INSTITUT DE MATHÉMATIQUES

Propriétés locales des groupes finis

Thèse de doctorat

présentée à la

Faculté des Sciences de
l'Université de Lausanne

par

Stancu Radu

Diplômé en Mathématiques
Université de Genève

Jury

M. le Prof. Aurelio Bay, président
M. le Prof. Jacques Thévenaz, directeur de thèse
M. le Prof. Pierre de la Harpe, expert
M. le Prof. Markus Linckelmann, expert

LAUSANNE
2002

Remerciements

Je remercie profondement le Professeur Jacques Thévenaz d'avoir assumé la direction de mon travail. Sa force mathématique, ses conseils clairvoyants, son intransigence, son soutien moral et sa disponibilité ont été essentiels pour l'aboutissement de ce doctorat.

Je remercie le Professeur Markus Linkelmann et son épouse, le Professeur Rhada Kessar, pour les longues discutions mathématiques et pour les idées astucieuses dont j'ai profité pleinement. Je remercie le Professeur Pierre de la Harpe pour ses nombreux commentaires et pour m'avoir fait comprendre au plus profond plusieurs aspects de mon travail.

Je remercie le Professeur Thierry Vust pour sa constante disponibilité et son écoute à mon égard. Je remercie mes collègues de Genève et Lausanne pour tous les moments agréables passés en leur companie.

Je remercie de tout mon coeur Anne-Lise, Cécilia et François pour m'avoir accueilli avec amour dans leur famille et pour m'avoir offert la possibilité de faire des études en Suisse. Enfin, mais pas en dernier lieu, merci infiniment à Veronika, à mes parents et à mes frères pour leur amour et leur soutien inconditionnel.

Table des matières

Résumé

Le but de ce travail est d'approfondir certains aspects de la structure locale d'un groupe fini. Soit p un nombre premier et G un groupe fini. La *catégorie de Frobenius de G*, notée $F_p(G)$, est la catégorie qui a comme objets les p-sous-groupes de G et comme morphismes, les morphismes de groupe donnés par les conjugaisons par les éléments de G. On appelle ces morphismes des *p-fusions*. Cette catégorie est étudiée en détail dans le premier chapitre. On verra que $F_p(G)$ fournit des informations importantes sur G et, dans certains cas, même la structure de G.

En 1967 Alperin a demontré [Al] que les morphismes dans $F_p(G)$ au-dessous d'un p-sous-groupe de Sylow P de G peuvent être décrits à partir du groupe $N_G(P)/C_G(P)$ et des groupes $N_G(E)/C_G(E)$, où E parcourt la famille des p-sous-groupes *essentiels* de G contenus dans P. Le chapitre 2 est consacré aux p-sous-groupes essentiels. Comme les p-sous-groupes essentiels sont rares, on trouve des conditions sur un p-groupe Q pour que Q ne puisse jamais être réalisé comme p-sous-groupe essentiel d'un groupe fini. Pour $p = 2$, on obtient que, à l'exception de $C_2 \times C_2$ et Q_8, les groupes de quaternions, diédraux et semi-diédraux ont cette propriété. Pour p impair, on montre que certaines tours d'extensions scindées dans lesquelles le sous-groupe normal est un p-groupe cyclique, un cas spécial de produit semi-direct d'un p-groupe abélien par un p-groupe cyclique et les p-groupes métacycliques non-abéliens ne peuvent pas non plus être réalisés comme des p-sous-groupes essentiels.

Un des résultats de cette théorie est qu'un groupe fini G ne contient pas de p-sous-groupes essentiels si et seulement si $F_p(G) = F_p(N_G(P))$, où P est un p-sous-groupe de Sylow de G. Etant donné qu'il y a peu de p-sous-groupes essentiels, on peut se poser la question s'il y a des p-groupes P tels que, quelle que soit leur réalisation comme un p-sous-groupe de Sylow dans un groupe G, on a $F_p(G) = F_p(N_G(P))$. On appelle un tel p-groupe *résistant*. Burnside avait déjà remarqué que les p-groupes abéliens avaient cette propriété. Dans le chapitre 3 on présente d'autres exemples de groupes résistants. Le résultat principal de ce travail est que les p-groupes extraspéciaux généralisés sont résistants. Par ailleurs, pour p impair, on donne une autre preuve du fait, démontré par Glauberman et Dietz, que les p-groupes métacycliques sont résistants.

Une catégorie sur un p-groupe P est une catégorie ayant comme objets les sous-groupes de P et comme morphismes, un ensemble de morphismes de groupe injectifs. Dans les années '90, Puig construit un système d'axiomes sur ce type de catégorie dans le but de généraliser $F_p(G)$. Si une catégorie sur P satisfait ce système d'axiomes alors on appelle cette catégorie un système complet de Frobenius sur P. Le chapitre 4 est consacré à la description des systèmes complets de Frobenius et à la généralisation dans ce nouveau contexte des résultats des chapitres précédents. On définit la notion de groupe résistant dans les systèmes complets de Frobenius et on démontre que les p-groupes appartenant aux familles du chapitre 3 restent résistants dans ce contexte.

