$, les éléments de la forme x^{p^n} forment un sous-groupe et $|G : G^{p^n}| = |\Omega_n(G)|$, pour tout $n \in \mathbb{N}^*$.*

(c) *Si G est de classe strictement inférieure à p, ou si l'exposant de G est égal à p ; alors G est régulier.*

(d) *Si $\gamma_{p-1}(G)$ est cyclique, alors G est régulier.*

(e) *Si $|G : G^p| < p^p$, alors G est régulier.*

(f) *Si $|\gamma_2(G) : \gamma_2(G)^p| < p^{p-1}$, alors G est régulier.*

(g) *Si G ne possède aucun sous-groupe normal d'ordre p^{p-1} et d'exposant p, alors G est régulier.*

(h) *Tout 2-groupe régulier est abélien.*

(k) *(A. Mann) Pour $p > 2$, si tout sous-groupe de G peut être engendré par $\frac{p-1}{2}$, alors G est régulier.*

Démonstration. Voir [11, §§7, 9]. □

Nous nous consacrons maintenant à une autre famille de p-groupes, qui a reçu un intérêt croissant dans ces dernières années. On entend ici les p-groupes p-centraux. Un groupe G est dit *p-central* si le centre de G contient tous les éléments d'ordre p (d'ordre divisant 4 si $p = 2$). On réfère le lecteur à l'introduction de [35] pour quelques informations sur les premières études de ces groupes. En fait, on va discuter des généralisations des p-groupes p-centraux, en montrant essentiellement qu'ils sont fortement semi-abéliens.

La première généralisation est due à M. Y. Xu, où il avait considéré les p-groupes avec la propriété $\Omega_1(\gamma_{p-1}(G)) \leq \mathrm{Z}(G)$ (voir [79]). Le résultat fondamental pour ces groupes étant

Théorème 1.3.5. *Soit G un p-groupe avec $p > 2$, vérifiant $\Omega_1(\gamma_{p-1}(G)) \leq \mathrm{Z}(G)$. Alors G est fortement semi-abélien.*

Démonstration. Voir [79]. □

Ceci implique alors que l'exposant de $\Omega_n(G)$ est au plus égal à p^n, pour tout entier positif n ; et aussi G vérifie l'inégalité (1.3), ce qui implique immédiatement un résultat de Thompson, qui affirme que dans un p-groupe p-central G (p impair), $\mathrm{d}(G) \leq \mathrm{d}(\mathrm{Z}(G))$. Dans le même article [79], on peut trouver des nouvelles démonstrations et des généralisations de quelques résultats connus, qui sont basées sur le Théorème 1.3.5.

Pour $p = 2$ le théorème ci-dessus est faux comme le montre le groupe des quaternions Q_8. On doit renforcer la condition du théorème précédent pour couvrir ce cas ; ceci est compris dans le théorème qui suit.

Dans [35], J. González-Sánchez et T. S. Weigel ont considéré une autre généralisation. Ils définissent la *p^i-centralité* de la façon suivante : Un groupe G est dit *p^i-central de hauteur k* si tous les éléments de G d'ordre divisant p^i sont contenus dans $Z_k(G)$. Le résultat suivant est nouveau dans la littérature, bien qu'il soit inspiré par des résultats dans [35].

Théorème 1.3.6. *Soit G un p-groupe. Si G est p-central de hauteur $p-2$ ou p^2-central de hauteur $p-1$; alors G est fortement semi-abélien.*

D'abord on va démontrer trois lemmes.

Lemme 1.3.7. *Soit G un p-groupe. Si G est p-central de hauteur $p-1$; alors*

$$(xy^{-1})^p = 1 \Rightarrow x^p = y^p,$$

pour tout $x, y \in G$.

Démonstration. Soient $x \in G$, $t \in \Omega_1(G)$, $\langle t\rangle^G$ la clôture normale de $\langle t\rangle$, et $H = \langle x\rangle\langle t\rangle^G$. Par hypothèse $\langle t\rangle^G \leq Z_{p-1}(G)$; et puisque $H/\langle t\rangle^G$ est cyclique, on a

$$\gamma_2(H) = [H, \langle t\rangle^G] \leq [H, Z_{p-1}(G)] \leq Z_{p-2}(G).$$

Il en résulte que $\gamma_p(H) = 1$ et $\gamma_2(H) \leq \Omega_1(G)$. Pour $p \geq 3$, H est régulier ainsi que $\Omega_1(G)$, ce qui implique d'après Proposition 1.3.4(b) que $\gamma_2(H)$ est d'exposant p . Il en résulte de la définition d'un groupe régulier que H est p-abélien (c'est à dire, $(ab)^p = a^p b^p$ pour tout $a, b \in H$). On en déduit que $(xt)^p = x^p t^p = x^p$. Pour $p = 2$, on a $t \in \mathrm{Z}(G)$, donc $(xt)^2 = x^2 t^2 = x^2$. Ceci montre que pour tout $x, y \in G$:

$$(xy^{-1})^p = 1 \Rightarrow x^p = y^p$$

□

Le résultat suivant est du à J. González-Sánchez et T. S. Weigel ([35, Theorem B] ; on a inclu une preuve pour la commodité du lecteur.

Lemme 1.3.8. *Soient G un p-groupe, et i, k deux entiers positifs. Si G est p^i-central de hauteur k, avec $k \leq p-2$, ou $k \leq p-1$ et $i \geq 2$; alors $G/\Omega_1(G)$ est p^i-central de hauteur k.*

Démonstration. Soit le sous-groupe $N = \langle x \,|\, x^{p^i} \in \Omega_1(G)\rangle$; nous avons à prouver que $[N,_k G] \leq \Omega_1(G)$. D'après Théorème 1.1.16, on a

$$[N,_r G]^p \leq [P_1,_r G][N,_{(p-1)+r} G]$$

où $P_1 = \langle x^p \,|\, x^{p^i} \in \Omega_1(G)\rangle$. Il en résulte de Lemme 1.3.7 que $P_1 = \langle x^p \,|\, x^{p^{i+1}} = 1\rangle$, donc en particulier $P_1 \leq \Omega_i(G) \leq Z_k(G)$. D'où $[P_1,_r G] = 1$ pour tout $r \geq k$. Soit s le plus petit entier positif tel que $[N,_{(p-1)+s} G]$. Il suffit de montrer que $s \leq k$, car ceci implique

$$[N,_k G]^p \leq [P_1,_k G][N,_{(p-1)+k} G] = 1.$$

Par absurde, supposons que $s > k$. D'abord pour $k \leq p-2$, on a

$$[N,_s G]^p \leq [P_1,_s G][N,_{(p-1)+s} G] = 1,$$

d'où $[N,_s G] \leq \Omega_1(G) \leq Z_{p-2}(G)$; ceci implique que $[N,_{p-2+s} G] = 1$, ce qui contredit la définition de s. Maintenant pour $k = p-1$, on a d'après Théorème 1.1.16

$$[N,_{s-1} G]^{p^2} \leq [P_2,_{s-1} G][P_1,_{p+s-2} G][N,_{2(p-1)+s-1} G],$$

où $P_j = \langle x^{p^j} \mid x^{p^{i+1}} = 1 \rangle$, $j = 1, 2$. On a $P_1, P_2 \leq \Omega_i(G) \leq Z_k(G)$, $s-1 \geq k$ et $p+s-2 \geq k$; d'où $[P_2,_{s-1} G][P_1,_{p+s-2} G] = 1$. De plus, $2(p-1)+s-1 \geq p-1+s$, et ainsi $[N,_{2(p-1)+s-1} G] = 1$. Ceci montre que $[N,_{s-1} G] \leq \Omega_2(G) \leq Z_k(G)$, ce qui implique $[N,_{p+s-2} G] = 1$. Ceci contredit la définition de s. □

Lemme 1.3.9. *Soit G un p-groupe. Si G est p-central de hauteur $p-2$ ou p^2-central de hauteur $p-1$; alors G est semi-abélien.*

Démonstration. En vertu de Lemme 1.3.7, il suffit de montrer que :

$$x^p = y^p \Rightarrow (xy^{-1})^p = 1$$

pour tout $x, y \in G$. Supposons donc que $x^p = y^p$. En vertu de Lemme 1.3.8, et par récurrence sur l'ordre de G on doit supposer que $(xy^{-1})^p \in \Omega_1(G)$. Il en résulte de Lemme 1.3.7, que $(xy^{-1})^{p^2} = 1$, d'où $xy^{-1} \in Z_{p-1}(G)$. Soit $H = \langle t \rangle^G \langle x \rangle$, où $t = xy^{-1}$. On a

$$\gamma_2(H) = [H, \langle t \rangle^G] \leq [H, Z_{p-1}(G)] \leq Z_{p-2}(G).$$

Il en résulte que $\gamma_p(H) = 1$. Pour $p = 2$, H est abélien ; donc en particulier $K = \langle x, y \rangle \leq H$, est abélien. Il en résulte immédiatement que $(xy^{-1})^2 = 1$. Pour $p \geq 3$, K est régulier. Aussi, x^p et y commutent, donc

$$x^p = (x^p)^y = (x[x, y])^p,$$

or $|\langle x, [x, y] \rangle| < |K| \leq |G|$, l'hypothèse de récurrence implique que $[x, y]^p = 1$. Il en résulte que $\gamma_2(K) \leq \Omega_1(K)$, est d'exposant p. D'où K est p-abélien, et ainsi $(xy^{-1})^p = x^p y^{-p} = 1$. □

Démonstration de Théorème 1.3.6. On doit démontrer, pour tout $x, y \in G$ que

$$(xy^{-1})^{p^n} = 1 \Leftrightarrow x^{p^n} = y^{p^n} \text{ pour tout entier positif } n.$$

Pour $n = 1$, ceci est démontré dans Lemme 1.3.9. Supposons que cette propriété est vraie pour $n-1$, pour tous les p-groupes satisfaisant l'hypothèse du théorème. On a $(xy^{-1})^{p^n} = 1$ équivaut $(xy^{-1})^{p^{n-1}} = 1 \mod \Omega_1(G)$, par Lemme 1.3.7. En vertu de Lemme 1.3.8, ceci équivaut $x^{p^{n-1}} = y^{p^{n-1}} \mod \Omega_1(G)$. Il revient au même de dire que $(x^{p^{n-1}} y^{-p^{n-1}})^p = 1$, par Lemme 1.3.7. Finalement, par Lemme 1.3.9, ceci est équivalent à $x^{p^n} = y^{p^n}$. □

En particulier, le théorème précédent permet de généraliser le Théorème C de [35], qui coïncide avec le résultat suivant pour $n = 1$.

Corollaire 1.3.10. *Soit G un p-groupe. Si G est p-central de hauteur $p-2$ ou p^2-central de hauteur $p-1$; alors $|G : G^{p^n}| \leq \Omega_n(G)$, pour tout entier positif n.*

Suivant [33], on dit qu'un p-groupe G est *potent* si $\gamma_{p-1}(G) \leq G^p$ ($\gamma_2(G) \leq G^4$ pour $p = 2$). Ces groupes sont d'abord étudiés par D. E. Arganbright dans [8], et récemment par J. González-Sánchez et A. Jaikin-Zapirain dans [33]. Cette notion généralise celle d'un groupe puissant, et coïncide avec elle pour $p = 2, 3$. Il est démontré que si G est un p-groupe potent et $p \geq 3$, alors G satisfait, pour tout entier positif n, les trois propriétés qui suivent.

1. L'exposant de $\Omega_n(G)$ est au plus p^n ;
2. G^{p^n} coïncide avec les éléments de la forme g^{p^n}, $g \in G$;
3. $|G : G^{p^n}| = |\Omega_n(G)|$.

En général, on va appeler p-groupe avec une *p-structure régulière* tout p-groupe G qui satisfait les trois propriétés ci-dessus. Donc en particulier les p-groupes potents ont une p-structure régulière pour $p \geq 3$. C'est important de connaitre les p-groupes avec une p-structure régulière qui ne sont pas fortement semi-abéliens, ainsi que l'inverse.

Problème 6. *Supposons que G est un p-groupe potent et que p est impair. Est-ce que G est fortement semi-abélien ?*

Une réponse positive implique que tout p-groupe potent, possède un automorphisme non-intérieur d'ordre p ; ceci résulte de notre Théorème B, et d'un résultat de A. Abdollahi pour $p = 2$ (voir [2]). Notons qu'il suffit de montrer que G est semi-abélien pour avoir cette conséquence.

Nous terminons cette section par un problème posé par M. Y. Xu (voir [80, Problem 2]).

Problème 7. *Est ce que tout p-groupe semi-abélien est fortement semi-abélien ?*

1.4 Sur un probléme de Mingyao Xu

Xu avait demandé si un p-groupe G satisfaisant $p \geq 3$ et $\Omega_1(\gamma_{p-1}(G)) \leq \mathrm{Z}(G)$ a forcément une p-structure régulière (voir [80, Problem 3]). Pour cela il suffit de montrer que G^{p^n} coïncide avec l'ensemble des éléments de la forme x^{p^n}, $x \in G$. On a montré dans [10] que la réponse est négative. Celle-ci résulte du théorème important suivant du à D. Bubboloni and G. Corsi Tani (voir [18]).

Théorème 1.4.1. *Soient d et n deux entiers positifs et F le groupe libre à d générateurs. Fixons un nombre premier impair p et soit $G_n = F/\lambda_{n+1}(F)$, où $\lambda_{n+1}(F)$ désigne le $(n+1)$-ème terme de la suite p-centrale descendante de F. Alors G_n est un p-groupe p-central ; plus précisément on a $\Omega_1(G_n) = \lambda_n(F)/\lambda_{n+1}(F)$.*

On peut trouver l'analogue du résultat précédent dans l'article [35] (voir [35, Proposition 2.2 et Exemple 2.1]). On a mentionné dans le premier chapitre que la suite p-centrale descendante d'un p-groupe atteint 1 ; donc un p-groupe engendré par d éléments est un quotient de G_n pour certain n. Il en résulte

Corollaire 1.4.2. *Tout p-groupe, $p \geq 3$, est un quotient d'un p-groupe p-central.*

Le corollaire précédent répond en particulier à une question posée par A. Mann dans [62].

Corollaire 1.4.3. *Un p-groupe p-central, $p \geq 3$, n'a pas forcément une p-structure régulière.*

Démonstration. Sinon, tous les p-groupes G_n ont une p-structure régulière. Si les éléments de la forme x^p dans un groupe G forment un sous-groupe, alors ceci reste vrai pour tous les quotients de G. Il en résulte que pour tout p-groupe G, G^p coïncide avec l'ensemble des éléments de la forme x^p, $x \in G$. Une contradiction. □

Le corollaire précédent répond à la question de Xu ci-dessus mentionnée.

Signalons finalement une autre conséquence du Corollaire 1.4.2. La classe des p-groupes p-centraux est considérée comme la duale de la classe des p-groupes puissants. Un p-groupe G est dit puissant si $\gamma_2(G) \leq G^{2p}$. La limite projective d'un système de p-groupes puissants est un pro-p groupe avec une structure très rigide ; et ces pro-p groupes jouent un rôle capital dans la théorie des p-groupes analytiques p-adiques ([25]). Il est naturel de demander s'il y a quelques restrictions sur la structure d'une limite projective de p-groupes p-centraux.

Soit F un groupe libre de type fini. Tout sous-groupe normal de F d'indice une puissance de p, contient un sous-groupe $\lambda_n(F)$ pour certain n. Donc

$$\widehat{F}_p \cong \varprojlim F/\lambda_n^p(F)$$

où $\widehat{F}_p$ est la pro-p complétion de F. Donc le pro-p groupe libre $\widehat{F}_p$ est limite projective des p-groupes p-centraux. Ainsi, il n' y a aucune restriction raisonnable sur la structure d'une telle limite projective.

Chapitre 2

Groupes adjoints et groupes d'automorphismes

2.1 Groupes adjoints d'anneaux p-nuls

En général, un anneau A est un groupe abélien muni d'une multiplication $(x, y) \mapsto xy$, qui est bi-additive (il revient au même de dire qu'elle est distributive à gauche et à droite par rapport à l'addition).

Si la multiplication est associative, on dit que A est un anneau associatif, et désormais, par un anneau on entend un anneau associatif.

Un anneau avec un élément neutre pour la multiplication est dit unitaire. Dans ce cas, les éléments inversibles pour la multiplication forment un groupe $A^\times$, appelé le groupe des unités de A. Si A n'est pas unitaire, nous avons un analogue pour $A^\times$.

Définition 2.1.1. *Soit A un anneau. La loi adjointe de A est définie par $x \circ y = x + y + xy$. Pour celle-ci l'ensemble A est un monoïde d'élément neutre 0 ; le groupe des éléments inversibles dans ce monoïde est le groupe adjoint de l'anneau A, et est noté A°.*

Si A est unitaire, l'application $x \mapsto 1 + x$ définit un isomorphisme du groupe adjoint A° dans $A^\times$.

Un anneau A pour lequel les ensembles A et A° coïncident, est dit radical. Cette terminologie est liée au radical de Jacobson $\mathrm{J}(A)$ de A qui peut être défini en général comme le plus grand idéal contenu dans A°. Donc A est radical si et seulement si $\mathrm{J}(A) = A$. Les groupes adjoints des anneaux radicaux sont des objets intéressants à étudier, et le lecteur doit trouver plusieurs études dans ce contexte dans la littérature (voir la bibliographie de [24] pour quelques références). En particulier, ils ont quelques applications aux groupes factorisés (voir [7, §6]).

Par un idéal de A on entend une partie qui est à la fois un idéal à gauche et à droite. Le produit IJ de deux idéaux I et J de A, est le sous-groupe

additif de A engendré par tous les éléments ij, $i \in I$ et $j \in J$. C'est simple de voir que IJ est encore un idéal de A, et que le produit des idéaux est associatif. Ce produit permet de définir une suite canonique d'idéaux de A :

$$A^1 = A \quad \text{et} \quad A^{n+1} = A^n A, \text{ pour } n \geq 1.$$

L'associativité du produit implique que $A^{n+m} = A^n A^m$, pour $n, m \geq 1$. Aussi, A^n coïncide avec le sous-groupe additif engendré par tous les produits de n éléments de A. On peut définir A^0 comme un idéal formel qui satisfait $A^0 I = I A^0 = I$, pour tout idéal I de A.

Définition 2.1.2. *Un anneau A est dit nilpotent si $A^{n+1} = 0$, pour certain entier non-négatif n. Le plus petit entier n qui vérifie cette propriété s'appelle la classe de nilpotence de A.*

Notons que tout anneau nilpotent A est radical. En effet, dans ce cas tout élément x de A est nilpotent, et donc $x \in A^\circ$; puisque si $x^n = 0$ pour certain n, alors $x \circ \sum_{i=1}^{n-1} (-1)^i x^i = 0$.

Proposition 2.1.3 ([55, Theorem 1.6.4])**.** *Le groupe adjoint d'un anneau nilpotent de classe n est nilpotent de classe au plus n.*

En effet, la suite

$$0 \lhd (A^n)^\circ \lhd \cdots \lhd (A^2)^\circ \lhd A^\circ$$

est centrale dans A°. Ceci résulte immédiatement de l'identité :

$$x' \circ y' \circ x \circ y = y'x - x'y + x'y'x + y'xy + x'y'xy$$

pour tout $x, y \in A$; et x' désigne l'inverse de x dans A°.

Dans la suite de cette section, p désigne un nombre premier fixé.