Abstract

The purpose of this work is to deeper understand some aspects of the local structure of a finite group. Let p be a prime number and G a finite group. The *Frobenius category of* G, denoted by $F_p(G)$, is the category whose objects are the p-subgroups of G and whose morphisms are morphisms of group given by conjugation by the elements of G. We call these morphisms *p-fusions*. This category is studied in detail in the first chapter. We'll see that $F_p(G)$ gives important informations on G and, in some cases, even the structure of G.

In 1967 Alperin proved [Al] that the morphisms in $F_p(G)$ under a Sylow p-subgroup P of G can be completely understood from the group $N_G(P)/C_G(P)$ and the groups $N_G(E)/C_G(E)$, where E is in the family of the *essential* p-subgroups contained in P. Chapter 2 is devoted to the essential p-subgroups. As the essential p-subgroups are rare, we'll find conditions on a p-group Q so that Q can't be realised as an essential p-subgroup of a finite group. For $p = 2$, we obtain that, excepting $C_2 \times C_2$ and Q_8, the quaternions, dihedral and semi-dihedral groups have this property. For p odd, we show that some towers of split extensions in which the normal subgroup is a cyclic p-group, a special case of semi-direct product of an abelian p-group by a cyclic p-group and the metacyclic p-groups cannot be realised as essential p-subgroups.

One of the results of this theory is that a finite group G doesn't contain essential p-subgroups if and only if $F_p(G) = F_p(N_G(P))$ where P is a Sylow p-subgroup of G. Knowing that there are few essential p-subgroups, we can wonder if there are p-groups P, such that, for any realisation of P as a Sylow p-subgroup of a finite group G, we have $F_p(G) = F_p(N_G(P))$. We call such a group *resistant*. Burnside had already remarked that the abelian groups have this property. In chapter 3 we present others examples of resistant groups. The main result of this work is that the generalized extraspecial p-groups are resistants. For p odd, we also give another proof of the fact, showed by Glaubermann and Dietz, that the metacyclic p-groups are resistants.

A category over a p-group P is a category whose objects are the subgroups of P and whose morphisms are injective group morphisms. In the '90's, Puig built a system of axioms on this type of category, with the aim of generalizing $F_p(G)$. If a category over P satisfies this system of axioms, we call this category a full Frobenius system over P. Chapter 4 is devoted to the description of the full Frobenius systems and to the generalization to this new field of results from the chapters before. We define the notion of resistant p-group in the full Frobenius systems and we prove that the p-groups in the families of Chapter 3 remain resistant in the full Frobenius systems.

Introduction

Qui dit algèbre, dit classification et qui dit groupes finis, dit la classification des groupes finis simples. La compréhension des groupes finis simples a occupé et occupe toujours l'esprit de beaucoup d'algébristes. Leur classification a été achevée au début des années '80, mais D. Gorenstein, un des grands artisans de la preuve, a immédiatement reconnu la nécessité d'un projet de 'révision'. Celle-ci s'avère, en effet, nécessaire car la preuve existante de la classification s'étend sur dix à quinze mille pages de journal, partagées entre quelques 500 articles tous écrits entre 1950 et le début des années '80. Les révisionnistes, dans le rang desquels on compte aujourd'hui R. Lyons et R. Solomon, avec une vision globale de la classification, qui permet d'aborder différemment certains points clef de la démarche mathématique, espèrent obtenir une réduction du nombre de pages nécessaires pour la preuve à trois-quatre mille. En même temps, ils sont convaincus qu'une preuve substantiellement plus courte ne peut être obtenue qu'avec des méthodes radicalement nouvelles.

Dans le travail qui suit, on ne part pas à la recherche de méthodes nouvelles. On se contente d'approfondir certains aspects d'une des anciennes méthodes, qui est l'étude de la structure p-locale d'un groupe fini G, où p est un nombre premier qui divise l'ordre de G, c'est-à-dire l'étude des normalisateurs dans G des p-sous-groupes de G. Notons $O_{p'}(G)$ le plus grand sous-groupe normal de G d'ordre premier à p. On peut démontrer que les structures p-locales de G et $G/O_{p'}(G)$ sont isomorphes. Donc, la maîtrise de la structure p-locale de G fournit, tout au plus, la connaissance de $G/O_{p'}(G)$. Le théorème suivant, dû à Frobenius, montre qu'en partant de la structure p-locale, on peut avoir des informations précises sur $G/O_{p'}(G)$.

Théorème (Frobenius) *Soit G un groupe fini. Supposons que, pour tout p-sous-groupe P de G, le groupe $N_G(P)/C_G(P)$ est un p-groupe. Alors $G/O_{p'}(G)$ est un p-groupe.*

Pour l'étude p-locale de G on organise les p-sous-groupes non-triviaux en une catégorie, appelée, au vu du théorème précédent, la catégorie de Frobenius. Cette catégorie, notée $F_p(G)$ aura donc comme objets les p-sous-groupes de G et comme morphismes, les morphismes de groupes donnés par les conjugaisons par les éléments de G. On appelle ces morphismes des p-fusions. La question du rapport entre la connaissance de $F_p(G)$ et $G/O_{p'}(G)$ sera étudiée avec plus de détails dans le premier chapitre.

Un important pas en avant est fait par Alperin en 1967, dans [Al], quand il démontre que les morphismes dans la sous-catégorie pleine de $F_p(G)$ au-dessous d'un p-sous-groupe de Sylow P de G, peuvent être décrits uniquement à l'aide des normalisateurs des p-sous-groupes de P choisis dans une certaine famille. On rappelle que la sous-catégorie pleine de $F_p(G)$ au-dessous de P, notée $F_p(G)_{\leq P}$, est une catégorie ayant comme objets les sous-groupes non-triviaux de P

et comme morphismes, tous les morphismes de $F_p(G)$ entre ces objets. Alperin a démontré que la famille dont on parlait précédemment, des sous-groupes de P, peut être réduite aux intersections de P avec les p-sous-groupes de Sylow de G.

Neuf ans plus tard, dans son travail de doctorat [Pu1], Puig raffine ce résultat en restreignant la famille mentionnée plus haut à P et aux p-sous-groupes essentiels de G contenus dans P. La définition et les propriétés des p-sous-groupes essentiels font l'objet du deuxième chapitre. Dans ce même chapitre on discute les conséquences du théorème d'Alperin, dans sa version donnée par Puig. A la fin du chapitre on trouve des familles de p-groupes qui, grâce à leur structure, ne peuvent jamais être réalisés comme p-sous-groupes essentiels dans un groupe fini G.

Une des conséquences du théorème d'Alperin est le fait que, si G ne contient pas de p-sous-groupes essentiels, alors toutes les fusions dans $F_p(G)_{\leq P}$ peuvent être données par la conjugaison par des éléments du normalisateur $N_G(P)$. On dit alors que $N_G(P)$ contrôle la p-fusion dans G. Si P a cette propriété quel que soit le groupe fini G ayant P comme p-sous-groupe de Sylow, on dit que P est résistant. Bien avant le théorème d'Alperin, ce phénomène a été observé par Burnside dans le cas où P est un p-groupe abélien. Donc les groupes abéliens sont la première classe de p-groupes résistants.

Dans la littérature, il y a une notion cohomologique équivalente à celle de p-groupe résistant ; c'est la notion de p-groupe de Swan. Un p-groupe P est appelé de Swan si, pour toute réalisation de P comme p-sous-groupe de Sylow dans un groupe fini G, la restriction en cohomologie induit un isomorphisme entre les anneaux $H^*(G, \mathbf{F}_p)$ et $H^*(N_G(P), \mathbf{F}_p)$ de cohomologie modulo p. En 1990, Mislin a démontré que l'isomorphisme en cohomologie entre $H^*(G, \mathbf{F}_p)$ et $H^*(N_G(P), \mathbf{F}_p)$ est équivalent au contrôle de la p-fusion par $N_G(P)$ dans G. Une conséquence de ce résultat est l'équivalence des notions de p-groupe résistant et p-groupe de Swan.

En utilisant des méthodes cohomologiques, Green et Minh [GM] et Martino et Priddy [MP] ont démontré que la plupart des p-groupes extraspéciaux et, respectivement, pour p impair, les p-groupes métacycliques, sont de Swan. Dans le chapitre 3 de ce travail on va généraliser le résultat sur les p-groupes extraspéciaux et on va donner une nouvelle preuve de celui sur les p-groupes métacycliques, en évitant les méthodes cohomologiques.

Un autre outil de grande importance dans l'étude de la structure d'un groupe fini est la théorie de la représentation, qui consiste à regarder des quotients d'un groupe G comme des groupes de matrices inversibles, à coefficients dans un corps k. Pour toutes les informations liées à la structure p-locale, le plus approprié c'est de travailler sur un corps de caractéristique p. Le précurseur de cette approche est R. Brauer dans les années '40. Par ces nouvelles méthodes, Brauer a démontré des résultats profonds de la théorie des groupes.