Définition 2.1.4. *Soient A un anneau, et $i, j, k \in \mathbb{N}$. On dit que A est (i, p^j, k)-nul si $R^i \Omega_j(R) R^k = 0$.*

Une version plus particulière de cette définition est introduite par l'auteur et B. Daoud dans [39].

Lemme 2.1.5. *Soit A un anneau (i, p^j, k)-nul. Alors A est (ni, p^{nj}, nk)-nul, pour tout entier positif n.*

Démonstration. Pour $n = 1$, le résultat n'est que la définition. Supposons que ce résultat est démontré pour n. Or $p^j \Omega_{(n+1)j}(A) \leq \Omega_{nj}(A)$, on a par récurrence $A^{ni}(p^j \Omega_{(n+1)j}(A)) A^{nk} = 0$, et donc $A^{ni} \Omega_{(n+1)j}(A) A^{nk} \leq \Omega_j(A)$. Il en résulte que

$$A^i A^{ni} \Omega_{(n+1)j}(A) A^{nk} A^k = A^{(n+1)i} \Omega_{(n+1)j}(A) A^{(n+1)k} = 0.$$

□

Proposition 2.1.6. *Soit A un p-anneau. Si A est (i, p^j, k)-nul, pour certain $j \geq 1$; alors tout élément de A est nilpotent, et en particulier A est radical.*

Démonstration. Soit $x \in A$. On a $p^n x = 0$ pour certain $n \in \mathbb{N}$. Il en résulte que $x \in \Omega_{nj}(R)$, et par Lemme 2.1.5, on a $x^{n(i+k)+1} = 0$. □

En général, un p-anneau (i, p^j, k)-nul n'est pas forcément nilpotent. En effet, soit $A = \prod_{n\geq 1} p\mathbb{Z}/p^n\mathbb{Z}$. Alors A est $(0, p, 1)$-nul ; et comme il est commutatif, A est (i, p^j, k)-nul, pour tous $i, j, k \in \mathbb{N}$ tels que i, j ou j, k sont positifs ; mais on a $A^m \cong \prod_{n>m} p^m\mathbb{Z}/p^n\mathbb{Z}$, pour tout $m \geq 1$; d'où A n'est pas nilpotent. En revanche on a

Proposition 2.1.7. *Soit A un anneau dont le groupe additif A^+ est d'exposant fini p^m. Si A est (i, p^j, k)-nul, pour certain $j \geq 1$, alors A est nilpotent de classe au plus égale à $\lceil \frac{m}{j} \rceil (i + k)$.*

Démonstration. Soit $n = \lceil \frac{m}{j} \rceil$. Comme $m = \frac{m}{j} j \leq nj$, on a $A = \Omega_{nj}(A)$; donc d'après Lemme 2.1.5, $A^{ni} A A^{nk} = A^{n(i+k)+1} = 0$.

□

En vertu de Proposition 2.1.3, on a

Corollaire 2.1.8. *Soit A un anneau dont le groupe additif A^+ est d'exposant fini p^m. Si A est (i, p^j, k)-nul, pour certain $j \geq 1$, alors le groupe adjoint A° est nilpotent de classe au plus égale à $\lceil \frac{m}{j} \rceil (i + k)$..*

Tout sous-anneau d'un anneau (i, p^j, k)-nul est encore (i, p^j, k)-nul. Ceci n'est pas évident pour les anneaux quotients, mais il reste vrai pour certains d'eux.

D'abord, définissons l'annihlateur $\mathfrak{A}(A)$ d'un anneau A,

$$\mathcal{U}(A) = \{x \in A \quad | \quad xA = Ax = 0\}$$

qui est un idéal de A. On peut généraliser cette notion, est définir la suite d'idéaux :

$$\mathcal{U}_0(A) = 0 \quad \text{et} \quad \mathcal{U}_{n+1}(A)/\mathcal{U}_n(A) = \mathcal{U}(A/\mathcal{U}_n(A))$$

Notons que A est nilpotent si et seulement $\mathcal{U}_n(A) = 0$ pour certain entier non-négatif n. Dans ce cas la classe de nilpotence de A coïncide avec le plus petit entier n qui vérifie $\mathcal{U}_n(A) = 0$.

Proposition 2.1.9. *Soit A un anneau (i, p^j, k)-nul. Alors*

(i) *l'anneau quotient $A/\mathcal{U}_n(A)$ est (i, p^j, k)-nul, pour tout $n \in \mathbb{N}$;*

(ii) *l'anneau quotient $A/\Omega_n(A)$ est (i, p^j, k)-nul, pour tout $n \in \mathbb{N}$;*

(iii) *si (M_t) est une famille d'idéaux de A, telle que A/M_t soit (i,p^j,k)-nul pour tout i, alors $A/\cap_t M_t$ est (i,p^j,k)-nul.*

Démonstration. (i) Le résultat est trivial pour $n=0$. Supposons que $n=1$. Si $x\mathfrak{A}(A) \in \Omega(A/\mathcal{U}(A))$, alors $p^j x \in \mathcal{U}(A)$. Donc $p^j(xA) = p^j(Ax) = 0$, ce qui signifie que xA et Ax sont inclus dans $\Omega_j(A)$. L'hypothèse sur A implique que $A^i(xA)A^k = (A^ixA^k)A = 0$ et $A^i(Ax)A^k = A(A^ixA^k) = 0$, d'où $A^ixA^k \subseteq \mathcal{U}(A)$. Nous avons $(A/\mathcal{U}(A))^k = A^k\mathcal{U}(A)/\mathcal{U}(A)$, donc $(A/\mathcal{U}(A))^i x\mathcal{U}(A)(A/\mathcal{U}(A))^k = 0$, ce qui montre que $A/\mathcal{U}(A)$ est (i,p^j,k)-nul. Maintenant par récurrence sur n, si le résultat est vrai pour $n-1$, alors $(A/\mathcal{U}_{n-1}(A))/\mathcal{U}(A/\mathcal{U}_{n-1}(A))$ est (i,p^j,k)-nul. Nous avons $\mathcal{U}(A/\mathcal{U}_{n-1}(A)) = \mathcal{U}_n(A)/\mathcal{U}_{n-1}(A)$, et

$$(A/\mathcal{U}_{n-1}(A))/(\mathcal{U}_n(A)/\mathcal{U}_{n-1}(A)) \cong A/\mathcal{U}_n(A).$$

Ceci montre que $A/\mathcal{U}_n(A)$ est (i,p^j,k)-nul.

(ii) Si $x\Omega_n(A) \in \Omega_j(A/\Omega_n(A))$, alors $p^jx \in \Omega_n(A)$. Donc $p^n(p^jx) = p^j(p^nx) = 0$, et par suite $p^nx \in \Omega_j(A)$, ce qui implique $p^n(A^ixA^k) = 0$. Nous avons alors $A^ixA^k \subseteq \Omega_n(A)$, ce qui implique que $A/\Omega_n(A)$ est (i,p^j,k)-nul.

(iii) Soit $M = \cap_t M_t$. Si $xM \in \Omega(A/M)$, alors $p^jx \in M$, et ainsi $p^jx \in M_t$, pour tout indice t. Il en résulte que $A^ixA^k \subseteq M_t$ pour tout indice t, d'où $A^ixA^k \subseteq M$. Donc A/M est (i,p^j,k)-nul.

□

Le troisième résultat dans la proposition ci-dessus montre que tout anneau A contient un plus petit idéal $L_{(i,p^j,k)}(A)$ tel que $A/L_{(i,p^j,k)}(A)$ est (i,p^j,k)-nul. En effet, il suffit de prendre $L_{(i,p^j,k)}(A)$ égal à l'intersection de tous les idéaux I de A pour lesquels A/I est (i,p^j,k)-nul. On peut l'appeler le (i,p^j,k)-résiduel de A, bien qu'on n'aille pas le discuter ultérieurement.

Lorsque $i+k$ est petit par rapport à p, la p-structure de A°, où A est un anneau (i,p^j,k)-nul, est totalement contrôlée par celle de A^+. Cette assertion est précisée dans le théorème suivant. Une version particulière de ce résultat peut être trouvée dans [39].

Théorème 2.1.10. *Soit A un p-anneau fini. Supposons que A est (i,p^j,k)-nul, où $i+k \leq p-2$ et $j \geq 1$ ou bien $i+k \leq p-1$ et $j \geq 2$. Alors $\Omega_{\{n\}}(A^\circ) = \Omega_n(A^+)$, pour tout $n \geq 1$. En particulier on a $\Omega_{\{n\}}(A^\circ) = \Omega_n(A^\circ)$, pour tout $n \geq 1$.*

Démonstration. Notons par $x^{(k)}$ la puissance k-ème d'un élément x dans le groupe A°.

Supposons d'abord que $n=1$. On a $px=0$ implique que $x^{i+k+1}=0$, et comme $i+k+1 \leq p$, on a $x^p = 0$. Il en résulte

$$x^{(p)} = \sum_{t=1}^{p} \binom{p}{t} x^t = \sum_{t=1}^{p-1} \binom{p}{t} x^t = 0,$$

ceci montre que $\Omega_1(A^+) \subseteq \Omega_{\{1\}}(A^\circ)$. On va démontrer l'inclusion inverse par récurrence sur l'ordre de A. Soit $U = \Omega_1(A^+) \cap \mathcal{U}(A)$. D'après Proposition 2.1.7, A est nilpotent, donc $U \neq 1$; de plus A/U est (i, p^j, k)-nul d'après Proposition 2.1.9. Si $x^{(p)} = 0$, alors par récurrence on doit supposer que $px \in U$; d'où $pxy = 0$, pour tout $y \in A$ et $p^2x = 0$. Si $j \geq 2$, alors $x^p = 0$; et si $j = 1$ et $i + k \leq p - 2$ alors $x^{2+i+k} = 0$, et donc $x^p = 0$. Nous avons alors

$$0 = x^{(p)} = \sum_{i=1}^{p} \binom{p}{i} x^i = px$$

ceci démontre l'inclusion $\Omega_{\{1\}}(A^\circ) \subseteq \Omega_1(A^+)$.

Maintenant on raisonne par récurrence sur n. Si $x \in \Omega_n(A^+)$, alors $px \in \Omega_{n-1}(A^+)$. Ceci implique que $x+\Omega_{n-1}(A^+) \in \Omega_1((A/\Omega_{n-1}(A^+))^+)$. Proposition 2.1.9 (ii) et l'étape $n = 1$ implique $x+\Omega_{n-1}(A^+) \in \Omega_{\{1\}}((A/\Omega_{n-1}(A^+))^\circ)$. Donc $x^{(p)} \in \Omega_{n-1}(A^+)$, et par récurrence $x^{(p)} \in \Omega_{\{n-1\}}(A^\circ)$. D'où $x \in \Omega_{\{n\}}(A^\circ)$. Il en résulte que $\Omega_n(A^+) \subseteq \Omega_{\{n\}}(A^\circ)$. L'inclusion inverse découle de la même façon.

Finalement, l'égalité $\Omega_n(A^\circ) = \Omega_{\{n\}}(A^\circ)$ résulte du fait que $(\Omega_n(A^+))^\circ$ est un sous-groupe de A° et $\Omega_n(A^\circ)$ est engendré par $\Omega_{\{n\}}(A^\circ)$. □

On va montrer dans la section suivante que, dans un sens, on ne peut pas améliorer le théorème précédent.

Le résultat suivant peut être considéré comme une généralisation de [39, Theorem B].

Théorème 2.1.11. *Soient A un p-anneau fini et H un sous-groupe de A°. Supposons que A est (i, p^j, k)-nul, où $i+k \leq p-2$ et $j \geq 1$ ou bien $i+k \leq p-1$ et $j \geq 2$. Alors $|H : H^p| \leq |\Omega_1(H)|$.*

Démonstration. Supposons que A est un contre exemple d'ordre minimal. Donc pour certain sous-groupe H de A°, on a $|H : H^p| > |\Omega_1(H)|$; supposons que H est minimal pour cette propriété. On va démontrer que ces hypothèses produisent une contradiction.

Soit $U = \mathcal{U}(A) \cap \Omega_1(A^+)$. En vertu de Proposition 2.1.7, $\mathcal{U}(A)$ n'est pas trivial, et donc U n'est pas trivial. Proposition 2.1.9 implique que Théorème 2.1.11 est vrai pour l'anneau A/U. Or $U^+ \cong U^\circ$, on va noter les deux par U. On a $HU/U \cong H/H \cap U$ est un sous-groupe de $A^\circ/U = (A/U)^\circ$, donc

$$|(H/H \cap U) : (H/H \cap U)^p| \leq \Omega_1(H/H \cap U). \tag{2.1}$$

Soit $K/H\cap U = \Omega_1(H/H\cap U)$. Supposons d'abord que $K < H$, donc par minimalité de H on a $|K : K^p| \leq |\Omega_1(K)|$; et puisque $K/H\cap U \cong \Omega_1(HU/U)$ on a d'après Théorème 2.1.10, $K^p \leq H \cap U$, et évidement $K^p \leq H^p$, donc $K^p \leq H^p \cap U$. Ceci implique que

$$|K : H^p \cap U| \leq |\Omega_1(K)| \leq |\Omega_1(H)|; \tag{2.2}$$

on a

$$(H/H\cap U)^p = H^p(H\cap U)/H\cap U \cong H^p/H^p\cap U$$

donc l'inégalité (2.1) peut être s'écrit

$$\frac{|H:H^p||H^p\cap U|}{|H\cap U|} \leq \frac{K}{|H\cap U|},$$

celle ci avec l'inégalité (2.2) implique que $|H:H^p| \leq |\Omega_1(H)|$, ce qui contredit l'hypothèse sur H. Donc on doit supposer que $K = H$, ce qui revient à dire que HU/U est d'exposant p, ce qui implique d'après Théorème 2.1.10 que $HU/U \subseteq \Omega_1((A/U)^+)$. Pour $p \geq 3$, Proposition 2.1.7 implique que $\Omega_1((A/U)^+)$ est nilpotent de classe au plus $p-2$, donc $H/H\cap U$ est de classe au plus égale à $p-2$; et puisque $H\cap U$ est contenu dans le centre de H il en résulte que H est nilpotent de classe au plus $p-1$, donc il est régulier (voir Proposition 1.3.4(c)), ceci produit une contradiction (voir Proposition 1.3.4(b)). On doit alors supposer que $p = 2$. On a HU/U et U sont d'exposant 2, d'où H est d'exposant au plus 4, ce qui implique d'après Théorème 2.1.10 que $H \subseteq \Omega_2(A)$, mais $\Omega_2(A)^2 = 0$ par définition de A. Ceci montre que H est abélien, ce qui entraine la dernière contradiction. □

Corollaire 2.1.12. *Soient A un p-anneau fini et H un sous-groupe de A°. Supposons que A est $(0, p, p-\epsilon)$-nul ou $(p-\epsilon, p, 0)$-nul, où $\epsilon = 2$ si $p \geq 3$, et $\epsilon = 1$ si $p = 2$. Alors* $\mathrm{d}(H) \leq \mathrm{d}(A^+)$.

Démonstration. Or H est un p-groupe, on a

$$p^{\mathrm{d}(H)} = |H : H'H^p| \leq |H : H^p| \leq |\Omega_1(H)|.$$

Théorème 2.1.10 implique que $\Omega_1(H) \subset \Omega_1(A^+)$; et $|\Omega_1(A^+)| = p^{\mathrm{d}(A^+)}$. D'où $\mathrm{d}(H) \leq \mathrm{d}(A^+)$.

□

2.2 Rang du groupe adjoint d'un anneau, et une conjecture de O. Dickenschied

Rappelons que *le rang (de Prüfer)* d'un groupe G est le plus petit entier $r = r(G)$ tel que tout sous-groupe de type fini de G peut être engendré par r éléments (si un tel entier n'existe pas on pose $r(G) = \infty$). Supposons que A est un anneau radical. Il est démontré dans [6] que si $r(A^\circ)$ est fini, alors $r(A^+)$ est fini et borné en terme de $r(A^\circ)$ seulement. La réciproque n'est pas forcément vraie comme le montre un exemple due à Ya. Sysak (voir [7, Proof of Theorem 6.1.2]).

En revanche, O. Dickenschied (voir [24]) a démontré que si, en plus, tout élément de A est nilpotent, ou si le groupe additif de A est périodique,

alors la réciproque est vraie. Plus précisément, il a démontré sous l'une des conditions précédentes que $r(A^\circ) \leq \epsilon r(A^+)$, où $\epsilon = 2$ si A^+ne contient aucune involution, et $\epsilon = 3$ sinon. Le problème peut être réduit, sous l'une des conditions précédentes, au cas où A est un p-anneau nilpotent fini (p un nombre premier) ; et encore, il suffit d'établir l'inégalité $r(A^\circ) \leq \epsilon r(A^+)$ dans ce cas. La démonstration de cette dernière est basée sur un lemme technique sur les séries formelles, et sur une propriété des p-groupes puissants (powerful p-groups). Dans [39], on a établi cette inégalité pour tous les p-anneaux finis, sans supposer qu'ils sont nilpotents. Notre approche est différente et est basée sur une version plus faible du Corollaire 2.1.12(voir [39, Corollary B]).

Proposition 2.2.1. *Soient A un p-anneau fini, et P un p-sous-groupe de Sylow de A°. Alors $r(P) \leq \epsilon r(A^+)$, où $\epsilon = 2$ si $p \geq 3$ et $\epsilon = 3$ si $p = 2$.*

Démonstration. Notons d'abord que $U = p'R$ est un p-anneau $(0, p, 1)$-nul ; où $p' = p$ si $p \geq 3$, et $p' = 4$ si $p = 2$. En effet, soient $x, y \in U$ tels que $p'x = 0$. On peut écrire $y = p'a$ pour certain $a \in A$; donc $xy = x(p'a) = (p'x)a = 0$. Soit H un p-sous-groupe de A°. Alors

$$\mathrm{d}(H) \leq \mathrm{d}(H/H \cap U^\circ) + \mathrm{d}(H \cap U^\circ).$$

Corollaire 2.1.11 implique que $\mathrm{d}(H \cap U^\circ) \leq \mathrm{d}(U^+) \leq \mathrm{d}(A^+)$. D'autre part, $H/H \cap U^\circ \cong HU^\circ/U^\circ$ est un sous-groupe de $A^\circ/U^\circ \cong (A/U)^\circ$, d'où

$$p^{\mathrm{d}(H/H\cap U^\circ)} \leq |(A/U)^\circ| \leq |A/U|.$$

Maintenant, si $p > 2$ alors $|A/U| = p^{\mathrm{d}(A^+)}$; et si $p = 2$ alors

$$|A/U| = |A/2A||2A/4A| = p^{d(A^+)}p^{d((2A)^+)} \leq p^{2d(A^+)}.$$

Ceci achève la démonstration. □

Le théorème qui suit, réfute la conjecture suivante de O. Dickenschied (voir [24, Remark (b)]) :

Conjecture 2.2.2. *Soit A un p-anneau nilpotent fini. Alors $r(A^\circ) \leq \epsilon r(A^+)$, où $\epsilon = 1$ si $p \geq 3$ et $\epsilon = 2$ si $p = 2$.*

D'abord, on a besoin de quelques notations. La lettre R désigne un anneau commutatif et unitaire fini. On note $I_p(R)$ l'idéal de R défini par :

$$I_p(R) = \{a + pb \,|\, a, b \in R \text{ and } pa = 0\}.$$

L'application $a \mapsto (a^p - a) + I_p(R)$, détermine un homomorphisme de R^+ dans le groupe additif de l'anneau quotient $R/I_p(R)$; on note $K_p(R)$ son noyau. Donc $K_p(R)$ est l'ensemble des éléments $a \in R$ satisfaisant $a^p - a \in I_p(R)$, et $K_p(A)$ est un sous-groupe additif de A.

L'idéal de $R[X]$ engendré par les deux polynômes X^{p+1} and X^p+pX sera noté $J_p(R,X)$; et $A_p(R,X)$ désignera l'anneau quotient $XR[X]/J_p(R,X)$. Pour un polynôme $f(X)=\sum_{i=0}^n a_iX^i \in R[X]$, on note $\omega(f)$ le plus petit indice i tel que $a_i \neq 0$ (on pose $\omega(f)=+\infty$ si $f(X)=0$).

Théorème 2.2.3. *L'anneau $A=A_p(R,X)$ est nilpotent de classe au plus p. Et si R est fini d'ordre une puissance de p et R^+ n'est pas élémentaire abélien alors $r(A^\circ) > r(A^+)$; de plus, l'entier positif $r(A^\circ)-r(A^+)$ peut avoir des valeurs arbitrairement grandes.*

Démontrons d'abord le lemme suivant.

Lemme 2.2.4. *Soit $a \in R$. Alors le polynôme aX^p appartient à $J_p(R,X)$ si, et seulement si, $a \in I_p(R)$.*

Démonstration. Supposons que aX^p appartient à $J_p(R,X)$, alors $R[X]$ contient deux polynômes $f(X)=\sum_{i=0}^n a_iX^i$ et $g(X)=\sum_{i=0}^m b_iX^i$, tels que

$$aX^p = pf(X)X + f(X)X^p + g(X)X^{p+1}$$

ceci implique en particulier que

$$pa_{p-1}+a_0=a \quad \text{et} \quad pa_0=0$$

d'où $a \in I_p(R)$. Inversement, si $a \in I_p(R)$, alors a peut s'écrire $a=b+pc$, où $b,c \in A$ et $pb=0$. Donc

$$aX^p = bX^p + pcX^p = -(pb)X + c(pX^p) = c(pX^p) \mod J_p(R,X)$$

or $X^{p+i}+pX^{i+1} \in J_p(R,X)$, et $X^{p+i} \in J_p(R,X)$, pour tout $i \geq 1$. Il en résulte que $pX^p \in J_p(R,X)$, d'où $aX^p \in J_p(R,X)$. □

Puisque R is commutatif, il en résulte que $A=A_p(R,X)$ est commutatif. Donc A° est un groupe abélien. Soient $\Omega^+(A)$ et $\Omega^\circ(A)$ les sous-groupes engendrés par les éléments d'ordre p dans A^+ et A° respectivement.

Proposition 2.2.5. *Soient $f=\sum_{i=1}^n a_iX^i \in XR[X]$, et $\bar{f}$ son image dans $A=A_p(R,X)$. Alors*

1. *$\bar{f} \in \Omega^\circ(A)$ si, et seulement si, $a_1 \in K_p(R)$;*
2. *$\bar{f} \in \Omega^+(A)$ si, et seulement si, $a_1 \in I_p(R)$;*
3. *l'application $\sum_{i=1}^n a_iX^i \mapsto a_1$ induit un isomorphisme de $A^+/\Omega^+(A)$ sur $R^+/I_p(R)$. De plus, $\Omega^\circ(A)$ est un sous-groupe de A^+ et $\Omega^\circ(A)/\Omega^+(A)$ est isomorphe à $K_p(R)/I_p(R)$.*

Démonstration. (1) Soit $f^{(p)}$ la $p^{ème}$ puissance de f dans le groupe adjoint de $XR[X]$. On a

$$f^{(p)} = \sum_{i=1}^{p} \binom{p}{i} f^i = pa_1X + pg(X) + {a_1}^p X^p + h(X),$$

où $\omega(g) \geq 2$, and $\omega(h) \geq p+1$. Or $pX^i \in J_p(R,X)$, pour tout $i \geq 2$, il en résulte que $pg(X) \in J_p(R,X)$. Aussi, $J_p(R,X)$ contient $h(X)$, car il contient X^{p+1}. Donc

$$f^{(p)} = a_1(pX) + {a_1}^p X^p = ({a_1}^p - a_1)X^p \mod J_p(R,X).$$

D'où $\bar{f} \in \Omega^\circ(A)$ si, et seulement si, $({a_1}^p - a_1)X^p \in J_p(R,X)$, ce qui revient à dire que ${a_1}^p - a_1 \in I_p(R)$ d'après Lemme 2.2.4, et ainsi par définition $a_1 \in K_p(R)$.

(2) On a

$$pf = pa_1X = -a_1X^p \mod J_p(R,X).$$

Donc d'après Lemme 2.2.4, $\bar{f} \in \Omega^+(A)$ si, et seulement si, $a_1 \in I_p(R)$.

(3) Soit Φ la relation qui associe à tout élément $\bar{f} \in A$, l'élément $a_1 + I_p(R)$ de $R/I_p(R)$; où $f = \sum_{i=1}^{n} a_iX^i$. c'est simple de voir que si $g = \sum_{i=1}^{n} b_iX^i \in XR[X]$ est égal à f modulo $J_p(R,X)$, c'est à dire $\bar{f} = \bar{g}$, alors $b_1 - a_1 \in pR$; donc en particulier $b_1 - a_1 \in I_p(R)$. Ceci montre que Φ est une application bien définie. Il en résulte que Φ est un épimorphisme entre A^+ et le groupe additif de additive $R/I_p(R)$, et par (2) le noyau de Φ est $\Omega^+(A)$; ainsi Φ induit un isomorphisme entre $A^+/\Omega^+(A)$ et $R/I_p(R)$. Maintenant par (1) Φ applique $\Omega^\circ(A)$ exactement sur $K_p(R)$. D'où le résultat. □

Démonstration de Théorème 2.2.3 . Pour tout $f, g \in R[X]$, on a $\omega(fg) \geq \omega(f) + \omega(g)$. Ceci implique que $\omega(f_1f_2 \ldots f_{p+1}) \geq p+1$, chaque fois qu'on a une suite d'éléments $f_1, f_2 \ldots, f_{p+1}$ dans $XR[X]$. Il en résulte de $X^{p+1} \in J_p(R,X)$, que A est nilpotent de classe au plus égale à p.

Or R est fini, il en résulte que A^+ ainsi que A° sont des p-groupes abéliens finis, d'où $\Omega^+(A) = p^{r(A^+)}$ et $\Omega^\circ(A) = p^{r(A^\circ)}$. Donc $p^{r(A^\circ)-r(A^+)}$ est égal à l'ordre de $K_p(R)/I_p(R)$. Supposons que R est fini d'ordre une puissance de p et R^+ n'est pas élémentaire abélien. D'après Proposition 2.2.5 (3), il suffit de montrer que $K_p(R)/I_p(R)$ n'est pas trivial. On a $1 \in K_p(R)$; mais $1 \notin I_p(R)$. En effet, sinon on peut écrire $1 = b + pc$, où $b, c \in R$ et $pb = 0$. Soit $p^n > p$ l'ordre de 1 dans R^+ ; alors $p^{n-1}1 = p^{n-1}b + p^nc = 0$, contradiction.

Finalement, soit R le produit direct de m copies de $\mathbb{Z}_{p^2}$. Alors l'anneau $R/I_p(R)$ est isomorphe à un produit de m copies du corps $\mathbb{Z}_p$. Or tout élément de $\mathbb{Z}_p$ satisfait l'équation $X^p = X$, il en résulte que $x^p = x$ pour tout $x \in R/I_p(R)$. Donc $|K_p(R)/I_p(R)| = p^m$, et ainsi

$$r(A^\circ) - r(A^+) = m.$$

D'où $r(A^\circ) - r(A^+)$ peut être arbitrairement grand. □

On a mentionné dans la section précédente que le Théorème 2.1.10 ne peut pas être amélioré et voici l'illustration. D'abord notons que si A est $(0,p,p-1)$-nul ou $(p-1,p,0)$-nul, alors il est vrai que $\Omega_n(A^+) \subseteq \Omega_{\{n\}}(A^\circ)$, pour tout entier positif n. Ceci devient faux une fois que $p-1$ est remplacé par p. En effet, soit A l'anneau des matrices triangulaires supérieures de type $(p+1)\times(p+1)$ sur le corps $\mathbb{Z}_p$. On a $\Omega_1(A^+) = A$ et $AA^p = A^pA = 0$, donc A est $(p-1,p,0)$-nul et aussi $(0,p,p-1)$-nul. Considérons l'élément $a \in A$ donné par

$$a = \begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}.$$

Pour tout entier positif n, on a

$$(\mathbf{1}+a)^n = \begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{p} \\ & 1 & \binom{n}{1} & \ddots & \vdots \\ & & \ddots & \ddots & \binom{n}{2} \\ & & & 1 & \binom{n}{1} \\ & & & & 1 \end{pmatrix}$$

où $\mathbf{1}$ désigne la matrice unitaire. Donc $(\mathbf{1}+a)^p = \mathbf{1} + a^{(p)} \neq \mathbf{1}$. Ceci montre que $a \notin \Omega_{\{1\}}(A^\circ)$.

L'inclusion $\Omega_n(R^\circ) \subseteq \Omega_{\{n\}}(R^+)$ ne marche pas pour tous les A qui sont $(0,p,p-1)$-nuls ou $(p-1,p,0)$-nuls. En effet, soit $A = A_p(R,X)$, où R satisfait la condition du Théorème 2.2.3. On a vu que $\Omega_{\{1\}}(A^\circ)$ contient $\Omega_1(A^+)$ strictement. Montrons que A est $(0,p,p-1)$-nul (et donc $(p-1,p,0)$-nul). Soient $f, g_1, .., g_{p-1} \in XA[X]$ tels que $pf = p(\sum_{i=1}^n a_i X^i) \in J_p(R,X)$. On a $pa_iX^i \in J_p(R,X)$, pour $i \geq 2$, donc

$$pf = pa_1X = -a_1X^p = 0 \mod J_p(R,X).$$

D'autre part, on a

$$g_1...g_{p-1} = bX^{p-1} + \text{ termes supérieurs},$$

où $b \in A$. Il en résulte

$$fg_1...g_{p-1} = a_1bX^p = b(a_1X^p) = 0 \mod J_p(R,X).$$

D'où le résultat.

2.3 Applications aux groupes d'automorphismes de p-groupes

2.3.1 Anneaux de dérivations et leurs groupes adjoints

Soit N un sous-groupe de G. Notons $\mathrm{End}_N(G)$ l'ensemble des endomorphismes u de G tels que $x^{-1}u(x) \in N$, pour tout $x \in G$; en d'autres termes, $End_N(G)$ est l'ensemble de tous les endomorphismes qui laissent chaque classe (à gauche) modulo N invariante. C'est simple de voir que $\mathrm{End}_N(G)$ est un monoïde pour la composition usuelle des applications. Soit $\mathrm{Aut}_N(G)$ l'ensemble des automorphismes de G appartenant à $\mathrm{End}_N(G)$. Alors $\mathrm{Aut}_N(G)$ est un sous-groupe de $\mathrm{Aut}(G)$, qui coïncide avec le groupe des éléments inversibles dans le monoïde $\mathrm{End}_N(G)$.

Supposons que N est normal et abélien ; alors on peut le voir comme un G-module avec l'action $n^x = x^{-1}nx$, $x \in G$ et $n \in N$.

On appelle dérivation (homomorphisme croisé) de G dans N toute application $\delta : G \to N$ qui vérifie

$$\delta(xy) = \delta(x)^y\delta(y), \quad \text{pour tout } x, y \in G.$$

On note l'ensemble de ces dérivations par $\mathrm{Der}(G, N)$. Cet ensemble a une structure de groupe abélien pour la loi $(\delta_1 + \delta_2)(x) = \delta_1(x)\delta_2(x)$, où $\delta_1, \delta_2 \in \mathrm{Der}(G, N)$ et $x \in G$. On peut aussi définir une multiplication sur $\mathrm{Der}(G, N)$ par $(\delta_1\delta_2)(x) = \delta_2(\delta_1(x))$. On vérifie aisément que $\mathrm{Der}(G, N)$ est un anneau pour ces deux lois.

Maintenant, à chaque endomorphisme $u \in \mathrm{End}_N(G)$ on peut associer une dérivation $\delta_u \in \mathrm{Der}(G, N)$, définie par $\delta_u(x) = x^{-1}u(x)$, pour tout $x \in G$. Aussi, toute dérivation $\delta \in \mathrm{Der}(G, N)$ définit un endomorphisme $1 + \delta = u \in \mathrm{End}_N(G)$, donné par $u(x) = x\delta(x)$, pour tout $x \in G$.

Les détails de la preuve du résultat suivant sont laissés au lecteurs.

Proposition 2.3.1. *([57, Lemma 3.1]) Sous les notations ci-dessus, l'application $u \mapsto \delta_u$ est un isomorphisme du monoïde $\mathrm{End}_N(G)$ dans le monoïde adjoint de l'anneau $\mathrm{Der}(G, N)$. En particulier, ceci induit un isomorphisme entre $\mathrm{Aut}_N(G)$ et le groupe adjoint de $\mathrm{Der}(G, N)$.*

Cette relation a été établie pour la première fois par H. Laue dans [57]. Elle a été aussi établie (indépendamment) par l'auteur et B. Daoud dans [39] ; et au moins implicitement dans [20] par A. Caranti et S. Mattarei. Pour simplifier l'exposition, on va appeler l'homomorphisme défini dans la proposition précédente *l'isomorphisme de Laue*. Effectivement il y a deux isomorphismes de Laue, un isomorphisme de monoïdes et un autre de groupes, mais on pense que ceci ne produit aucune confusion.

Soit M sous-groupe normal de G qui commute avec N. Donc on peut voir N comme un G/M-module. L'épimorphisme canonique $s : G \longrightarrow G/N$

induit un homomorphisme injectif d'anneaux qui associe à $\delta \in \mathrm{Der}(G/M, N)$ la dérivation $\delta \circ s \in \mathrm{Der}(G, N)$. On va identifier $\mathrm{Der}(G/M, N)$ à son image par cet homomorphisme, ceci étant le sous-anneau de $\mathrm{Der}(G, N)$ des dérivations qui s'annulent sur M. Comme une dérivation $\delta \in \mathrm{Der}(G, N)$ s'annule sur M si et seulement si son endomorphisme associé $1 + \delta$ fixe tous les éléments de M, on a

Corollaire 2.3.2. *Sous les notations ci-dessus, l'isomorphisme de Laue induit un isomorphisme entre le sous-monoïde des endomorphismes dans* $\mathrm{End}_N(G)$ *qui fixent tous les éléments de* M *et le monoïde adjoint de* $\mathrm{Der}(G/M, N)$. *En particulier, ceci induit un isomorphisme entre le groupe des automorphismes dans* $\mathrm{Aut}_N(G)$ *qui fixent tous les éléments de* M *et le groupe adjoint de* $\mathrm{Der}(G/M, N)$.

Si M contient N, alors la multiplication dans l'anneau $\mathrm{Der}(G/M, N)$ et triviale, et donc le groupe adjoint de l'anneau $\mathrm{Der}(G/M, N)$ coïncide avec son groupe additif. Ceci implique

Corollaire 2.3.3. *Sous les notations ci-dessus, et si* $N \leq M$, *alors l'isomorphisme de Laue induit un isomorphisme entre le groupes des automorphismes dans* $\mathrm{Aut}_N(G)$ *qui fixent tous les éléments de* M *et le groupe abélien* $\mathrm{Der}(G/M, N)$.

2.3.2 Groupes d'automorphismes de p-groupes abéliens : deux questions de Y. Berkovich

Comme une première illustration de l'utilité de la relation de Laue, on va l'appliquer aux problèmes de Berkovich suivants :

Problème 75 [11]. Étant donné un p-groupe abélien G, étudier le groupe $A = \langle \alpha \in \mathrm{Aut}(G) \,|\, \alpha_{G/\Phi(G)} = id_{G/\Phi(G)} \rangle$.

Problème 81 [11]. Étant donné un p-groupe abélien G d'exposant $p^e > p$, étudier la structure du groupe de stabilisateur de la suite $G > G^p > \cdots > G^{p^e}$.

Problème 101 [11]. Soit G p-groupe abélien. Étudier la structure du groupe $\langle \alpha \in \mathrm{Aut}(G) \,|\, \alpha_{\Omega_1(G)} = id_{\Omega_1(G)} \rangle$.

On note que le Problème 101 est identique au Problème 756 [12]. Pour un p-groupe abélien G, la suite p-centrale descendante coïncide avec la suite $(G^{p^i})_i$; et en particulier $\Phi(G) = G^p$. D'après la Proposition 1.1.12, un automorphisme de G centralise $G/\Phi(G)$ si, et seulement, il centralise la suite $G \geq G^p \geq G^{p^2} \geq \ldots$. Ceci montre que les Problèmes 75 et 81 sont équivalents.

Soient $\mathrm{A}(G) = \{\alpha \in \mathrm{Aut}(G) \,|\, \alpha_{G/\Phi(G)} = id_{G/\Phi(G)}\}$ et $\mathrm{B}(G) = \{\alpha \in \mathrm{Aut}(G) \,|\, \alpha_{\Omega_1(G)} = id_{\Omega_1(G)}\}$. En vertu de Corollaire 2.3.2, on a $\mathrm{A}(G)$ est isomorphe au groupe adjoint de l'anneau $\mathrm{Der}(G/M, N)$, où $N = G^p$ et $M = 1$; en d'autres termes $\mathrm{A}(G)$ est isomorphe au groupe adjoint de l'anneau $\mathrm{Hom}(G, G^p)$. Aussi $\mathrm{B}(G)$ est isomorphe au groupe adjoint de $\mathrm{Der}(G/M, N)$, où $N = G$ et $M = \Omega_1(G)$, et donc au groupe adjoint de l'anneau $\mathrm{Hom}(G/\Omega_1(G), G)$. On est ainsi ramené à l'étude des anneaux $\mathrm{Hom}(G, G^p)$ et $\mathrm{Hom}(G/\Omega_1(G), G)$.

Lemme 2.3.4. *Soit G un p-groupe abélien (fini ou infini) et supposons que p est impair. Alors*

1. *L'anneau $\mathrm{Hom}(G, G^p)$ est $(1, p, 0)$-nul.*
2. *L'anneau $\mathrm{Hom}(G/\Omega_1(G), G)$ est $(0, p, 1)$-nul.*

Démonstration.
1. Soient $h, k \in \mathrm{Hom}(G, G^p)$ tels que $ph = 0$. Donc $\Im(h)$ est élémentaire abélien, ce qui implique que $G^p \leq \ker h$. Donc $h(k(x)) = 0$, pour tout $x \in G$; d'où $kh = 0$.
2. Soient $h, k \in \mathrm{Hom}(G/\Omega_1(G), G)$ tels que $ph = 0$. Donc $\Im(h) \leq \Omega_1(G)$, ce qui implique que $k(h(x)) = 0$, pour tout $x \in G$; et ainsi $hk = 0$.

□

Pour $p = 2$, le résultat précédent reste vrai si on remplace G^p et $\Omega_1(G)$ par G^4 et $\Omega_2(G)$ respectivement.