La donnée d'une représentation (irréductible) de G sur un corps k est équivalente à la donnée d'un module (simple) sur l'algèbre de groupe kG. On rappelle que kG est un espace vectoriel sur k de base G, avec en plus la multiplication définie par la multiplication dans G. L'algèbre kG peut être décomposée en produit direct d'algèbres indécomposables $kG \simeq \prod_{j=1}^{n} B_j$, uniques à isomorphisme d'algèbres près. A chaque B_j correspond un idempotent b_j du centre $Z(kG)$, tel que b_j se projette sur 1 dans B_j et sur zéro dans les autres facteurs. Autrement dit, on a une décomposition orthogonale $1 = \sum_{j=1}^{n} b_j$. De plus, l'algèbre B_j est isomorphe à l'algèbre kGb_j. On dit que kGb_j est une algèbre de bloc et b_j est un idempotent de bloc, ou tout simplement un bloc. Les blocs sont très importants, car toute la théorie de la représentation sur k se décompose naturellement sur les algèbres de bloc.

Il peut arriver qu'une algèbre de bloc kGb est isomorphe à une algèbre de matrices. Dans ce cas on dit que b est un bloc de défaut zéro. Si p ne divise pas l'ordre de G, alors tous les blocs sont de cette forme. Mais, quand p divise l'ordre de G, on a besoin de considérer des blocs avec des degrés de complexité plus élevés. Le premier invariant qui mesure cette complexité est le groupe de défaut du bloc. C'est un p-sous-groupe de G, unique à conjugaison près, dont la définition sera donnée dans le chapitre 4. Le groupe de défaut d'un bloc est trivial si et seulement si le bloc est de défaut zéro. A l'autre extrémité se situe le cas où le groupe de défaut d'un bloc b est un p-sous-groupe de Sylow de G. Soit b_0 l'unique bloc qui contient la représentation triviale de dimension 1. Dans ce cas le groupe de défaut de b_0 est un p-sous-groupe de Sylow de G. On appelle b_0 le bloc principal de kG.

Si Q est un p-sous-groupe de G, on note $(kG)^Q$ l'ensemble d'éléments de kG fixes par l'action de Q et on constuit le morphisme surjectif d'algèbres $br_Q : (kG)^Q \longrightarrow kC_G(Q)$, qui envoie $C_G(Q)$ sur lui-même par l'identité et toutes le autres éléments de la base sur zéro. On appelle ce morphisme le morphisme de Brauer. Comme $br_Q(1) = 1$, les blocs de G vont donner une partition des blocs de $kC_G(Q)$. Un bloc e de $kC_G(Q)$ sera associé à un bloc b de kG si e apparaît dans la décomposition de $\mathrm{br}_Q(b)$ dans $kC_G(Q)$.

Soit b un bloc de G. Une paire de Brauer, associée à b, est une paire (Q, e), où Q est un p-sous-groupe de G et e est un bloc de $kC_G(Q)$ associé à b. L'utilisation des telles paires a commencé avec Brauer (dans un cas particulier) et a été introduite systématiquement par J. L. Alperin et M. Broué à la fin des années '70. Ils ont défini une relation d'ordre partiel sur l'ensemble des paires de Brauer et ont obtenu un poset (ensemble partiellement ordonné). Leur idée était de voir les paires de Brauer comme une généralisation des p-sous-groupes. Entre autres ils ont remarqué que le poset des paires de Brauer associées au bloc principal est isomorphe (comme ensemble ordonné) au poset des p-sous-groupes de G. Les éléments maximaux du poset des paires de Brauer sont conjugués dans G (leurs première composantes sont les groupes de défaut de b) et jouent le rôle des p-sous-groupes de Sylow. Ce travail d'Alperin et Broué a jeté les fondations de la théorie p-locale des blocs.

Le poset des paires de Brauer associées à un bloc b de kG ensemble avec les morphismes induits par la conjugaison par les éléments de G forment une catégorie, qu'on appelle la catégorie de Brauer associée au bloc b. Cette catégorie est une généralisation de la catégorie de Frobenius, car la catégorie de Brauer associée au bloc principal est équivalente à la catégorie de Frobenius de G. Dans un article récent, [Pu2], Puig pousse la généralisation de la catégorie de Frobenius encore plus loin, en introduisant les systèmes complets de Frobenius sur un p-groupe P. La définition et les propriétés des systèmes complets de Frobenius sont discutés dans le chapitre 4. On y explique aussi que la sous-catégorie pleine au-dessous d'une paire maximale (définie d'une manière analogue à la sous-catégorie pleine de $F_p(G)$ au-dessous d'un p-sous-groupe de Sylow), de la catégorie de Brauer associée à un bloc b, est un système complet de Frobenius.

La fin du chapitre 4 est consacrée à la généralisation, aux systèmes complets de Frobenius, des notions et de résultats du chapitre 3. Dans un système complet de Frobenius, $\mathcal{F}$, sur un p-groupe P, on peut définir, par analogie avec les p-groupes, les notions de fusion et de sous-groupe essentiel. L'équivalent du théorème d'Alperin, pour les p-groupes, reste vrai dans le cadre des systèmes complets de Frobenius. On prouve, entre autres, une généralisation d'un théorème de Gilotti et Serena sur des conditions équivalentes pour le contrôle de fusion par le normalisateur d'un sous-groupe de P. On généralise la notion de p-groupe résistant et on démontre que les p-groupes appartenant aux deux familles du chapitre 4 sont aussi résistants dans le cadre des systèmes de Frobenius.