Si on a trois groupes abéliens M, N et L, alors il est bien connu que

$$\mathrm{Hom}(M \times L, N) \cong \mathrm{Hom}(M, N) \times \mathrm{Hom}(L, N)$$

$$\mathrm{Hom}(M, N \times L) \cong \mathrm{Hom}(M, N) \times \mathrm{Hom}(M, L)$$

$$\mathrm{Hom}(C_n, C_m) \cong C_{(n,m)}$$

où C_n désigne le groupe cyclique d'ordre n.

Il en résulte immédiatement de ces relations que

Lemme 2.3.5. *Soient G_1 et G_2 deux p-groupes abéliens. Alors le rang et l'exposant du groupe $\mathrm{Hom}(G_1, G_2)$ sont égaux respectivement à $\mathrm{d}(G_1)\,\mathrm{d}(G_2)$ et à $\min\{\exp(G_1), \exp(G_2)\}$.*

On a $G/\Omega_1(G) \cong G^p$; d'où le groupe abélien $\mathrm{Hom}(G/\Omega_1(G), G)$ est isomorphe à $\mathrm{Hom}(G^p, G)$. Ainsi les deux anneaux $\mathrm{Hom}(G, G^p)$ et $\mathrm{Hom}(G/\Omega_1(G), G)$ ont le même groupe additif (à isomorphisme près). On peut maintenant appliquer le Corollaire 2.1.8, Théorème 2.1.10 et le Corollaire 2.1.12 pour résoudre les problèmes de cette sous-section. Notons qu'on peut obtenir un résultat mieux que celui du Corollaire 2.1.12, en remarquant que le groupe adjoint de $\mathrm{Hom}(G/\Omega_1(G), \Omega_1(G^p))$ est de rang $\mathrm{d}(G)\,\mathrm{d}(G^p)$.

Proposition 2.3.6. *Soit G un p-groupe abélien, où p est impair, et soit X l'un des groupes $\mathrm{A}(G)$ ou $\mathrm{B}(G)$. Alors*

(i) *X est nilpotent de classe au plus égale à m, où $p^m = \exp(G^p)$;*

(ii) *soient $\sigma \in X$ et n un entier positif. Pour que $\sigma \in \Omega_{\{n\}}(X)$ il faut et il suffit que $x^{-1}\sigma(x) \in \Omega_n(G)$. En particulier, $\Omega_{\{n\}}(X)$ est un sous-groupe de X ;*

(iii) *le rang de X est égal à $\mathrm{d}(G)\,\mathrm{d}(G^p)$;*

(iv) $\exp(X) = \exp(G^p)$.

Il semble que le matériel développé dans ce chapitre peut donner des résultats plus fins que ceux dans la proposition précédente et surtout qu'il peut s'appliquer aux automorphismes des p-groupes abéliens infinis.

2.3.3 Rang et exposant des p-groupes d'automorphismes de p-groupes

Soit G un p-groupe abélien. Tout automorphisme σ de G induit d'une façon naturelle un automorphisme $\bar{\sigma}$ du quotient G/G^p. Ceci définit un homomorphisme $\sigma \mapsto \bar{\sigma}$ de $\mathrm{Aut}(G)$ dans $\mathrm{Aut}(G/G^p)$. Si G est de rang d, alors $\mathrm{Aut}(G/G^p)$ n'est autre que $\mathrm{GL}(d,p)$. Donc nous avons un homomorphisme de $\mathrm{Aut}(G)$ dans $\mathrm{GL}(d,p)$, dont le noyau est égal à $\mathrm{A}(G) = \mathrm{Aut}_{G^p}(G)$.

Soit H un p-sous-groupe de $\mathrm{Aut}(G)$. Alors

$$\mathrm{d}(H) \leq \mathrm{d}(H \cap \mathrm{A}(G)) + \mathrm{d}(H/(H \cap \mathrm{A}(G))).$$

En vertu de la Proposition 2.3.6, on a pour p impair :

$$\mathrm{d}(H \cap \mathrm{A}(G)) \leq \mathrm{d}(G)\,\mathrm{d}(G^p) \leq d^2;$$

d'autre part, $H/(H \cap \mathrm{A}(G))$ est isomorphe à un p-sous-groupe de $\mathrm{GL}(d,p)$.

Lemme 2.3.7 (Patterson [64])**.** *Supposons que p est impair. Alors tout p-sous-groupe de $\mathrm{GL}(d,p)$ peut être engendré par $\frac{1}{4}d^2$ éléments.*

(C'est important d'avoir une bonne estimation sur le p-rang de $\mathrm{GL}(d,p)$ lorsque $p = 2$.)

Il en résulte que $\mathrm{d}(H) \leq d^2 + \frac{d^2}{4} = \frac{5d^2}{4}$, pour $p \geq 3$. On a établi alors

Proposition 2.3.8. *Soit G un p-groupe abélien de rang d, avec p impair. Alors tout p-sous-groupe de $\mathrm{Aut}(G)$ peut être engendré par $\frac{5}{4}d^2$ éléments. En d'autres termes, le rang d'un p-Sylow de $\mathrm{Aut}(G)$ est au plus $\frac{5}{4}d^2$*

Supposons maintenant que $p = 2$. Si on considère G^4 au lieu de G^2, on obtient un homomorphisme de $\mathrm{Aut}(G)$ dans $\mathrm{GL}(d,\mathbb{Z}_4)$, dont le noyau est égal à $\mathrm{Aut}_{G^4}(G)$. Ce dernier est isomorphe au groupe adjoint de l'anneau $\mathrm{Hom}(G,G^4)$; et comme nous avons mentionné, cet anneau est $(1,p,0)$-nul. Ainsi, si H est un 2-sous-groupe de $\mathrm{Aut}(G)$, alors

$$\mathrm{d}(H \cap \mathrm{Aut}_{G^4}(G)) \leq \mathrm{d}(G)\,\mathrm{d}(G^4) \leq d^2.$$

D'autre part, $H/(H \cap \mathrm{Aut}_{G^4}(G))$ peut être plongé dans $\mathrm{GL}(d,\mathbb{Z}_4)$.

Lemme 2.3.9. *L'ordre d'un* 2*-Sylow de* $\mathrm{GL}(d,\mathbb{Z}_4)$ *est au plus égal à* $2^{\frac{1}{2}(3d^2-d)}$. *En particulier, tout* 2*-sous-groupe de* $\mathrm{GL}(d,\mathbb{Z}_4)$ *peut être engendré par* $\frac{1}{2}(3d^2-d)$ *éléments.*

Démonstration. Soit $A=\mathbb{Z}_4^d$. Donc $\mathrm{Aut}(A)=\mathrm{GL}(d,\mathbb{Z}_4)$. On a $\mathrm{Aut}(A)/\mathrm{Aut}_{A^2}(A)$ est un sous-groupe de $\mathrm{GL}(d,2)$; donc l'ordre de l'un de ses 2-Sylow est au plus $2^{\frac{d^2-d}{2}}$. D'autre part, $\mathrm{Aut}_{A^2}(A)$ est isomorphe au groupe adjoint de $\mathrm{Hom}(A,A^2)$, qui est d'ordre 2^{d^2}. D'où le résultat. □

Il en résulte que $\mathrm{d}(H)\leq d^2+\frac{3d^2-d}{2}=\frac{5d^2-d}{2}$. On a alors établi

Proposition 2.3.10. *Soit* G *un* 2*-groupe abélien de rang* d. *Alors tout* 2*-sous-groupe de* $\mathrm{Aut}(G)$ *peut être engendré par* $\frac{1}{2}(5d^2-d)$ *éléments.*

Les deux propositions précédentes sont déjà connues dans la littérature. Il semble que Kargapolov est le premier qui les a obtenues (voir [53]). Une autre démonstration a été établie par R. Baer and H. Heineken dans [9]. La preuve présentée ici est due à l'auteur et B. Daoud (voir [39]).

D. Segal et A. Shalev ([73]) ont démontré qu'il y a un analogue de ces résultats pour les autres p-groupes. Dans [39], on a utilisé une variante de l'argument de Segal et Shalev pour améliorer leur résultat. Le résultat présenté ci-dessous est nouveau ; il donne une très bonne estimation sur le p-rang de $\mathrm{Aut}(G)$ en terme du rang du p-groupe G, pour $p\geq 3$.

Théorème 2.3.11. *Soit* G *un* p*-groupe de rang* k, *avec* $p\geq 3$. *Alors tout* p*-sous-groupe de* $\mathrm{Aut}(G)$ *peut être engendré par* $\frac{5}{4}k^2$ *éléments.*

On commence par une variante d'un résultat de J. Alperin.

Lemme 2.3.12. *Soient* Γ *un* p*-groupe et* $G\lhd\Gamma$. *Supposons que* A *est un sous-groupe de* G *qui est abélien,* Γ*-invariant, d'exposant* $p^n>2$, *et maximal pour ces propriétés. Alors* $\Omega_n(\mathrm{C}_G(A))\leq A$.

Démonstration. Voir [11, Corollary 10.2]. □

Lemme 2.3.13. *Soient* G *un* p*-groupe, avec* $p\geq 3$. *Alors il existe un sous-groupe normal* H *de* G, *d'exposant* p *et de classe au plus* 2 *tel que* $p^{\mathrm{d}(G)}\leq|H|$.

Démonstration. Voir [56, Corollary 1]. □

Soit $C\leq\mathrm{Aut}(G)$. Suivant [38], on définit $\gamma_n(G,C)$ comme le sous-groupe de G engendré par tous les commutateurs $[x_1,x_2,..,x_k]$, $k\geq n$; où les x_i appartiennent à $G\cup C$ de telle façon que $x_1\in G$ et au moins $n-1$ d'eux sont dans C. On dit que C agit p-centralement sur $\gamma_n(G,C)$ si C fixe tout élément d'ordre divisant p ou 4 dans $\gamma_n(G,C)$.

Lemme 2.3.14. *Soient* G *un* p*-groupe et* $C\leq\mathrm{Aut}(G)$, *tels que* C *agisse* p*-centralement sur* $\gamma_n(G,C)$, *pour un certain* $n\leq p$. *Alors un élément* $\sigma\in C$ *satisfait* $\sigma^p=1$ *si et seulement si* $x^{-1}\sigma(x)\in\Omega_1([G,C])$, *pour tout* $x\in G$.

Démonstration. Voir [38, Proposition 2.9]. □

Démonstration de Théorème 2.3.11. Soient P un p-sous-groupe de $\mathrm{Aut}(G)$, et A un sous-groupe élémentaire abélien normal et P-invariant de G qui est maximal pour ces propriétés. Soit $C = \mathrm{C}_P(A)$. Il en résulte aisément du lemme de trois sous-groupes, appliqué dans le produit semi-direct GP, que $[G, C, A] = 1$, et donc $[G, C] \leq \mathrm{C}_G(A)$. D'après Lemme 2.3.12, $\Omega_1(\mathrm{C}_G(A)) \leq A$, et donc $\Omega_1([G, C]) \leq A$; ce qui montre que C agit p-centralement sur $\gamma_2(G, C)$. Il en résulte de Lemme 2.3.14, que $x^{-1}\sigma(x) \in \Omega_1([G, C]) \leq A$, pour tout $\sigma \in \Omega_1(C)$ et $x \in G$. D'où $\Omega_1(C)$ centralise G/A et A. D'après Proposition 2.3.3, $\Omega_1(C)$ est isomorphe à un sous-groupe de $\mathrm{Der}(G/A, A)$. Or toute dérivation dans $\mathrm{Der}(G/A, A)$ est totalement déterminée par ses valeurs sur un système générateur de G/A, il en résulte que $\mathrm{Der}(G/A, A)$ est isomorphe à un sous-groupe de A^d, où $d = \mathrm{d}(G)$. Ceci implique en particulier que $\mathrm{d}(\Omega_1(C)) \leq kd \leq k^2$. Aussi, d'après Lemme 2.3.13, $\mathrm{d}(C)) \leq \mathrm{d}(\Omega_1(C))$, car $\Omega_1(C)$ est élémentaire abélien ; et ainsi $\mathrm{d}(C) \leq k^2$. D'autre part, P/C opère fidèlement sur A ; donc P/C est isomorphe à un sous-groupe de $\mathrm{GL}(k, p)$. Le résultat découle maintenant de Lemme 2.3.7. □

Proposition 2.3.15. *Soit G un p-groupe non-trivial de classe c, et soit $t = \min\{r, s\}$, où $p^r = \exp(G/G')$ et $p^s = \exp(\mathrm{Z}(G))$. Alors l'exposant de $\mathrm{Aut}_{\Phi(G)}(G)$ est au plus égal à p^{tc-1}.*

Démonstration. Soit n la longueur p-centrale de G. Par Proposition 1.1.12, $\mathrm{Aut}_{\Phi(G)}(G)$ centralise la suite p-centrale descendante de G ; et donc en vertu de Proposition 1.1.10, l'exposant de $\mathrm{Aut}_{\Phi(G)}(G)$ divise p^{n-1}. Maintenant on va lier les suites centrales ascendante et descendante de G à sa suite p-centrale descendante. Si A est un p-groupe abélien d'exposant p^m, on définit sa p-suite par

$$1 < A^{p^{m-1}} < ... < A^p < A.$$

Cette suite est de longueur m, et ses facteurs sont d'exposant p. Avec cette notion, on peut raffiner chaque facteur de la suite centrale ascendante ou descendante de G, par sa p-suite. On obtient deux suites centrales de G dont les facteurs sont d'exposant p, et leurs longueurs sont respectivement $s_1(G) = \sum_{i=1}^{c} e(Z_i/Z_{i-1})$ et $r_1(G) = \sum_{i=1}^{c} e(\gamma_i/\gamma_{i+1})$; avec la notation $p^{e(H)} = \exp H$. D'après Proposition 1.1.11, $n \leq min\{r_1, s_1\}$, et donc l'exposant de $\mathrm{Aut}_{\Phi(G)}(G)$ est au plus égal à $p^{\min\{r_1,s_1\}-1}$.
Finalement, d'après Proposition 1.1.8 et Corollaire 1.1.5, on a $exp(Z_i/Z_{i-1}) \leq exp(Z(G))$ et $exp(\gamma_i/\gamma_{i+1}) \leq exp(G/\gamma_2)$; il en résulte que $r_1(G) \leq rc$ et $s_1(G) \leq sc$. D'où le résultat. □

Corollaire 2.3.16. *Sous les notations précédentes et si G peut être engendré par d éléments, alors l'exposant d'un p-sous-groupe de $\mathrm{Aut}(G)$ ne dépasse pas p^{tc+d-2}.*

Démonstration. Notons seulement que si P est un p-sous-groupe de $\mathrm{Aut}(G)$, alors $P\,\mathrm{Aut}_{\Phi(G)}(G)/\,\mathrm{Aut}_{\Phi(G)}(G)$ se plonge dans $\mathrm{GL}(d,p)$; et l'exposant d'un p-Sylow de $\mathrm{GL}(d,p)$ ne dépasse pas p^{d-1}. □

Ces deux derniers résultats sont mieux que [39, Théorème C] ; de plus leur preuve ne provient pas des anneaux.

2.3.4 Groupes d'automorphismes centraux

Soit G un groupe arbitraire. Rappelons qu'un endomorphisme θ de G est dit *central* s'il appartient à $\mathrm{End}_{\mathrm{Z}(G)}(G)$, ce qui revient à dire que $x^{-1}\theta(x) \in \mathrm{Z}(G)$, pour tout $x \in G$. On note $\mathrm{Aut}_z(G)$ le groupe des automorphismes centraux de G (certains auteurs le note $\mathrm{Aut}_c(G)$). L'isomorphisme de Laue dans ce cas applique $\mathrm{End}_{\mathrm{Z}(G)}(G)$ dans $\mathrm{Hom}(G, \mathrm{Z}(G))$; il est aussi connu sous le nom *"application de Adney-Yen"*.

On dit que G est *purement non-abélien* s'il ne possède aucun facteur direct abélien (non trivial).

Lemme 2.3.17. *Soit G un groupe. Alors G est purement non-abélien si, et seulement si, l'anneau $\mathrm{Hom}(G, \mathrm{Z}(G))$ ne contient aucun idempotent non nul.*

Démonstration. Si G possède un facteur direct abélien (non trivial) A, alors $A \leq \mathrm{Z}(G)$; ainsi la projection sur A est un idempotent non nul de $\mathrm{Hom}(G, \mathrm{Z}(G))$. Inversement, si $e : G \longrightarrow \mathrm{Z}(G)$, est un idempotent non nul ; alors $\Im(e)$ est un facteur direct non-trivial de G. □

Supposons que G satisfait les conditions minimale et maximale. Alors G/G' et $\mathrm{Z}(G)$ sont finis, et donc l'anneau $\mathrm{Hom}(G, \mathrm{Z}(G))$ est fini, car son ordre est égal à celui de $\mathrm{Hom}(G/G', \mathrm{Z}(G))$. Dans ce cas, l'ensemble $\{h^n \mid n \in \mathbb{N}^*\}$ contient un idempotent, pour tout $h \in \mathrm{Hom}(G, \mathrm{Z}(G))$ (ceci étant un exercice élémentaire en théorie des semi-groupes). Donc si G est purement non-abélien, alors tout élément de $\mathrm{Hom}(G, \mathrm{Z}(G))$ est nilpotent, et en particulier cet anneau est radical. Inversement, il est simple de voir que dans un anneau radical, tout idempotent est nul. On a donc établi

Proposition 2.3.18 (Adney-Yen)**.** *Soit G un groupe qui satisfait la condition maximale et minimale. Alors l'anneau $\mathrm{Hom}(G, \mathrm{Z}(G))$ est radical si et seulement si G est purement non-abélien.*

La version originale de Adney et Yen stipule que (pour G fini) l'application $\sigma \mapsto \delta_\sigma$ définie de $\mathrm{Aut}_z(G)$ dans $\mathrm{Hom}(G, \mathrm{Z}(G))$ est une bijection si et seulement si G est purement non-abélien (voir par exemple [50, Theorem 2.1]).

Le radical de Jacobson d'un anneau artinien est nilpotent ; ce résultat classique implique que tout anneau radical artinien est nilpotent. D'où

Corollaire 2.3.19. *Soit G un groupe qui satisfait les conditions maximale et minimale. Alors l'anneau* $\mathrm{Hom}(G, \mathrm{Z}(G))$ *est nilpotent si et seulement si G est purement non-abélien.*

Il en résulte de la Proposition 2.1.3 que

Corollaire 2.3.20. *Soit G un groupe qui satisfait les conditions maximale et minimale. Si G est purement non-abélien, alors son groupe d'automorphismes centraux est nilpotent.*

Pour une autre démonstration, lorsque G est fini, le lecteur est référé à [50, Proposition 4.1]. Il semble que ce résultat a été établi beaucoup plus tôt.

Supposons maintenant que G est un p-groupe. Désignons par $S(G)$ le sous-groupe $(G^{2p}G')\cap \mathrm{Z}(G)$. Le même argument pour le Lemme 2.3.4, montre que

Lemme 2.3.21. *Soit G un p-groupe. Alors*

1. *l'anneau* $\mathrm{Hom}(G, S(G))$ *est $(1, p, 0)$-nul ;*
2. *l'anneau* $\mathrm{Hom}(G/\Omega(\mathrm{Z}(G)), \mathrm{Z}(G))$ *est $(0, p, 1)$-nul.*

Le résultat suivant généralise la Proposition 2.3.6 ; sa démonstration est basée sur le matériel développé dans la première section de ce chapitre et elle est similaire à celle de la Proposition 2.3.6.