Dans ce travail on donne des exemples de familles de p-groupes qui ne peuvent jamais être réalisés comme des p-sous-groupes essentiels et des familles de p-sous-groupes résistants et on expose des méthodes pour aborder les problèmes qui sont reliés à l'étude de ces groupes. Le rêve serait de classifier à isomorphisme près tous les p-groupes qui ont ces propriétés. D'autre part, toutes les méthodes qu'on a utilisées pour la catégorie de Frobenius ont pu être appliquées, avec des petites modifications, aux systèmes complets de Frobenius. Une question naturelle s'impose : est-ce qu'il y a un p-groupe P qui est résistant dans le cadre de la catégorie de Frobenius et ne l'est pas dans le cadre des systèmes complets de Frobenius ?

Des rêves que j'aimerais matérialiser, des questions auxquelles j'aimerais répondre au plus vite.

Chapitre 1

La catégorie de Frobenius

Soit p un nombre premier. On débute le chapitre par la présentation des propriétés générales des p-groupes. On va introduire ensuite la notion de catégorie de Frobenius d'un groupe fini, associée à p et celle de contrôle de la p-fusion. On démontre que les sous-groupes normaux, d'ordre premier à p, ne jouent aucun rôle dans la catégorie de Frobenius. De plus, on a une équivalence de catégories entre la catégorie de Frobenius d'un groupe et la sous-catégorie pleine au-dessous d'un p-sous-groupe de Sylow. Le rêve serait de montrer que, si un sous-groupe H contrôle la p-fusion dans un groupe fini G, alors $G \simeq H\mathrm{O}_{p'}(G)$. Ceci n'est pas vrai en général, mais vrai si G est p-résoluble. Si, de plus, G est p-nilpotent alors un p-sous-groupe de Sylow de G contrôle la p-fusion dans G.

1.1 Généralités sur les p-groupes

Soit G un groupe fini. Fixons quelques notations.

Notation 1.1.1 Soient Q, R deux sous-groupes de G et $g, h \in G$. On note $Q \leq R$ ou $R \geq Q$ le fait que Q est un sous-groupe de R. Si les inégalités sont strictes, ça signifie que Q est un sous-groupe propre de P. Posons ${}^{g}h := ghg^{-1}$, le conjugué de h par g et $[g,h] := ghg^{-1}h^{-1}$, le commutateur de g et h. Par ailleurs, ${}^{g}R$ désigne $gRg^{-1} = \{gug^{-1} | u \in R\}$ et $[Q,R]$ désigne $QRQ^{-1}R^{-1} = \{vuv^{-1}u^{-1} | v \in Q, u \in R\}$. On note $R \xrightarrow{g} Q$ le morphisme de R dans Q induit par la conjugaison par g, c'est-à-dire $x \mapsto {}^{g}x$, étant sous-entendu que ${}^{g}R \leq Q$. Une autre notation équivalente est $\mathrm{conj}(g) : R \longrightarrow Q$.

Par l'ensemble $N_G(R) := \{g \in G \,|\, {}^{g}R = R\}$ on désigne le normalisateur de R dans G et par l'ensemble $C_G(R) := \{g \in G \,|\, {}^{g}u = u, \forall u \in R\}$ on désigne le centralisateur de R dans G. Ces deux ensembles sont des sous-groupes de G.

Le symbole 1 désigne l'élément neutre du groupe.

Un outil important dans l'étude des groupes finis est l'action d'un groupe sur un ensemble. On dit que G agit sur un ensemble X si on a une application de $G \times X$ dans X qu'on note $(g,x) \mapsto g * x$ et qui satisfait $g * (h * x) = (gh) * x$ et $1 * x = x$.

L'ensemble $Gx := \{g * x | g \in G\}$ s'appelle l'orbite de x. L'ensemble X est partitioné en orbites sous l'action de G. La cardinalité de l'orbite Gx est donnée par $|G : G_x|$ où le groupe $G_x := \{g \in G | g * x = x\}$ est le stabilisateur de x dans G. Si on note par $\{O_i,\, i \in I\}$ l'ensemble d'orbites de X dans G et par $\mathrm{Fix}(X)$ l'ensemble des éléments de X fixes par l'action de G, on a

$$X = \bigsqcup_{i \in I} O_i = \mathrm{Fix}(X) \bigsqcup (\bigsqcup_{\substack{i \in I \\ |O_i| \neq 1}} O_i) \, .$$

Cette partition de X est d'une grande utilité car le nombre d'éléments dans les orbites non-triviales de X sont des diviseurs non-triviaux de l'ordre de G. On obtient ainsi des informations sur la taille de $\mathrm{Fix}(X)$.

Soit maintenant p un nombre premier. Un p-groupe est un groupe fini d'ordre une puissance de p.

Définition 1.1.2 *Un p-sous-groupe de G est un sous-groupe de G, qui est un p-groupe. Un p-sous-groupe de Sylow de G est un p-sous-groupe P de G tel que l'indice $|G : P|$ est premier à p.*

Suite à cette définition, encore quelques notations.

Notation 1.1.3 On désigne par p'-groupe, respectivement p'-élément, un groupe, respectivement un élément, d'ordre premier à p. On note $\mathrm{O}_{p'}(G)$ le plus grand p'-sous-groupe normal de G et par $\mathrm{O}_p(G)$ le plus grand p-sous-groupe normal de G.

La pierre de base de toute construction sur le p-sous-groupes d'un groupe fini est constituée par les théorèmes de Sylow. Ce sont des théorèmes fondamentaux de la théorie des groupes finis.

Théorème 1.1.4 (Sylow) *Soit G un groupe fini et p un nombre premier. Alors*

a) G possède un p-sous-groupe de Sylow.

b) Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.

c) Deux p-sous-groupes de Sylow de G sont conjugués entre eux par un élément de G.

d) Soit n_p le nombre des p-sous-groupes de Sylow de G et P un p-sous-groupe de Sylow de G. On a $n_p = |G : N_G(P)| \equiv 1 \pmod p$.

Pour la preuve de ce théorème voir par exemple Curtis et Reiner [CR, §6] ou Suzuki [Su, Thm. 2.2.2]. D'autres résultats sur la structure d'un p-groupe sont donnés dans l'énoncé suivant.

Proposition 1.1.5 *Soit P un p-groupe. On a les propriétés suivantes :*

a) Le centre $Z(P)$ n'est pas trivial.

b) Si $Q < P$, alors $Q < N_P(Q)$.

c) Tout sous-groupe propre maximal de P est d'indice p dans P.

d) Tout groupe d'ordre p^2 est abélien.

La preuve est classique et peut être trouvée dans Suzuki [Su, Thm. 2.1.4, Thm. 2.1.6]. Elle se base sur l'action de P sur des ensembles. Par exemple, pour a), on fait agit P sur lui-même, par conjugaison. On en déduit que p divise l'ordre de $Z(P)$; mais $Z(P)$ contient toujours 1, donc $|Z(P)| \geq p$.

Remarque 1.1.6 Par le point b) plus haut, pour qu'un p-sous-groupe P d'un groupe fini G soit un p-sous-groupe de Sylow de G, il suffit que P soit un p-sous-groupe de Sylow de son normalisateur $N_G(P)$. En effet, soit S un p-sous-groupe de Sylow de G, qui contient P. On a $N_S(P) \leq N_G(P)$, donc $N_S(P) = P$, car P est un p-sous-groupe de Sylow de $N_G(P)$. Par le point b) de la proposition antérieure, on a $P = S$.

Une autre propriété immédiate des p-groupes est la suivante.

Proposition 1.1.7 *Soit P un p-groupe et Q un sous-groupe normal, non-trivial de P. Alors $Q \cap Z(P)$ est un p-groupe non-trivial.*

Preuve. On fait agir P sur Q par conjugaison. Les points fixes par l'action de P sont exactement $Q \cap Z(P)$. Comme 1 est toujours un point fixe, on déduit que $|Q \cap Z(P)| \geq p$, donc $Q \cap Z(P)$ n'est pas trivial. □

Définition 1.1.8 *Soit G un groupe. Une série normale de G est une suite des sous-groupes de G emboîtés les uns dans les autres $G = G_n \geq \ldots \geq G_1 \geq G_0 = 1$, tels que, pour tout $1 \leq i \leq n$, G_{i-1} est un sous-groupe normal de G_i.*

On est maintenant en mesure d'énoncer une propriété des p-groupes, qui sera très utile par la suite. On désigne par $\mathrm{Aut}(P)$ le groupe d'automorphismes de P.

Proposition 1.1.9 *Soient P un p-groupe et A un sous-groupe de $\mathrm{Aut}(P)$ qui centralise les quotients d'une série normale de P. Alors A est un p-groupe.*

Pour la preuve on renvoie à Gorenstein [Gr, Cor. 5.3.3]. L'intérêt de l'étude des p-groupes réside dans le fait qu'on peut obtenir de l'information sur un groupe fini, à partir de ses p-sous-groupes de Sylow, si p divise l'ordre de G. Le théorème suivant, dû à Frobenius, en est la preuve.