Proposition 2.3.22. *Soient G un p-groupe, $X = \mathrm{Aut}_{S(G)}(G)$, et $a = \min\{e, f\}$, où $p^e = \exp(G/G')$ et $p^f = \exp(S(G))$. Alors*

(i) *X est nilpotent de classe au plus égale à a ($\lceil a/2\rceil + 1$ pour $p = 2$) ;*

(ii) *soient $\sigma \in X$ et n un entier positif. Pour que $\sigma \in \Omega_{\{n\}}(X)$ il faut et il suffit que $x^{-1}\sigma(x) \in \Omega_n(S(G))$. En particulier, $\Omega_{\{n\}}(X)$ est un sous-groupe de X ;*

(iii) $\exp(X) = p^a$ *;*

(iv) *le rang de X est égal à* $\mathrm{d}(G)\,\mathrm{d}(S(G))$.

Maintenant, soient X le groupe des automorphismes centraux de G fixant tous les éléments de $\Omega(\mathrm{Z}(G))$, et $b = \min\{e, f\}$, où $p^e = \exp(G/(\Omega(\mathrm{Z}(G))G'))$ et $p^f = \exp(\mathrm{Z}(G))$. Alors

(v) *X est nilpotent de classe au plus égale à b ($\lceil b/2\rceil + 1$ pour $p = 2$) ;*

(vi) *soient $\sigma \in X$ et n un entier positif. Pour que $\sigma \in \Omega_{\{n\}}(X)$ il faut et il suffit que $x^{-1}\sigma(x) \in \Omega_n(\mathrm{Z}(G))$. En particulier, $\Omega_{\{n\}}(X)$ est un sous-groupe de X ;*

(vii) $\exp(X) = p^b$ *;*

(viii) *le rang de X est au plus égal à* $\mathrm{d}(G)\,\mathrm{d}(\mathrm{Z}(G))$.

Si le centre d'un groupe G est trivial, alors le centre de $\mathrm{Aut}(G)$ est aussi trivial ; ceci résulte immédiatement du fait que $\mathrm{Hom}(G, \mathrm{Z}(G))$ est trivial. C'est naturel de se demander à quel point le centre de Aut est contrôlé par $\mathrm{Z}(G)$. Considérons cette question pour les p-groupes.

Théorème 2.3.23. *Soient G un p-groupe, $p \geq 3$, et $P = \mathrm{Aut}_{S_1}(G)\,\mathrm{Inn}(G)$, où S_1 est le sous-groupe des éléments d'ordre au plus p dans $S(G)$. Soit p^t le plus petit entre $\exp(G/G')$ et $\exp(\mathrm{Z}(G))$. Alors l'exposant de $\mathrm{C}_{\mathrm{Aut(G)}}(P)$ divise $p^t(p-1)$; et en particulier l'exposant de $\mathrm{Z}(\mathrm{Aut(G)})$ divise $p^t(p-1)$.*

Démonstration. Soit $\sigma \in \mathrm{C}_{\mathrm{Aut(G)}}(P)$. Or σ commute avec tous les automorphismes intérieurs, on a $x^{-1}\sigma(x) \in \mathrm{Z}(G)$, et ainsi $x^{-1}\sigma^{p-1}(x) \in \mathrm{Z}(G)$, pour tout $x \in G$. Soient M un sous-groupe maximal de G, et $r : G \to \mathbb{Z}_p$ un homomorphisme de noyau égal à M. Soit $z \in S_1$, et posons $h(x) = z^{r(x)}$; alors l'application $1+h : x \mapsto xh(x)$ définit un automorphisme de G qui appartient à $Aut_{S_1}(G)$. Il en résulte que σ commute avec h ; donc $\sigma(z)^{r(x)} = z^{r(\sigma(x))}$. Si $x \in M$, alors $z^{r(\sigma(x))} = \sigma(z)^{r(x)} = 1$; donc $\sigma(x) \in M$. Ceci montre que M est σ-invariant, et donc σ induit un automorphisme sur le quotient G/M. Le groupe d'automorphismes de G/M est d'ordre $p-1$, ce qui implique que σ^{p-1} induit l'identité sur G/M, ce qui revient à dire que $x^{-1}\sigma^{p-1}(x) \in M$, pour tout $x \in G$. Ceci étant vrai pour tout sous-groupe maximal M, et donc $x^{-1}\sigma^{p-1}(x) \in \Phi(G)$, pour tout $x \in G$. Il en résulte que σ^{p-1} appartient à $Aut_{S(G)}(G)$; donc d'après la proposition précédente $\sigma^{p^t(p-1)} = 1$. □

En général, le terme $p-1$ ne peut pas être omis de la borne précédente ; pour cela il suffit de considérer le groupe d'automorphismes d'un p-groupe cyclique. Notons aussi que d'autres informations sur $\mathrm{C}_{\mathrm{Aut}}(P)$ (comme son ordre et son rang) peuvent être déduites de la Proposition 2.3.22, mais elles dépendent apparemment d'autres invariants en dehors de $\mathrm{Z}(G)$.

On termine ce chapitre par une caractérisation des p-groupes (p impair), dont tous les automorphismes centraux d'ordre p sont intérieurs.

Théorème 2.3.24. *Soit G un p-groupe, avec $p \geq 3$. Alors G possède un automorphisme central non-intérieur d'ordre p si, et seulement si,* $\mathrm{d}(\frac{Z_2(G)}{\mathrm{Z}(G)}) \neq \mathrm{d}(G)\,\mathrm{d}(\mathrm{Z}(G))$.

Démonstration. Une implication est bien connue dans la littérature (voir par exemple [2, Corollary 2.3]), et aussi sa vérification est simple. On va prouver l'autre implication, et donc supposons que $\mathrm{d}(\frac{Z_2(G)}{\mathrm{Z}(G)}) = \mathrm{d}(G)\,\mathrm{d}(\mathrm{Z}(G))$. Soit I le groupe additif de l'anneau $\mathrm{Hom}(G, \mathrm{Z}(G))$; on a alors $\mathrm{d}(I) = \mathrm{d}(G)\,\mathrm{d}(\mathrm{Z}(G))$, et donc notre hypothèse implique que l'image de $\Omega_1(\mathrm{Z}(\mathrm{Inn}(G)))$ par l'isomorphisme de Laue (ou de Adney-Yen) coïncide avec I. Si $\mathrm{Z}(G) \not\leq \Phi(G)$, alors il existe un élément $g \in \mathrm{Z}(G)$, tel que $g \notin M$, pour certain sous-groupe maximal M. Soient z un élément d'ordre p dans $S(G)$, et $r : G \to \mathbb{Z}_p$ un homomorphisme de noyau égal à M, et posons $h(x) = z^{r(x)}$, pour tout

$x \in G$. On a $h \in I$, et donc $1 + h$ est un automorphisme intérieur de G ; mais $1 + h(g) = gz^i$, pour certain $0 < i < p$; une contradiction. On a donc $\mathrm{Z}(G) \leq \Phi(G)$, et ainsi $\mathrm{Z}(G) = S(G)$. En vertu de Proposition 2.3.22 (ii), si σ est un automorphisme central d'ordre p, alors $\delta_\sigma \in I$; ceci implique que σ et intérieur. □

Chapitre 3

Groupes d'automorphismes et cohomologie

3.1 Automorphismes et premier groupe de cohomologie

Soient G un groupe, et A un G-module (à droite), ce qui revient à donner un homomorphisme de G dans le groupe d'automorphismes du groupe abélien A. Soient $g \in G$ et $a \in A$. Si A est noté additivement, on note ag l'image de a par l'automorphisme induit par g ; et si A est noté multiplicativement, on la note a^g.

Dire que A est un G-module (à droite) revient aussi à dire que A a une structure de $\mathbb{Z}[G]$-module à droite, où $\mathbb{Z}[G]$ désigne l'algèbre de G sur $\mathbb{Z}$. En effet, un homomorphisme de G dans $\mathrm{Aut}(A)$ se prolonge uniquement en un homomorphisme d'anneaux de $\mathbb{Z}[G]$ dans $\mathrm{End}(A)$, donc A est un $\mathbb{Z}[G]$-module. Réciproquement, un homomorphisme d'anneaux de $\mathbb{Z}[G]$ dans $\mathrm{End}(A)$, induit un homomorphisme du groupe des unités de $\mathbb{Z}[G]$ dans $\mathrm{Aut}(A)$, et comme tout élément de G est inversible dans $\mathbb{Z}[G]$, on obtient en particulier un homomorphisme de G dans $\mathrm{Aut}(A)$.

On note $H_n(G, A)$, $n \in \mathbb{N}$, les groupes d'homologie de G à coefficients dans A ; et les groupes de cohomologie sont notés $H^n(G, A)$, $n \in \mathbb{N}$. Pour la définition et les suites exactes formées par ces groupes, le lecteur peut se référer par exemple à [46, 16, 70].

Usuellement, les éléments de $H^1(G, A)$ sont interprétés comme les classes de conjugaison des compléments de A dans $A \rtimes G$. Mais, sous la lumière de §2.3, $H^1(G, A)$ peut prendre un autre sens utile. La connexion avec l'étude des automorphismes des groupes vient du fait que

$$H^1(G, A) \cong \mathrm{Der}(G, A)/\mathrm{Ider}(G, A),$$

où $\mathrm{Der}(G, A)$ est le groupe des dérivations (homomorphismes croisés) de G dans A, comme défini dans §2.3 ; rappelons une autre fois qu'une telle

dérivation est une application $\delta : G \to A$ qui vérifie

$$\delta(xy) = \delta(x)^y \delta(y), \quad \text{pour tout } x, y \in G.$$

Le groupe $\mathrm{Ider}(G, A)$ désigne les dérivations intérieures (induites par des éléments de A) de G dans A ; c'est à dire les dérivations de la forme $\delta_a(x) = a^{-1}a^x$, pour un certain $a \in A$.

Supposons que A est un sous-groupe normal du groupe G. Donc A a une structure naturelle de G-module. Soit $C = \mathrm{C}_G(A)$; ainsi A peut être vu comme un G/C-module, et comme C satisfait les conditions du corollaire 2.3.3, l'isomorphisme de Laue induit un isomorphisme :

$$\phi : \mathrm{Der}(G/C, A) \longrightarrow \mathrm{Aut}_A^C(G);$$

où par $\mathrm{Aut}_A^C(G)$ on entend le groupes des automorphismes dans $\mathrm{Aut}_A(G)$, qui fixent tous les éléments de C.

Cet isomorphisme applique $\mathrm{Ider}(G/C, A)$ sur des automorphismes intérieurs dans $\mathrm{Der}(G/C, A)$; plus précisément, si δ_a est la dérivation intérieure induite par $a \in A$, alors

$$\phi(\delta_a)(x) = x\delta_a(x) = xa^x a^{-1} = x^{a^{-1}};$$

donc $\phi(\delta_a)$ est l'automorphisme intérieur induit par a^{-1}.

Pour qu'un automorphisme intérieur τ_g de G appartienne à $\mathrm{Aut}_A^C(G)$, il faut et il suffit que $[g, G] \subseteq A$ et $[g, C] = 1$; ceci revient à dire que $gA \in \mathrm{Z}(G/A) = \overline{A}/A$ et $g \in \mathrm{C}_G(C)$. Aussi, τ_g est induit par une dérivation intérieure si, et seulement si, $x^g = x^{a^{-1}}$, pour tout $x \in G$; et ceci revient à dire que $g \in A\,\mathrm{Z}(G)$. On a établi alors :

Proposition 3.1.1. *Sous les notations précédentes ; pour que ϕ applique $\mathrm{Ider}(G/C, A)$ exactement sur les automorphismes intérieurs dans $\mathrm{Aut}_A^C(G)$, il faut et il suffit que $\overline{A} \cap \mathrm{C}_G(\mathrm{C}_G(A)) \leq A\,\mathrm{Z}(G)$.*

Corollaire 3.1.2. *Supposons que A est un sous-groupe abélien normal d'un groupe G, qui vérifie $\overline{A} \cap \mathrm{C}_G(\mathrm{C}_G(A)) \leq A\,\mathrm{Z}(G)$. Alors $\mathrm{Aut}_A^C(G)$ contient des automorphismes non-intérieurs si, et seulement si, $H^1(G/C, A) \neq 0$.*

Évidement, la condition ci-dessus est vérifiée si $\mathrm{C}_G(\mathrm{C}_G(A)) \leq A$. Pour ceci, on peut prendre par exemple A maximal entre les sous-groupes abéliens normaux de G, puisque dans ce cas $\mathrm{C}_G(A) = A$. Un autre exemple important est le cas $A = \mathrm{Z}(\Phi(G))$, avec G satisfaisant la condition de Deaconescu-Silberberg.

Plus ou moins, le corollaire précédent est bien-connu (voir par exemple [37] ou [48]) ; usuellement, il est formulé avec la condition $A = \mathrm{Z}(N)$, où $N \lhd G$ et $\mathrm{C}_G(N) = \mathrm{Z}(N)$. Notre condition $\overline{A} \cap \mathrm{C}_G(\mathrm{C}_G(A)) \leq A\,\mathrm{Z}(G)$, semble plus faible, mais on ne sait pas encore produire des exemples intéressants.

3.2 Cohomologie de Tate et Théorème de Gaschütz-Uchida

Dans cette section, on suppose que G est fini. Dans ce cas, on peut définir *la trace* $\tau = \tau_A : A \longrightarrow A$, par

$$\tau(a) = \prod_{x \in G} a^x.$$

Notons A_G le sous-module des éléments de A fixés par G, et $[A, G]$ le sous-module de A des éléments de la forme $a^{-1}a^g$, $a \in A$ et $g \in G$. Il est bien connu que $H^0(G, A) = A_G$, et $H_0(G, A) = A/[A, G]$. On peut voir facilement que A^τ l'image de τ est incluse dans A_G, et que $[A, G] \leq \ker \tau$. Ainsi $\tau = \tau_A$ induit un homomorphisme

$$\tau_A^* : H_0(G, A) \longrightarrow H^0(G, A),$$

avec $\tau_A^*(\bar{x}) = \tau_A(x)$, pour tout $\bar{x} \in A/[A, G]$.

Posons $\hat{H}^0(G, A) = \operatorname{coker} \tau_A^*$, et $\hat{H}^{-1}(G, A) = \ker \tau_A^*$. Autrement dit,

$$\hat{H}^0(G, A) = A_G/A^\tau, \text{ et } \hat{H}^{-1}(G, A) = \ker \tau/[A, G].$$

Posons aussi

$$\hat{H}^n(G, A) = H^n(G, A), \text{ pour } n \geq 1;$$

et

$$\hat{H}^n(G, A) = H_{-n-1}(G, A), \text{ pour } n \leq -2.$$

On appelle ces groupes $\hat{H}^n(G, A)$, les groupes de *cohomologie de Tate* de G a coefficients dans A.

Proposition 3.2.1. *Toute suite exacte de G-modules $0 \to A \to B \to C \to 0$, induit une suite exacte de cohomologie*

$$\cdots \to \hat{H}^n(G, B) \to \hat{H}^n(G, C) \xrightarrow{\delta} \hat{H}^{n+1}(G, A) \to \hat{H}^{n+1}(G, B) \to \ldots$$

De plus, cette construction est naturelle dans le sens que tout homomorphisme de suites exactes courtes de G-modules, induit un homomorphisme de suites exactes de cohomologie.

(Il revient au même de dire que la suite $\{\hat{H}^n(G, -)\}_{n \in \mathbb{Z}}$ définit un foncteur cohomologique au sens de Grothendieck).

Démonstration. Pour $n \geq 1$ et $n \leq -2$, cette suite correspond aux suites exactes longues d'homologie et de cohomologie usuelles. Donc il suffit de

l'établir pour $n = -1, 0$. Ce n'est pas difficile de voir que le diagramme suivant est commutatif :

$$\begin{array}{ccccccccc} H_1(G,C) & \to & H_0(G,A) & \to & H_0(G,B) & \to & H_0(G,C) & \to & 0 \\ \downarrow & & \tau_A^* \downarrow & & \tau_B^* \downarrow & & \tau_C^* \downarrow & & \downarrow \\ 0 & \to & H^0(G,A) & \to & H^0(G,B) & \to & H^0(G,C) & \to & H^1(G,A) \end{array}$$

Sachant que $\hat{H}^{-1}(G,A) = \ker \tau_A^*$, et $\hat{H}^0(G,A) = \operatorname{coker} \tau_A^*$, le *Lemme du serpent* (voir par exemple [46, Lemma III.5.1]) implique qu'il existe un homomorphisme (connectant) naturel

$$\hat{H}^{-1}(G,C) \xrightarrow{\delta} \hat{H}^0(G,A)$$

tel que la suite

$$\cdots \to \hat{H}^{-2}(G,C) \to \hat{H}^{-1}(G,A) \to \hat{H}^{-1}(G,B) \to \hat{H}^{-1}(G,C) \xrightarrow{\delta} \hat{H}^0(G,A)$$
$$\to \hat{H}^0(G,B) \to \hat{H}^0(G,C) \to \hat{H}^1(G,A) \to \dots$$

est exacte.

□

Pour un groupe abélien X, on peut munir $X \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ d'une structure de G-module (à droite), en posant $(x \otimes a)^g = x \otimes ag$, pour $a \in \mathbb{Z}[G]$, $x \in X$, et $g \in G$. Un G-module qui est isomorphe à $X \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ (pour un certain groupe abélien X) est dit *induit*. Dualement, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$ peut être vu comme un G-module, et tout module de cette forme est dit *co-induit*.

Rappelons que pour calculer l'homologie d'un groupe quelconque G à coefficients dans un G-module A, on choisit n'importe quelle résolution projective de $\mathbb{Z}$ (vue comme G-module à gauche trivial) :

$$\cdots \to P_n \to \cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0,$$

et on considère le complexe de chaines

$$\mathcal{C} : \cdots \to A \otimes_G P_n \to \cdots \to A \otimes_G P_1 \to A \otimes_G P_0 \to 0.$$

Le n-ème groupe d'homologie $H_n(G,A)$ n'est que le groupe d'homologie $H_n(\mathcal{C})$ (le type d'isomorphisme de $H_n(\mathcal{C})$ ne dépend pas de la résolution choisie).

Supposons alors que $A \cong X \otimes_{\mathbb{Z}} \mathbb{Z}[G]$, ou en d'autres termes que A est un G-module induit. Comme

$$(X \otimes_{\mathbb{Z}} \mathbb{Z}[G]) \otimes_G P_i \cong X \otimes_{\mathbb{Z}} (\mathbb{Z}[G] \otimes_G P_i) \cong X \otimes_{\mathbb{Z}} P_i,$$

le complexe $\mathcal{C}$ ci-dessus, devient

$$\mathcal{C} : \cdots \to X \otimes_{\mathbb{Z}} P_n \to \cdots \to X \otimes_{\mathbb{Z}} P_1 \to X \otimes_{\mathbb{Z}} P_0 \to 0.$$

Comme les P_i sont aussi projectifs comme $\mathbb{Z}$-modules, l'homologie du complexe $\mathcal{C}$ coïncide avec l'homologie du groupe trivial à coefficients dans X. Mais $H_n(1, X) = 0$, pour $n \geq 1$ (considérons par exemple la résolution $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$).