Théorème 1.1.10 *Soit G un groupe fini. Supposons que, pour tout p-sous-groupe P de G, le groupe $N_G(P)/C_G(P)$ est un p-groupe. Alors $G/O_{p'}(G)$ est un p-groupe.*

Pour la preuve de ce théorème on a besoin d'outils plus puissants, comme le théorème d'Alperin, qui sera presenté dans le chapitre 2 ; voir [Gr, Thm. 7.4.5] pour la preuve détaillée. Les groupes $N_G(P)/C_G(P)$ sont appelés des *sous-groupes p-locaux* de G. Leur étude fera l'objet de la section suivante.

1.2 La structure p-locale d'un groupe fini

Pour étudier les sous-groupes p-locaux d'un groupe fini G, on organise les p-sous-groupes de G dans une catégorie, qu'on appelle la catégorie de Frobenius.

Définition 1.2.1 *Soit G un groupe fini et p un nombre premier. La catégorie de Frobenius de G, notée $F_p(G)$, est la catégorie qui a comme objets les p-sous-groupes de G et dont les morphismes sont les homomorphismes de groupe induits par la conjugaison par les éléments de G.*

Remarque 1.2.2 On a bien sûr $(R \xrightarrow{g} Q) = (R \xrightarrow{h} Q)$ si et seulement si $h^{-1}g \in C_G(R)$. Par conséquent,

$$\mathrm{Hom}_{F_p(G)}(R, Q) = \{g \in G \mid {}^gR \leq Q\}/C_G(R)\,.$$

Soit P un p-sous-groupe de Sylow de G. On dit que deux sous-groupes de P p-fusionnent dans G s'ils sont conjugués par un élément de G. Le long de ce travail on va s'intéresser aux phénomènes de p-fusion dans G et, surtout, au problème du contrôle de la p-fusion dans G, c'est à dire trouver un sous-groupe H de G qui réalise par conjugaison à l'intérieur de H toutes les p-fusions données par G. Dans ce qui suit on analyse plus en détail cette notion.

Premièrement on va voir que les sous-groupes normaux de G, d'ordre premier à p, ne jouent aucun rôle au niveau de $F_p(G)$.

Proposition 1.2.3 *Soit $N := \mathrm{O}_{p'}(G)$ et soit $f : G \longrightarrow \overline{G} := G/N$ l'application quotient. Alors f induit une équivalence de catégories entre $F_p(G)$ et $F_p(\overline{G})$. Réciproquement, si $f : G \longrightarrow H$ induit une équivalence de catégories entre $F_p(G)$ et $F_p(H)$, alors $\mathrm{Ker}(f)$ est un p'-groupe.*

Pour la démonstration de cette proposition on aura besoin du résultat technique suivant.

Lemme 1.2.4 *Avec les notations de la proposition 1.2.3, soit $Q \in F_p(G)$ et $\overline{Q}$ son image dans $\overline{G} := G/N$. Alors $C_G(Q)$ se surjecte sur $C_{\overline{G}}(\overline{Q})$. Plus précisément, tout élément de $C_{\overline{G}}(\overline{Q})$ se relève dans un élément de $N_G(Q)$ et*

$$C_G(Q) = f^{-1}(C_{\overline{G}}(\overline{Q})) \cap N_G(Q)\,.$$

Preuve. L'inclusion du membre du gauche dans celui de droite est triviale. Pour l'inclusion dans l'autre sens on travaille dans $N_G(Q)$. Comme Q y est normal, Q et $N_G(Q) \cap N$ se normalisent réciproquement. De plus, $Q \cap (N_G(Q) \cap N) = \{1\}$, donc, pour tous $u \in Q$ et $n \in N$, on a $[n, u] = 1$, car ce commutateur appartient en même temps à Q et à $N_G(Q) \cap N$. Soit maintenant $g \in f^{-1}(C_{\overline{G}}(\overline{Q})) \cap N_G(Q)$. Alors $f(gug^{-1}) = f(u)$, pour tout $u \in Q$, ce qui entraîne $gug^{-1} = uz$ pour un $z \in N$. En fait, on a aussi $z \in N_G(Q)$ car $[g, u] \in N_G(Q)$. Donc $z \in N_G(Q) \cap N$. Soit p^n, $n \in \mathbf{Z}_{\geq 0}$ l'ordre de u. Alors $1 = (gug^{-1})^{p^n} = (uz)^{p^n} = u^{p^n} z^{p^n}$. Pour la dernière égalité on utilise le fait que $u \in Q$ et $z \in N_G(Q) \cap N$ commutent. Ainsi $z = 1$ car il est en même temps d'ordre une puissance de p et d'ordre premier à p et donc $g \in C_G(Q)$. Il reste à voir que tout élément de $C_{\overline{G}}(\overline{Q})$ se relève en un élément de $N_G(Q)$. Soit $\overline{g} \in C_{\overline{G}}(\overline{Q})$ et soit $g \in G$ un de ses relevés. Les groupes Q et ${}^gQ$ sont des p-sous-groupes de Sylow de NQ, donc ils sont conjugués par un élément $nq \in NQ$. Ceci entraîne que $n^{-1}g \in N_G(Q)$, qui est aussi un relevé de $\overline{g}$. □