Soit $S \leq G$. Alors $\mathbb{Z}[G]$ est libre en tant que S-module, ce qui revient aussi à dire que $\mathbb{Z}[G] \cong \oplus_i \mathbb{Z}[S]$. Comme le produit tensoriel est distributive par rapport à la somme directe, on a

$$A \cong X \otimes_{\mathbb{Z}} (\oplus_i \mathbb{Z}[S]) \cong (\oplus_i X) \otimes_{\mathbb{Z}} \mathbb{Z}[S],$$

donc A est induit en tant que S-module. Il en résulte que

Pour tout G-module induit A, $H_n(S, A) = 0$, pour tous $S \leq G$ et $n \geq 1$.

D'une façon analogue, il résulte que

Pour tout G-module co-induit A, $H^n(S, A) = 0$, pour tous $S \leq G$ et $n \geq 1$.

Rappelons que le G-module A est dit *cohomologiquement trivial* si $\hat{H}^k(S, A) = 0$, pour tout $S \leq G$, et pour tous les entiers k.

Proposition 3.2.2. *Tout G-module induit est cohomologiquement trivial.*

Démonstration. Supposons que $A = X \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ (c-à-d, A est induit). Pour un élément $\alpha \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$, considérons

$$\Phi(\alpha) = \sum_{g \in G} g^{\alpha} \otimes g^{-1}.$$

Cette somme est bien définie puisque G est fini. Donc, on a une application $\alpha \mapsto \Phi(\alpha)$, à valeurs dans A. C'est simple de voir que Φ est un homomorphisme de G-module. Si $\Phi(\alpha) = 0$, alors $g^{\alpha} = 0$, pour tout $g \in G$, mais comme G forme une base de $\mathbb{Z}[G]$, on a $\alpha = 0$. Aussi, tout élément a de A peut s'écrire sous la forme $\sum_{g \in G} x_g \otimes g^{-1}$. L'application qui prend la valeur $x_g \in X$, pour chaque $g \in G$, se prolonge uniquement à un homomorphisme α de $\mathbb{Z}[G]$ dans X, et $\Phi(\alpha) = a$. On a montré que Φ est un isomorphisme de G-module, et donc A est un G-module co-induit. La discussion qui précède la proposition implique que $\hat{H}^k(S, A) = 0$, pour tout $S \leq G$, et pour tout entier $k \neq 0, -1$. Les cas $k = 0, -1$, se traitent plus simplement. □

Pour tout G-module A, nous avons un homomorphisme surjectif de G-module, $A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to A$, qui applique $a \otimes g$ sur a^g. Le noyau de ce morphisme est un G-module qu'on note $A^{(-1)}$. Posons $A^{(0)} = A$, et définissons par récurrence, $A^{(-n-1)} = (A^{(-n)})^{(-1)}$, $n \geq 0$.

On peut aussi définir un homomorphisme de G-module $A \to A \otimes_{\mathbb{Z}} \mathbb{Z}[G]$, qui applique chaque $a \in A$ sur $\sum_{g \in G} a^g \otimes g^{-1}$. Le conoyau de ce morphisme est un G-module qu'on note $A^{(1)}$. On définit par récurrence, $A^{(n+1)} = (A^{(n)})^{(1)}$, $n \geq 0$.

Corollaire 3.2.3. *(Décalage de dimension) Pour tout G-module A, et pour tout $S \leq G$, on a*

$$\hat{H}^{n+k}(S, A) = \hat{H}^n(S, A^{(k)}) = 0,$$

pour tous $n, k \in \mathbb{Z}$.

Démonstration. Par récurrence, il suffit d'établir le résultat pour $k = 1$ et $k = -1$.

Pour $k = -1$, considérons la suite exacte de S-modules

$$0 \to A^{(-1)} \to A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to A \to 0.$$

Par Proposition 3.2.1, on a une suite exacte de cohomologie

$$\cdots \to \hat{H}^{n-1}(S, A \otimes_{\mathbb{Z}} \mathbb{Z}[G]) \to \hat{H}^{n-1}(S, A) \xrightarrow{\delta} \hat{H}^n(S, A^{(-1)}) \to \hat{H}^n(S, A \otimes_{\mathbb{Z}} \mathbb{Z}[G]) \to \dots$$

mais, $A \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ est un G-module induit, ainsi le résultat est immédiat d'après Proposition 3.2.2.

Pour $k = 1$, on procède d'une façon analogue avec la suite

$$0 \to A \to A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to A^{(1)} \to 0.$$

□

Le théorème suivant est obtenu indépendamment par Gaschütz ([29]), et Uchida ([75]). Notons que ceci généralise les résultats de Nakayama sur la trivialité de cohomologie des p-groupes (voir [70, §IX]). Essentiellement, ce théorème est utilisé par Gaschütz pour démontrer son célèbre résultat sur l'existence des p-automorphismes non-intérieurs (voir [30]). À propos, K. Gruenberg ([37]) a dit :

"One of the most ingenious applications of cohomology to a purely group theoretical problem is the recent solution by Gaschütz of the question whether every finite p-group has outer automorphisms of order p."

Théorème 3.2.4. *Soient G un p-groupe, et A un G-module qui est aussi un p-groupe. Si $\hat{H}^n(G, A) = 0$, pour certain entier n, alors A est cohomologiquement trivial.*

La démonstration qu'on va donner suit de près celle de [47]. Montrons d'abord

Lemme 3.2.5. *Pour tout $S \leq G$ d'indice p, on a*

$$\hat{H}^0(G, A) = 0 \Leftrightarrow \hat{H}^0(S, A) = 0 \text{ et } \hat{H}^0(G/S, A_S) = 0.$$

Démonstration. Nous avons une suite évidente de G/S-modules

$$0 \to A^{\tau_S} \to A_S \to \hat{H}^0(S, A) \to 0.$$

Cette suite induit une suite exacte de cohomologie ordinaire :

$$0 \to (A^{\tau_S})_{G/S} \to (A_S)_{G/S} \to \hat{H}^0(S, A)_{G/S} \to H^1(G/S, A^{\tau_S}) \to \dots$$

on a $(A_S)_{G/S} = A_G$, et comme $(A^{\tau_S})_{G/S}$ et A_G contient $A^\tau = (A^{\tau_S})^{\tau_{G/S}}$, on peut les quotienter par A^τ. Il en résulte immédiatement

$$0 \to \hat{H}^0(G/S, A^{\tau_S}) \to \hat{H}^0(G, A) \to \hat{H}^0(S, A)_{G/S} \to \hat{H}^1(G/S, A^{\tau_S}).$$

Maintenant, si $\hat{H}^0(G, A) = 0$, alors $\hat{H}^0(G/S, A^{\tau_S}) = 0$, mais comme G/S est cyclique, on a $\hat{H}^1(G/S, A^{\tau_S}) = 0$ (Herbrand). Il résulte de la suite exacte précédente que $\hat{H}^0(S, A)_{G/S} = 0$. Comme G/S est $\hat{H}^0(S, A)$ sont des p-groupes, l'ensemble des points fixes dans $\hat{H}^0(S, A)$ n'est trivial sauf si $\hat{H}^0(S, A) = 0$. Ceci implique alors que $A^{\tau_S} = A_S$, d'où $0 = \hat{H}^0(G/S, A^{\tau_S}) = \hat{H}^0(G/S, A_S)$.

Inversement, si $\hat{H}^0(S, A) = \hat{H}^0(G/S, A_S) = 0$, alors $A^{\tau_S} = A_S$, et ainsi $\hat{H}^0(G/S, A^{\tau_S}) = 0$. en vertu de la suite exacte ci-dessus, on a $\hat{H}^0(G, A) = 0$. □

Lemme 3.2.6. *Sous les notations du Théorème 3.2.4, on a*

$$\hat{H}^0(G, A) = 0 \Leftrightarrow \hat{H}^1(G, A) = 0.$$

Démonstration. Le lemme est vrai lorsque $|G| = p$, par un résultat classique de Herbrand. Par récurrence sur l'ordre de G, supposons que le résultat est vrai pour tout p-groupe d'ordre $< |G|$. Soit S un sous-groupe de G d'indice p. Si $\hat{H}^0(G, A) = 0$, alors par le lemme précédent, on a $\hat{H}^0(S, A) = \hat{H}^0(G/S, A_S) = 0$. Par récurrence, on a $\hat{H}^1(S, A) = \hat{H}^1(G/S, A_S) = 0$, et en vertu de la suite exacte d'inflation-restriction (voir par exemple [70, §VII.6])

$$0 \to \hat{H}^1(G/S, A_S) \to \hat{H}^1(G, A) \to \hat{H}^1(S, A),$$

on a $\hat{H}^1(G, A) = 0$.

Inversement, si $\hat{H}^1(G, A) = 0$, alors d'après la suite exacte d'inflation-restriction ci-dessus, on a $\hat{H}^1(G/S, A_S) = 0$. Aussi, le décalage de dimension implique $\hat{H}^0(G, A^{(1)}) = 0$, et donc par le lemme précédent on a $\hat{H}^0(S, A^{(1)}) = 0$ (comme $A^{(1)}$ est un p-groupe). Une autre fois, le décalage de dimension entraine $\hat{H}^1(S, A) = 0$. On a établi $\hat{H}^1(S, A) = \hat{H}^1(G/S, A_S) = 0$, donc par récurrence $\hat{H}^0(S, A) = \hat{H}^0(G/S, A_S) = 0$, d'où $\hat{H}^0(G, A) = 0$ par le lemme précédent. □

La démonstration du Théorème 3.2.4, est facile maintenant. Si $\hat{H}^n(G, A) = 0$, pour certain n, alors $\hat{H}^0(G, A^{(n)}) = 0$ et $\hat{H}^1(G, A^{(n-1)}) = 0$, par le décalage de dimension. Comme $A^{(n)}$ est un p-groupe, le Lemme 3.2.6, implique

que $\hat{H}^1(G, A^{(n)}) = 0$ et $\hat{H}^0(G, A^{(n-1)}) = 0$. Revenons en arrière par le procédé de décalage, on obtient $\hat{H}^{n+1}(G, A) = \hat{H}^{n-1}(G, A) = 0$. Il est trivial maintenant de montrer par récurrence sur $k \geq 1$ que

$$\hat{H}^{n+k}(G, A) = \hat{H}^{n-k}(G, A) = 0.$$

Aussi, comme $\hat{H}^0(G, A^{(n)}) = 0$, le Lemme 3.2.5, implique que $\hat{H}^0(S, A^{(n)}) = 0$, pour tout sous-groupe S d'indice p dans G, et par récurrence sur l'indice de S, ceci implique que $\hat{H}^0(S, A^{(n)}) = 0$, pour tout $S \leq G$; d'où $\hat{H}^n(S, A) = 0$. C'est immédiat maintenant que pour tout $k \geq 0$:

$$\hat{H}^{n+k}(S, A) = \hat{H}^{n-k}(S, A) = 0.$$

Ceci achève la démonstration du théorème.

3.3 Non-trivialité de cohomologie pour les p-groupes semi-abéliens

Cette section est consacrée à la démonstration des deux résultats suivants :

Théorème 3.3.1. *Soient G un p-groupe semi-abélien et N un sous-groupe normal de G tel que G/N ne soit pas cyclique ou un quaternion généralisé. Alors $\hat{H}^n(G/N, \mathrm{Z}(N)) \neq 0$, pour tout entier n.*

Théorème 3.3.2. *Soit G un p-groupe semi-abélien. Alors G possède un automorphisme non-intérieur d'ordre p, qui fixe tous les éléments de $\Phi(G)$.*

D'abord, montrons le résultat suivant du à Schmid ([67, Proposition 1]).

Proposition 3.3.3. *Soient G un p-groupe, et $1 \neq A$ un G-module qui est aussi un p-groupe. Si A est cohomologiquement trivial, alors $\mathrm{C}_G(A_K) = K$, pour tout $K \leq G$.*

Démonstration. Supposons que $K < \mathrm{C}_G(A_K)$, et soit xK un élément d'ordre p dans le centre du p-groupe $\mathrm{C}_G(A_K)/K$. Alors, K est un sous-groupe maximal dans $H = \langle x, K \rangle$. Le théorème de Gaschütz-Uchida implique que $\hat{H}^0(H, A) = 0$, donc par Lemma 3.2.5, $\hat{H}^0(H/K, A_K) = 0$. Comme H/K opère trivialement sur A_K, on a $(A_K)_{H/K} = A_K$, et $\tau_{H/K}(x) = x^p$, pour tout $x \in A_K$. D'où $(A_K)^{\tau_{H/K}} < A_K$, ce qui revient à dire que $\hat{H}^0(H/K, A_K) \neq 0$, contradiction. □

Lemme 3.3.4. *Soient G un p-groupe semi-abélien et N un sous-groupe normal de G tel que G/N ne soit pas cyclique ou un quaternion généralisé. Posons $A = \mathrm{Z}(N)$, et soit S/N un sous-groupe d'exposant p dans G/N. On a alors $A^p \leq A_{S/N}$, et ainsi $\mathrm{C}_{S/N}(A^p) = S/N$.*

Démonstration. Soient $x \in S$, et $a \in A$. On a $x^p \in N$, et donc par la version faible du Lemme 1.2.2, on a $[x,a]^p = 1$. Il en résulte que $(a^{-1}a[a,x])^p = 1$; et comme G est semi-abélien, on a

$$a^p = (a[a,x])^p = (a^x)^p = (a^p)^x.$$

D'où $A^p \leq A_{S/N}$. □

Démonstration du Théorème 3.3.1. Supposons que $\hat{H}^n(G/N, A) = 0$, pour certain entier n, où A désigne $\mathrm{Z}(N)$. Comme G/N n'est pas cyclique ou un quaternion généralisé Q_{2^m}, il y a un sous-groupe S/N dans G/N d'exposant p et d'ordre au moins p^2. Par Gaschütz-Uchida, implique que $\hat{H}^n(S/N, A) = 0$, et donc A est un S/N-module cohomologiquement trivial. Soit $K/N \leq S/N$ un sous-groupe d'ordre p. Encore, par Gaschütz-Uchida, on a $\hat{H}^0(K/N, A) = 0$. Or $\hat{H}^0(K/N, A) = A_{K/N}/A^\tau = 0$, où A^τ est l'image de A par l'homomorphisme trace $\tau : A \to A$ induit K/N. Comme K/N est cyclique d'ordre p, cette homomorphisme est donné par

$$\tau(a) = aa^x \dots a^{x^{p-1}},$$

pour tout $a \in A$; et n'importe quel élément $x \in K - N$. Il en résulte que

$$\tau(a) = (ax^{-1})^p x^p.$$

Comme G est semi-abélien, $a \in \ker\tau$ si, et seulement si $a^p = 1$; d'où $\ker\tau = \Omega_1(A)$. Ceci implique que $|A^\tau| = |A^p|$. On a $A_{K/N} = A^\tau$, et $A^p \leq A_{K/N}$; en vertu du lemme précédent, on a $A^p = A_{K/N}$. Par Proposition 3.3.3, $\mathrm{C}_{S/N}(A^p) = \mathrm{C}_{S/N}(A_{K/N}) = K/N$, mais le lemme précédent implique que $S/N = K/N$, une contradiction.

□

Démonstration du Théorème 3.3.2. Supposons pour une contradiction que tout automorphisme de G d'ordre p est intérieur. Soit $A = \mathrm{Z}(\Phi(G))$. En vertu de la réduction de Deaconescu-Silberberg, on peut supposer que $\mathrm{C}_G(A) = \Phi(G)$, et donc $\mathrm{C}_G(\mathrm{C}_G(A)) = A$. Si on démontre que $\mathrm{Der}(G/\mathrm{C}_G(A), A) = \mathrm{Der}(G/\Phi(G), \mathrm{Z}(\Phi(G))$ est d'exposant p ; alors d'après Corollaire 3.1.2, on a

$$\hat{H}^1(G/\Phi(G), \mathrm{Z}(\Phi(G))) = 0;$$

ceci contredit le théorème 3.3.1. Montrons alors que pour toute dérivation $\delta \in \mathrm{Der}(G, \mathrm{Z}(\Phi(G))$ qui est nulle sur $\Phi(G)$, $\delta(x)^p = 1$, pour tout $x \in G$. Soit $x \in G$; alors

$$\delta(x^p) = \delta(x)\delta(x)^x \dots \delta(x)^{x^{p-1}} = (\delta(x)x^{-1})^p x^p.$$

Comme δ est nulle sur $\Phi(G)$, on a $\delta(x^p) = (\delta(x)x^{-1})^p x^p = 1$; le fait que G est semi-abélien implique que $\delta(x)^p = 1$. □

Chapitre 4

Automorphismes quasi-centraux

Soit G un p-groupe. On a vu dans §2.3 que pour tout sous-groupe central A qui est contenu dans G'^{2p}, le groupe $\mathrm{Aut}_A(G)$ a une belle p-structure. On va généraliser ce résultat au cas où $A \leq Z_k(G)$, pour k suffisamment petit. Ceci est traité dans la première section.

Soit Z un sous-groupe normal d'ordre p de G. Si Z est invariant sous l'action d'un endomorphisme θ de G, alors θ induit un endomorphisme $\hat{\theta} \in \mathrm{End}(G/Z)$, donné par $\hat{\theta}(xZ) = \theta(x)Z$. On dit dans ce cas que θ est un prolongement de $\hat{\theta}$. Il est naturel de se demander quels sont les endomorphismes de G/Z qui se prolongent à G. La deuxième section de ce chapitre traite le problème de prolongement des endomorphismes centraux de G/Z.

Le reste du chapitre est consacré au problème de Berkovich pour les p-groupes de coclasse 2. Le cas $p = 2$ est traité indépendamment.

4.1 Anneaux de dérivations quasi-centrales

Soient G un groupe arbitraire, et A, B deux sous-groupes abéliens normaux de G tels que $B \leq A$ et $\delta(B) \subseteq B$ pour tout $\delta \in \mathrm{Der}(G, A)$. Alors on a un plongement canonique de l'anneau $\mathrm{Der}(G, B)$ dans $\mathrm{Der}(G, A)$.

Comme A/B est un sous-groupe abélien normal de G/B, on peut le considérer comme un G/B-module (à droite). Pour tout $\delta \in \mathrm{Der}(G, A)$, on peut associer une dérivation $\tilde{\delta}$ de G/B dans A/B, en posant $\tilde{\delta}(xB) = \delta(x)B$, pour tout $xB \in G/B$. Donc nous avons une application $\delta \mapsto \tilde{\delta}$ définie de $\mathrm{Der}(G, A)$ dans $\mathrm{Der}(G, B)$; qui est de plus un homomorphisme d'anneaux. La démonstration du résultat suivant est immédiate.

Proposition 4.1.1. *Sous la notation précédente, on a une suite exacte d'homomorphismes d'anneaux*

$$0 \to \mathrm{Der}(G, B) \to \mathrm{Der}(G, A) \to \mathrm{Der}(G/B, A/B).$$

Supposons maintenant que G est fini, et que $A \leq \Phi(G)$. Si $\delta : G \mapsto A$ est une dérivation, alors l'endomorphisme $1 + \delta$ est surjectif. En effet, sinon il existe un sous-groupe maximal M de G qui contient $x\delta(x)$, pour tout $x \in G$; ce qui implique que $x \in M$ pour tout $x \in G$; ce qui est contradictoire. La finitude de G implique alors que $1 + \delta$ est un automorphisme de G. Donc il en résulte de la relation de Laue que

Lemme 4.1.2. *Si G est fini et si $A \leq \Phi(G)$, alors l'anneau* $\mathrm{Der}(G, A)$ *est radical, et par suite nilpotent.*

Soit K un sous-groupe caractéristique de G. Le lemme ci-dessus implique que $\delta(k) \in K \cap A$, pour tout $k \in K$ et pour tout $\delta \in \mathrm{Der}(G, A)$. Donc par la Proposition 4.1.1, on a une suite exacte d'homomorphismes d'anneaux

$$0 \to \mathrm{Der}(G, K \cap A) \to \mathrm{Der}(G, A) \to \mathrm{Der}(G/K \cap A, A/K \cap A).$$

Proposition 4.1.3. *Soient G un p-groupe et A un sous-groupe normal abélien de G qui vérifie $A \leq G'G^{2p}$. Si $A \leq Z_k(G)$, alors l'anneau* $\mathrm{Der}(G, A)$ *est $(k, p, 0)$-nul.*

Démonstration. Pour $k = 1$, le résultat est immédiat par Lemme 2.3.21. Supposons que la proposition est vraie pour $k - 1$. Pour $K = \mathrm{Z}(G)$, la suite exacte précédente peut s'écrire

$$0 \to \mathrm{Hom}(G, \mathrm{Z}(G) \cap A) \to \mathrm{Der}(G, A) \to \mathrm{Der}(\bar{G}, \bar{A}),$$

où $\bar{G}$ désigne $G/\mathrm{Z}(G) \cap A$, et $\bar{A}$ est l'image de A dans $\bar{G}$. Soient $\delta, \delta_1, .., \delta_k \in \mathrm{Der}(G, A)$, telles que $2p\delta = 0$. Comme $A \leq Z_k(G)$, $\bar{A}$ est contenu dans $Z_{k-1}(\bar{G})$; et aussi on a $\bar{A} \leq \overline{G'G^{2p}} = \bar{G}'\bar{G}^{2p}$; donc par l'hypothèse de récurrence, l'anneau $\mathrm{Der}(\bar{G}, \bar{A})$ est $(k-1, p, 0)$-nul. Si on note par $\tilde{\delta}$ l'image de δ dans $\mathrm{Der}(\bar{G}, \bar{A})$, alors on a $2p\tilde{\delta} = 0$, et donc $\tilde{\delta}_{k-1} \ldots \tilde{\delta}_1 \tilde{\delta} = 0$, ce qui montre que $\delta_{k-1} \ldots \delta_1 \delta \in \mathrm{Hom}(G, \mathrm{Z}(G) \cap A)$. L'ordre de l'homomorphisme $\delta_{k-1} \ldots \delta_1 \delta$ divise $2p$, et donc son noyau contient $G'G^{2p}$ et en particulier A. D'où $(\delta_k \delta_{k-1} \ldots \delta_1 \delta)(x) = (\delta_{k-1} \ldots \delta_1 \delta)(\delta_k(x)) = 1$, pour tout $x \in G$. Ainsi $\delta_k \delta_{k-1} \ldots \delta_1 \delta = 0$. □

En vertu de la relation de Laue, la proposition précédente et les deux théorèmes 2.1.10 et 2.1.11, impliquent qu'il y a une restriction sévère sur la p-structure de $\mathrm{Aut}_A(G)$, lorsque $k = p - 2$ et $p \geq 3$, ou $k = 1$ et $p = 2$ (notons que les cas $p = 2, 3$ ont déjà été traités dans la Section 2.3). Plus précisément on a

Théorème 4.1.4. *Soit G un p-groupe et A un sous-groupe normal abélien de G qui vérifie $A \leq G'G^{2p}$ et $A \leq Z_k(G)$. Si $p \geq 3$ et $k = p - 2$, ou $p = 2$ et $k = 1$, alors*

(i) *pour tout $n \geq 1$, on a $\Omega_n(\mathrm{Aut}_A(G)) = \Omega_{\{n\}}(\mathrm{Aut}_A(G)) = \mathrm{Aut}_{A_i}(G)$, où A_i désigne $\Omega_n(A)$;*

(ii) *pour tout sous-groupe P de $\mathrm{Aut}_A(G)$, on a $|P : P^p| \leq |\Omega_1(P)|$.*

Un dual du théorème précédent est démontré dans un contexte plus général dans [38]. Regardant le résultat principal de ce dernier article, il est naturel de se demander s'il y a un analogue au Théorème précédent lorsque A n'est pas abélien.

4.2 Prolongement d'endomorphismes centraux

Sous la lumière de la relation de Laue, le problème de prolongement mentionné dans le début du chapitre, peut se réduire dans certains cas à un problème de prolongement de dérivations.

Dans la suite de cette section, on suppose que G est un p-groupe, p impair, A est un sous-groupe normal de G d'ordre p^2 est d'exposant p (et donc de rang 2), et on note Z_1 l'intersection de A avec le centre de G. C'est simple de voir que Z_1 est invariant par toutes les dérivations dans $\mathrm{Der}(G, A)$, et donc d'après la Proposition 4.1.1, on a une suite exacte

$$0 \to \mathrm{Hom}(G, Z_1) \to \mathrm{Der}(G, A) \to \mathrm{Hom}(G/Z_1, A/Z_1).$$

Si on note G/Z_1 et A/Z_1 par $\bar{G}$ et $\bar{A}$ respectivement, on a le diagramme commutatif suivant

$$\begin{array}{ccc} \mathrm{End}_A(G) & \longrightarrow & \mathrm{End}_{\bar{A}}(\bar{G}) \\ \downarrow & & \downarrow \\ \mathrm{Der}(G, A) & \longrightarrow & \mathrm{Hom}(\bar{G}, \bar{A}) \end{array}$$

où les flèches verticales désignent les isomorphismes de Laue. Le problème de prolongement des endomorphismes dans $\mathrm{End}_{\bar{A}}(\bar{G})$ revient alors à caractériser les groupes G tels que la suite suivante soit exacte,

$$0 \to \mathrm{Hom}(G, Z_1) \to \mathrm{Der}(G, A) \to \mathrm{Hom}(G/Z_1, A/Z_1) \to 0.$$

C'est un peu surprenant que ce problème dépend seulement de la structure du treillis des sous-groupes de $G/\gamma_3(G)G^p$. Avant d'annoncer notre résultat, on a besoin de quelques nouvelles notions.

Définition 4.2.1. *Soit C un sous-groupe maximal de G. On dit que G est plein par rapport à C, si tout sous-groupe maximal $M \neq C$ contient un sous-groupe K qui vérifie :*

(a) *K n'est pas normal et il est d'indice p^2 dans G ;*

(b) *$K \cap C$ est normal dans G, et il contient G^p.*

Une définition équivalente étant : pour tout sous-groupe maximal M de G, $M \cap C$ contient un sous-groupe maximal L qui est G-invariant et le quotient G/L est non-abélien d'exposant p. En effet, partant de la première définition, on peut prendre $L = K \cap C$. Inversement, on peut prendre K/L un sous-groupe de M/L d'ordre p qui est non-central dans G/L.

Voici quelques conséquences directes de la définition précédente :

(i) Pour que G soit plein par rapport à un sous-groupe maximal C il faut et il suffit que $G/\gamma_3(G)G^p$ soit plein par rapport à $C/\gamma_3(G)G^p$.

(ii) Si G est plein par rapport à un de ses sous-groupes maximaux, alors G ne peut pas être puissant.

(iii) Si G est plein par rapport à C, alors G est plein par rapport à $\sigma(C)$ pour tout $\sigma \in Aut(G)$.

La proposition suivante montre qu'il y a pleinement de p-groupes satisfaisant la définition précédente.

Proposition 4.2.2. *Si G n'est pas puissant et peut être engendrer par deux éléments, alors G est plein par rapport à tous ses sous-groupes maximaux.*

Démonstration. Soit C un sous-groupe maximal de G. Posons $N = \gamma_3(G)G^p$, et $G_1 = G/N$. Il en résulte que G_1 est d'exposant p et de classe au plus 2 ; et donc $\Phi(G_1) \leq Z(G_1)$, et ainsi $\Phi(G)/N \leq Z(G/N)$.

Si G_1 est abélien, alors $\gamma_2(G) \leq \gamma_3(G)G^p$. Ceci implique que $\gamma_2(G) \leq G^p$, et donc G est puissant, une contradiction. D'où G est de classe égale à 2.

Soit $M \neq C$ un sous-groupe maximal de G. Si $M_1 = M/N$ est cyclique, alors $|M_1| = p$, puisque G_1 est d'exposant p. Cela implique que $|G_1| = p^2$; d'où G_1 is abélien, une contradiction. Donc M_1 n'est pas cyclique, et ainsi il contient $p + 1$ sous-groupe maximal. Soit K/N un sous-groupe maximal de M/N qui est différent de $\Phi(G)/N$.

(a) Il en résulte immédiatement que $K \leq M$ est d'indice p^2. Si K est normal dans G, alors $\gamma_2(G) \leq K$. Puisque $G^p \leq K$, on obtient $\Phi(G) = K$, une contradiction. Donc K n'est pas normal dans G.

(b) On a $K \cap C \leq M \cap C = \Phi(G)$, donc $(K \cap C)/N \leq \Phi(G)/N \leq Z(G/N)$. D'où $K \cap C$ est normal dans G.

Ceci achève la démonstration. □

Le résultat principal de cette section étant

Théorème 4.2.3. *Supposons que G est purement non-abélien, $C = \mathrm{C}_G(A)$, et $Z_1 = A \cap Z(G)$. Alors la suite*

$$0 \to \mathrm{Hom}(G, Z_1) \to \mathrm{Der}(G, Z_1) \to \mathrm{Hom}(G/Z_1, A/Z_1) \to 0$$

est exacte si et seulement si G est plein par rapport C.

On a besoin de quelques préliminaires pour la démonstration ; on suppose à travers que G est plein par rapport à $C = C_G(A)$, et K désigne un sous-groupe d'un sous-groupe maximal fixé $M \neq C$, qui satisfait les conditions de la définition 4.2.1.

Lemme 4.2.4. *Soit $y \in C - M$ et $x \in M - K$. Alors l'application $k \mapsto \alpha(k)$ de K dans $\mathbb{Z}_p$ définie par*

$$[k, y] = x^{\alpha(k)} \text{ mod } K$$

est un homomorphisme de groupe dont noyau est égal à $K \cap C$.

Démonstration. On a $K \neq K \cap C$ et $K/K \cap C \cong KC/C$ est d'ordre p. Il en résulte que $K \cap C$ est d'indice p^3 dans G, et donc $\gamma_3(G) \leq K \cap C$.

Soit $k, k' \in K$. alors

$$[kk', y] = [k, y][k, y, k'][k', y]$$

donc

$$[kk', y] = [k, y][k', y] \text{ mod } K$$

et ainsi

$$x^{\alpha(kk')} = x^{\alpha(k)} x^{\alpha(k')} \text{ mod } K.$$

Ceci montre que α est un homomorphisme.

Si α est nul, alors $\langle y \rangle \leq \mathrm{N}_G(K)$; et comme $M \leq \mathrm{N}_G(K)$, cela implique que $K \lhd G$, une contradiction. D'autre part, on a $K \cap C$ est normal dans G, et donc $K \cap C \leq \ker \alpha$; ceci implique que $K \cap C = \ker \alpha$, car $\ker \alpha$ est d'indice p dans K.

□

Lemme 4.2.5. *Pour tout $u \in A - Z_1$, il existe $z \in Z_1$ tel que $[k, u] = z^{\alpha(k)}$, pour tout $k \in K$; où $\alpha : K \to \mathbb{Z}_p$ est l'homomorphisme défini dans le Lemme 4.2.4.*

Démonstration. Comme $|A| = p^2$, on a $A \leq Z_2(G)$. Donc $[k, u] \in A \cap Z(G) = Z_1$, pour tout $k \in K$. Il en résulte que la relation $k \mapsto [k, u]$ est un homomorphisme de K dans Z_1, et son noyau est égal à $K \cap C$.

Pour chaque élément non-trivial z_0 de Z_1, on a un homomorphisme $\beta : K \to \mathbb{Z}_p$ avec $[k, u] = {z_0}^{\beta(k)}$. On a ainsi deux homomorphismes α et β définis de K de $\mathbb{Z}_p$, et leurs noyaux sont égaux à $K \cap C$. On peut alors les identifier à des homomorphismes dans $\mathrm{Hom}(K/(K \cap C), \mathbb{Z}_p)$ qui est isomorphe à $\mathbb{Z}_p$. Donc il existe un entier $0 < i < p$ tel que $\beta = i\alpha$, et ainsi on a pour $z = z_0^i$,

$$[k, u] = z_0^{\beta(k)} = z^{\alpha(k)}, \text{ pour tout } k \in K.$$

□

Le lemme suivant est la clé pour démontrer le théorème 4.2.3.

Lemme 4.2.6. *Soit $y \in C-M$ et $x \in \Phi(G)-K$. Alors pour tout $u \in C-Z_1$, il existe $z \in Z_1$ tel que $\delta : G \to A$ définie par $\delta(kx^jy^i) = z^ju^i$ est une dérivation ; où $k \in K$ et $i, j \in \mathbb{N}$.*

Démonstration. Soit z comme défini dans le lemme précédent.

D'abord, montrons que δ est une application bien définie. Tout élément $g \in G$ s'écrit comme $g = kx^jy^i$, où $k \in K$ et $i, j \in \mathbb{N}$. Si $g = kx^jy^i = k'x^{j'}y^{i'}$, alors $y^i = y^{i'} \bmod M$. Donc p divise $i - i'$; c-à-d $i - i' = pl$ pour certain entier l. On a $kx^jy^{pl} = k'x^{j'}$. Or $y^{pl} \in G^p \leq K$, on a $x^j = x^{j'} \bmod K$; et donc p divise $j - j'$. Comme A is élémentaire abélien, on a $u^{i-i'} = z^{j-j'} = 1$, et donc $z^ju^i = z^{j'}u^{i'}$.

Montrons maintenant que δ est une dérivation. Soit $g = kx^jy^i$ et $g' = k'x^{j'}y^{i'}$. On a

$$\begin{aligned} gg' &= kx^j[y^{-i}, x^{-j'}k'^{-1}]k'x^{j'}y^{i+i'} \\ &= kx^j[y^{-i}, k'^{-1}][y^{-i}, x^{-j'}]^{k'^{-1}}k'x^{j'}y^{i+i'}. \end{aligned}$$

Comme $K \cap C$ est maximal dans K, $K \cap C$ est d'indice p^2 dans C ; et comme $K \cap C$ est normal dans G, on a $\gamma_2(C) \leq K \cap C$. D'où $k_1 = [y^{-i}, x^{-j'}]^{k'^{-1}} \in K \cap C$.

On a aussi

$$\begin{aligned} [y^{-i}, k'^{-1}] &= \prod_{r=i-1}^{0} [y^{-1}, k'^{-1}]^{y^{-r}} \\ &= \prod_{r=i-1}^{0} [y^{-1}, k'^{-1}][y^{-1}, k'^{-1}, y^{-r}] \\ &= [y^{-1}, k'^{-1}]^i k_2 \end{aligned}$$

pour certain $k_2 \in K$; et on a

$$\begin{aligned} [y^{-1}, k'^{-1}]^i &= ([y, k'^{-1}]^{y^{-1}})^{-i} = ([k'^{-1}, y]^i)^{y^{-1}} \\ &= [k'^{-1}, y]^i[[k'^{-1}, y]^i, y^{-1}] \\ &= x^{-i\alpha(k')}k_3 \end{aligned}$$

pour certain $k_3 \in K$. Il en résulte

$$\begin{aligned} gg' &= kx^jx^{-\alpha(k')}k_3k_2k_1k'x^{j'}y^{i+i'} \\ &= k_4x^{j+j'-i\alpha(k')}y^{i+i'} \end{aligned}$$

pour certain $k_4 \in K$. Par suite, $\delta(gg') = z^{j+j'-i\alpha(k')}u^{i+i'}$. D'autre part,

$$\delta(g)^{g'}\delta(g') = (z^ju^i)^{k'x^{j'}y^{i'}}z^{j'}u^{i'}.$$

Le fait que $x^{j'}y^{i'} \in C_G(A) = C$, implique

$$\begin{aligned}\delta(g)^{g'}\delta(g') &= (z^j u^i)^{k'} z^{j'} u^{i'} \\ &= z^j (u^{k'})^i z^{j'} u^{i'} \\ &= z^j u^i [u, k']^i z^{j'} u^{i'}\end{aligned}$$

Par Lemme 4.2.5, on a $[u, k']^i = z^{-i\alpha(k')}$; d'où

$$\delta(g)^{g'}\delta(g') = z^{j+j'-i\alpha(k')} u^{i+i'} = \delta(gg').$$

□

Démonstration du Théorème 4.2.3. D'abord on va montrer que si G est pleine par rapport à $C = C_G(A)$, alors la suite suivante est exacte.

$$\mathrm{Der}(G, A) \to \mathrm{Hom}(G/Z_1, A/Z_1) \to 0$$

Soit $f \in \mathrm{Hom}(G/Z_1, A/Z_1)$. Si $f = 0$, alors on peut la prolonger à la dérivation triviale dans $\mathrm{Der}(G, A)$. Donc supposons que $f \neq 0$. Comme $|A/Z_1| = p$, le noyau de f est un sous-groupe maximal dans G/Z_1 ; donc il a la forme M/Z_1, où M un sous-groupe maximal dans G. On a deux cas :

1. $M \neq C$.
   Soient $y \in C - M$, et $u \in A - Z_1$ tels que $uZ_1 = f(yZ_1)$. Soit K un sous-groupe de M satisfaisant les conditions (a) et (b) dans la définition 4.2.1, et soit $x \in \phi(G) - K$. Par le Lemme 4.2.6, il existe $z \in Z_1$ tel que $\delta : G \to A$ définie par $\delta(kx^j y^i) = z^j u^i$ est une dérivation ; et f est induit par δ.
2. $M = C$.
   Soit $t \in G - C$, et soit $u \in A - Z_1$ tel que $uZ_1 = f(tZ_1)$. L'identité

   $$(xu)^p = x^p u^p [x, u]^{\binom{p}{2}}, \text{ pour tout } x \in G$$

   implique

   $$u^{1+t+\ldots+t^{p-1}} = 1.$$

   Il est facile maintenant de voir que

   $$\delta(t^i m) = u^{1+t+\ldots+t^{i-1}}$$

   est une dérivation de G dans A, qui induit f.

Inversement, supposons que la suite ci-dessus est exacte. Soit $M \neq C$ un sous-groupe maximal de G. Comme G est purement non-abélien, $Z_1 \leq M$, et ainsi M/Z_1 est maximal dans G/Z_1. Soit l'homomorphisme canonique

$r : G/Z_1 \to \mathbb{Z}_p \cong G/M$. Si $u \in A - Z_1$, on peut définir un homomorphisme $f : G/Z_1 \to A/Z_1$, avec

$$f(xZ_1) = (uZ_1)^{r(xZ_1)}$$

Le noyau de f est égal à M/Z_1 ; et par hypothèse, f se prolonge à une dérivation $\delta : G \to A$. Considérons $K = \ker \delta = \{x \in G, \delta(x) = 1\}$.

On a $K \leq M$; sinon $G = MK$, ce qui implique que $G/Z_1 \leq ker(f)$, une contradiction. D'où K coïncide avec le noyau de la restriction $\delta/M : M \to A$. Puisque δ applique M sur Z_1, $\delta/M : M \to Z_1$ est un homomorphisme de groupes. Ceci implique que K est d'indice au plus p^2 dans G.

Si K est normal dans G, alors $\gamma_2(G) \leq K$. Soit $y \in C - M$ tel que $\delta(y) = u$, avec $u \in A - Z_1$. Alors pour tout $m \in M$, on a

$$\delta(my) = \delta(m)^y \delta(y) = \delta(m)u.$$

D'autre part, on a

$$\delta(my) = \delta(ym[m,y]) = \delta(ym)^{[m,y]}\delta([m,y]) = \delta(ym) = u^m\delta(m).$$

Ceci implique que $u^m = u$, pour tout $m \in M$. D'où $M \leq C_G(u) = C$, une contradiction. Donc K n'est pas normal dans G, et son indice dans G est p^2.

Finalement, on a $\delta(k^g) = 1$, pour tous $k \in K \cap C$ et $g \in G$; ce qui implique que $K \cap C \lhd G$. On a aussi $G^p \leq K$, puisque pour tout $x \in G$:

$$\begin{aligned} \delta(x^p) &= \prod_{r=o}^{p-1} \delta(x)^{x^i} = \prod_{r=o}^{p-1} \delta(x)[\delta(x), x^i] \\ &= \delta(x)^p [\delta(x), x]^{\binom{p}{2}} = 1. \end{aligned}$$

Ceci montre le résultat. □

Corollaire 4.2.7. *Soit G un p-groupe, qui est plein par rapport à tous ses sous-groupes maximaux, et qui a un centre cyclique. Alors pour tout sous-groupe élémentaire abélien A de G, tel que $A \lhd G$ et $A \leq \zeta_2(G)$; la suite*

$$0 \to \mathrm{Hom}(G, Z_1) \to \mathrm{Der}(G, A) \to \mathrm{Hom}(G/Z_1, A/Z_1) \to 0$$

est exacte. Ici $Z_1 = A \cap \mathrm{Z}(G)$.

Démonstration. Soit $f \in \mathrm{Hom}(G/Z_1, A/Z_1)$, et soit $(\bar{v}_1, ..., \bar{v}_s)$ une base du $\mathbb{Z}_p$-espace vectoriel A/Z_1. Pour tout $i \in \overline{1, s}$, soit A_i le sous-groupe de A défini par $A_i/Z_1 \cong < \bar{v}_i >$. Il en résulte immédiatement que A_i est un sous-groupe élémentaire abélien de rang 2, $A \lhd G$, et

$$\mathrm{Hom}(G/Z_1, A/Z_1) \cong \bigoplus_i \mathrm{Hom}(G/Z_1, A_i/Z_1).$$

Donc f peut s'écrire comme $f = \sum_i f_i$, où $f_i \in \mathrm{Hom}(G/Z_1, A_i/Z_1)$. Le Théorème 4.2.3, implique que f_i se prolonge à une dérivation $\delta_i : G \to A_i \subset A$. Il en résulte que $\delta = \sum_i \delta_i : G \to A$ est une dérivation, qui induit f.

□

4.3 Automorphismes non-intérieurs des p-groupes de coclasse 2

Dans cette dernière section, on établit

Théorème 4.3.1. *Soit G un p-groupe de coclasse 2. Alors G possède un automorphisme non-intérieur d'ordre p.*

Dans [4], on peut trouver une démonstration courte, qui nécessite pas le matériel développé dans la section précédente ; mais ce court argument n'est qu'une forme assez particulière du Théorème 4.2.3. Comme on a choisi d'inclure le Théorème 4.2.3 en toute généralité, l'argument qu'on va donner ici est un peu différent de celui dans [4]. Le cas $p = 2$, est bien sur indépendant de la section précédente.

Le cas où $p \geq 3$. Par Théorème 2.3.24, on peut supposer que $\mathrm{d}(G)\,\mathrm{d}(Z_1(G)) = \mathrm{d}(Z_2(G)/Z_1(G))$. Puisque G est de coclasse 2, $Z_2(G)/Z_1(G)$ est d'ordre au plus p^2 ; donc $\mathrm{d}(Z_2(G)/Z_1(G)) \leq 2$. Il en résulte que $|Z_2(G)/Z_1(G)| = p^2$, $|Z_1(G)| = p$, et $\mathrm{d}(G) = 2$. Donc G est 2-généré et $\mathrm{Z}(G)$ est cyclique. Aussi, moyennant la réduction de Deaconescu-Silberberg ([23]), on doit supposer que $\mathrm{C}_G(\mathrm{Z}(\Phi(G))) = \Phi(G)$, et donc $C_G(\Phi(G)) \leq \Phi(G)$.

Soit le sous-groupe H de G défini par $H/Z_1(G) = \Omega_1(Z_2(G)/Z_1(G))$, et soit $H_1 = \Omega_1(H)$. Or $\Phi(G) \leq \mathrm{C}_G(H_1)$, on a $H_1 = \mathrm{C}_G(\Phi(G)) \leq \Phi(G)$; et donc par Corollaire 4.2.7, on a la suite exacte :

$$0 \to \mathrm{Hom}(G, Z_1) \to \mathrm{Der}(G, H_1) \to \mathrm{Hom}(G/Z_1, H_1/Z_1) \to 0.$$

On a alors,

$$|\,\mathrm{Der}(G, H_1)| = |\,\mathrm{Hom}(G, Z_1)||\,\mathrm{Hom}(G/Z_1, H_1/Z_1)|.$$

Or

$$|\,\mathrm{Hom}(G, Z_1)| = |\,\mathrm{Hom}(G/\Phi(G), Z_1)| = |\,\mathrm{Hom}(\mathbb{Z}_p \oplus \mathbb{Z}_p, \mathbb{Z}_p)| = p^2,$$

et

$$|\,\mathrm{Hom}(G/Z_1, H_1/Z_1)| = p^2;$$

on a $|\,\mathrm{Der}(G, H_1)| = p^4$. D'où $\mathrm{Aut}_{H_1}(G) = p^4$. Maintenant, soit τ_g l'automorphisme intérieur induit par $g \in G$. Si $\tau_g \in \mathrm{Aut}_{H_1}(G)$, alors $[x, g] \in H_1 \leq Z_2(G)$; d'où $g \in Z_3(G)$. Puisque $Z_3(G)$ est d'ordre p^4, le groupe d'automorphismes intérieurs induit par $Z_3(G)$ est d'ordre $|\zeta_3(G)/\zeta(G)| = p^3$. Donc $\mathrm{Aut}_{H_1}(G)$ contient des automorphismes non-intérieurs. Il suffit maintenant de voir que $\mathrm{Aut}_{H_1}(G)$ est d'exposant p, ce qui résulte immédiatement du Théorème 4.1.4 (pour $p = 3$, voir le paragraphe après la démonstration du Théorème 2.2.3).

□

Pour $p = 2$, on ne peut que reproduire la démonstration établie dans [4], et il ressemble mieux de référer le lecteur à cet article pour cette démonstration, et pour une preuve alternative du cas $p > 2$.

Bibliographie

[1] A. Abdollahi, Cohomologically trivial modules over finite groups of prime power order, *J. Algebra* **342** (2011), 154-160

[2] A. Abdollahi, Powerful p-groups have noninner automorphisms of order p and some cohomology, *J. Algebra* **323** (2010), 779-789

[3] A. Abdollahi, *Finite p-groups of class* 2 *have noninner automorphisms of order p*, J. Algebra, **312** (2007), 876-879.

[4] A. Abdollahi, S. M. Ghoraishi, Y. Guerboussa, M. Reguiat and B. Wilkens, Noninner automorphisms of order p for finite p-groups of coclass 2, *J. Group Theory.* **17** (2014), 267-272.

[5] A. Abdollahi, M. Ghoraishi and B. Wilkens, Finite p-groups of class 3 have noninner automorphisms of order p, *Beitr. Algebra Geom.* **54**, No. 1, 363-381 (2013).

[6] B. Amberg and O. Dickenschied, On the adjoint group of a radical ring, *Canad. Math. Bull.* **38** (1995), 262-270.

[7] B. Amberg, S. Franciosi and F. de Giovanni, Products of groups, Oxford University Press, 1992.

[8] D.E. Arganbright, The power-commutator structure of finite p-groups, *Pacific J. Math.* **29** (1969), 11-17.

[9] R. Baer and H. Heineken, Radical groups of finite abelian subgroup rank, *Illinois J. Math.* **16** (1972), 533-580.

[10] M.. T. Benmoussa and Y. Guerboussa, Some properties of semi-abelian p-groups, *Bull. Aust. Math. Soc.* (2014) doi :10.1017/S000497271400080X.

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

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

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

[14] J. N. S. Bidwell, Automorphisms of direct products of finite groups II, *Arch. Math.* **91** (2008), 111-121.

[15] S. R. Blackburn, P. M. Neumann and G. Venkataraman, Enumeration of Finite Groups, Cambridge University Press, 2007.

[16] K. S. Brown, Cohomology of groups, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1982.

[17] D. Bubboloni, G. Corsi Tani, p-Groups with some regularity properties, *Ric. di Mat.* **49** (2) (2000), 327-339.

[18] D. Bubboloni, G. Corsi Tani, p-groups with all the elements of order p in the center, *Algebra Colloq.* **11** (2004), 181-190.

[19] A. Caranti, A module-theoretic approach to abelian automorphism groups, *Israel J. Math.*, DOI : 10.1007/s11856-014-1106-z (2014).

[20] A. Caranti and S. Mattarei, Automorphisms of p-groups of maximal class, *Rend. Sem. Mat. Univ. Padova* **115** (2006), 189 -198.

[21] F. Catino and M. M. Miccoli, A note on IA-automorphisms of two-generated metabelian groups, *Rend. Sem. Mat. Univ. Padova* **96** (1996), 99 -104.

[22] M.J. Curran, D.J. McCaughan, Central automorphisms that are almost inner, *Comm. Algebra,* **29** (2001), 2081-2087.

[23] M. Deaconescu, G. Silberberg, Noninner automorphisms of order p of finite p-groups, *J. Algebra* **250** (2002), 283-287.

[24] O. Dickenschied, On the adjoint group of some radical rings, Glasgow Math. J. 39 (1997), 35-41.

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

[26] B. Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups, *Comm. Algebra*, **30** (2002), 2271-2295.

[27] G. A. Fernández-Alcober, J. González-Sánchez et A. Jaikin-Zapirain, Omega subgroups of pro-p groups, *Isr. J. Math.* **166** (2008), 393-412.

[28] The GAP Group, GAP Groups, Algorithms, and Programming, www.gap-system.org.

[29] W. Gaschütz, Kohomologische Trivialitäten und äußere Automorphismen von p-Gruppen. *Math. Z.* **88**, 432-433 (1965).

[30] W. Gaschütz, Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen, *J. Algebra*, **4** (1966), 1-2.

[31] M. S. Ghoraishi, On noninner automorphisms of finite nonabelian p-groups, *Bull. Austral. Math. Soc.* **89** (2014), 202-209.

[32] S. M. Ghoraishi, A note on automorphisms of finite p-groups, *Bull. Aust. Math. Soc.* **87** (2013), 24-26.

[33] J. González-Sánchez and A. Jaikin-Zapirain, On the structure of normal subgroups of potent p-groups, *J. Algebra* **276** (2004), 193-209.

[34] J. González-Sánchez and A. Jaikin-Zapirain, Finite p-groups with small automorphism group, arXiv :1406.5772v1 [math.GR] (2014).

[35] J. González-Sánchez and T. S. Weigel, Finite p-central groups of height k, *Isr. J. Math.* **181** (2011), 125-143.

[36] D. Gorenstein, Finite groups, Chelsea, New York, 1980.

[37] K.W. Gruenberg, Cohomological Topics in Group Theory, *Lecture Notes in Math.*, vol. 143, Springer-Verlag, Berlin, 1970.

[38] Y. Guerboussa, p-Central action on finite groups, *J. Algebra* **424** (2014), 242-253.

[39] Y. Guerboussa and B. Daoud, Adjoint groups of p-nil rings and p-group automorphisms, *Bull. Belg. Math. Soc. Simon Stevin* **21** (2014), 339-349.

[40] Y. Guerboussa and B. Daoud, On central automorphisms of groups and nilpotent rings, preprint.

[41] P. Hall, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.* **36** (1933), 29-95.

[42] P. Hall and G. Higman, The p-length of a p-soluble group and reduction theorems for Burnside's problem, *Proc. London Math. Soc.* (3) **6** (1956), 1-42.

[43] G. T. Helleloid and U. Martin, The automorphism group of a finite p-group is almost always a p-group, *J. Algebra*, **312** (2007), 294-329.

[44] G. T. Helleloid, Automorphism Groups of Finite p-Groups : Structure and Applications, Ph.D thesis (2007).

[45] H. W. Henn and S. Priddy, p-nilpotence, classifying space indecomposability, and other properties of almost all finite groups, *Comment. Math. Helv.,* **69** (1994), 335-350.

[46] P. J. Hilton and U. Stammbach, A Course in Homological Algebra, Springer-Verlag, New York (1970).

[47] K. Hoechsmann, P. Roquette and H. Zassenhaus, A Cohomological Characterization of Finite Nilpotent Groups, *Arch. Math.* **19** (1968), 225-244.

[48] B. Huppert, Endliche Gruppen. I. *Die Grundlehren der Mathematischen Wissenschaften*, Band 134. Springer-Verlag, Berlin, 1967.

[49] B. Huppert and N. Blackburn, Finite Groups II, Springer-Verlag, Berlin, 1982.

[50] M.H. Jafari and A.R. Jamali, On the nilpotency and solubility of the central automorphism group of finite group, *Algebra Coll.* **15** :3 (2006), 485-492.

[51] V. K. Jain, P. K. Rai and M. K. Yadav, On finite p-groups with abelian automorphism group, *International Journal of Algebra and Computation* **23** (2013), 1063-1077.

[52] A. R. Jamalli and M. Viseh, On the existence of noninner automorphisms of order two in finite 2-groups, *Bull. Aust. Math. Soc.*, **87** (2013), 278–287.

[53] M. I. Kargapolov, On solvable groups of finite rank. (Russian). *Algebra i Logika,* **1**(5) (1962), 37-44.

[54] E. I. Khukhro, p-Automorphisms of Finite p-Groups, Cambridge University Press, 1998.

[55] R.L. Kruse and D.T. Price, Nilpotent rings, Gordon and Breach, New York, 2010.

[56] T.J. Laffey, The minimum number of generators of a finite p-group, *Bull. London Math. Soc.* **5** (1973) 288-290.

[57] H. Laue, On group automorphisms which centralize the factor group by an abelian normal subgroup, *J. Algebra.* **96** (1985), 532-547.

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

[59] J.C. Lennox, D.J.S. Robinson, The Theory of Infinite Soluble Groups, Oxford Univ. Press, Oxford, 2004.

[60] H. Liebeck, Outer automorphisms in nilpotent p-groups of class 2, *J. London Math. Soc.*, **40** (1965), 268-275.

[61] I. Malinowska, p-automorphisms of finite p-groups : problems and questions, in : *Advances in Group Theory 2002,* (2002), 111-127.

[62] A. Mann, Some questions about p-groups, *J. Aust. Math. Soc.*, **67** (3) (1999), 356-379.

[63] V.D. Mazurov and E. I. Khukhro, The Kourovka Notebook. Unsolved Problems in Group Theory. 18th Edition, Russian Academy of Sciences, Siberian Division, Institute of Mathematics, Novosibirsk, 2014.

[64] A. R. Patterson, The minimal number of generators for p-subgroups of $GL(n, p)$, *J. Algebra* **32** (1974), 132-140.

[65] L. Pyber, Enumerating finite groups of a given order,*Ann. Math.* **137** (1993) 203-20.

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

[67] P. Schmid, A cohomological property of regular p-groups, *Math. Z.* **175** (1980) 1-3.

[68] P. Schmid, Normal p-subgroup in the group of outer automorphisms of a finite p-group, *Math. Z.* **147** (1976), 271-277.

[69] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math.* Soc.(2) **55** (1997), 320-334.

[70] J.- P. Serre, Corps locaux, Hermann, Paris, 1968.

[71] M. Shabani Attar, On a conjecture about automorphisms of finite p-groups, *Arch. Math.* **93** (2009), 399-403.

[72] M. Shabani-Attar, Existence of noninner automorphisms of order p in some finite p-groups, *Bull. Aust. Math. Soc.*, **87** (2013), 272-277.

[73] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math.* Soc.(2) **55** (1997), 320-334.

[74] K. Shoda, Über die Automorphismengruppe einer endlichen Abelschen Gruppe, *Math. Ann.* **100** (1928), 674-686.

[75] K. Uchida. On Tannaka's conjecture on the cohomologically trivial modules. *Japan Acad.* **41** (1965), no. 4, 249-253.

[76] M. R. Vaughan-Lee, The Restricted Burnside Problem, 2nd edition, Oxford University Press, Oxford, 1993.

[77] U. H. M. Webb, An elementary proof of Gaschtüz' theorem, *Arch. Math.* **35** (1980), 23-26.

[78] D. L. Winter. The automorphism group of an extraspecial p-group, *Rocky Mountain J. Math.*, **2** (1972), 159-168.

[79] M.Y. Xu, A class of semi-p-abelian p-groups (in Chinese), *Kexue Tongbao* **26** (1981), 453-456. English translation in *Kexue Tongbao* (English Ed.) **27** (1982), 142-146

[80] M.Y. Xu, The power structure of finite p-groups, *Bull. Aust. Math. Soc.* **36** (1987), no. 1, 1-10.

[81] M. K. Yadav, Class preserving automorphisms of finite p-groups : a survey, Groups St Andrews - 2009 (Bath), *LMS Lecture Note Ser.* **388** (2011), 569-579.

ملخص

إن فرضية قديمة تقول بأن كل p- زمرة منهية غير آبلية تملك تشاكلا ذاتيا غير داخلي ذا رتبة p . في هذه الأطروحة نثبت صحة هذه االفرضية لفئة الـــ p – زمر المنتهية والنصف الآبلية. نثبت أيضا صحة هذه الفرضية لكل الـــ p زمر المنتهية ذات تصنف 2.

الكلمات و الجمل المهمة: p- زمرة ، كهومولوجية الز مر، حلقة عديمة القوى زمرة ادجونة.

تصنيف أمريكي للمواضيع. 16N20; 20D45 .

Abstract .

A long-standing conjecture asserts that every finite non-abelian p-group has a non-inner automorphism of order p. In this thesis, we prove the validity of this conjecture for the class of finite semi-abelian p-groups. This conjecture also is proved for finite p-groups of coclass 2.

Key words and phrases: p-groups, cohomology of groups, nilpotent rings, adjoint groups.

Mathematics Subject Classification: Primary: 20D45; Secondary: 16N20.

Résumé.

Une ancienne conjecture affirme que tout p-groupe fini non abélien admet un automorphisme non intérieur d'ordre p. Dans cette thèse, on prouve la validité de cette conjecture pour la classe des p-groupes finis semi-abéliens. Cette conjecture est aussi prouvée pour les p-groupes finis de coclasse 2.

Mots et Phrases Clés: p-groupes, cohomologie des groupes, anneaux nilpotent, groupes adjoints.

Mathematics Subject Classification: Primary: 20D45; Secondary: 16N20.