Revenons maintenant à notre proposition. On rappelle que deux catégories $\mathcal{A}$ et $\mathcal{B}$ sont *équivalentes* s'il existe un foncteur $F : \mathcal{A} \longrightarrow \mathcal{B}$ tel que
a) pour tout objet $B \in \mathcal{B}$ il existe on objet $A \in \mathcal{A}$, tel que $F(A)$ est isomorphe à B ;
b) F est plein, c'est-à-dire pour tout morphisme $h : B' \longrightarrow B''$ dans $\mathcal{B}$ il existe un morphisme $g : A' \longrightarrow A''$ dans $\mathcal{A}$, tel que $F(g) = h$;
c) F est fidèle, c'est-à-dire pour tous morphismes $g_1, g_2 : A \longrightarrow A$ dans $\mathcal{A}$, si $F(g_1) = F(g_2)$ alors $g_1 = g_2$;.

Preuve de Proposition 1.2.3. Pour montrer l'équivalence il suffit de montrer que le foncteur $f : F_p(G) \longrightarrow F_p(\overline{G})$ est surjectif, plein et fidèle.
a) Le fait que f est surjectif sur les objets est immédiat. En effet, soit R un p-sous-groupe de $\overline{G}$ et posons $\widetilde{R} := f^{-1}(R)$. Alors $\widetilde{R} = NQ$ pour tout choix de Q comme p-sous-groupe de Sylow de $\widetilde{R}$. De plus $R = \widetilde{R}/N = \overline{Q}$. Autrement dit, on a $f(Q) = R$.
b) Soit $\overline{R} \xrightarrow{\overline{g}} \overline{Q}$ un morphisme dans $F_p(\overline{G})$. Soient R, Q et g des relevés respectivement de $\overline{R}$, $\overline{Q}$ et $\overline{g}$. Par la partie a) on peut choisir R et Q pour qu'ils soient des p-sous-groupes de G. On a $\overline{{}^gR} \leq \overline{Q}$ et donc ${}^gR \leq NQ$. Comme Q est un p-sous-groupe de Sylow de NQ, ${}^gR$ est contenu dans un conjugué de Q dans NQ. Donc il existent $n \in N$ et $q \in Q$ tels que ${}^gR \leq {}^{nq}Q$. Ainsi ${}^{n^{-1}g}R \leq Q$ et $R \xrightarrow{n^{-1}g} Q$ est un morphisme de $F_p(G)$. Par ailleurs, l'image par f de $R \xrightarrow{n^{-1}g} Q$ dans $F_p(\overline{G})$ est $\overline{R} \xrightarrow{\overline{g}} \overline{Q}$, car $\overline{n^{-1}g} = \overline{g}$. Ceci prouve la plénitude de f.
c) Soient $R \xrightarrow{x} Q$ et $R \xrightarrow{y} Q$ ayant la même image par f, c'est-à-dire $\overline{x} = \overline{yc}$ où $\overline{c} \in C_{\overline{G}}(\overline{R})$. On a $\overline{{}^xR} = \overline{{}^yR}$, ce qui est équivalent à $N\,{}^xR = N\,{}^yR$. Comme $NQ/N \simeq Q$, on peut considérer la projection $\pi : NQ \longrightarrow Q$. On a alors $\pi^{-1}({}^xR) = \pi^{-1}({}^yR)$ ce qui implique ${}^xR = {}^yR$, ou, autrement dit, $xy^{-1} \in N_G(R)$. Donc $xy^{-1} \in f^{-1}(C_{\overline{G}}(\overline{R})) \cap N_G(R)$. Comme, par Lemme 1.2.4, on a $f^{-1}(C_{\overline{G}}(\overline{R})) \cap N_G(R) = C_G(R)$, il s'ensuit que f est fidèle.

Pour la réciproque, soit $f : G \longrightarrow H$ induisant une équivalence entre $F_p(G)$ et $F_p(H)$. Considérons un p-sous-groupe de Sylow, S, de $\mathrm{Ker}(f)$. Alors S et 1 deviennent isomorphes dans $F_p(H)$, donc S et 1 sont isomorphes dans G, ce qui entraîne $S = 1$. On en déduit que $\mathrm{Ker}(f)$ est un p'-groupe. □

Remarque 1.2.5 Soit H un sous-groupe de G. Pour dire si $F_p(G)$ et $F_p(H)$ sont équivalentes, il suffit, par cette proposition, de regarder les injections $f : H \longrightarrow G$.

Définition 1.2.6 *Soit H un sous-groupe de G. On dit que H contrôle la p-fusion, ou que H est un sous-groupe de p-contrôle, si l'inclusion $H \longrightarrow G$ induit une équivalence de catégories entre $F_p(H)$ et $F_p(G)$.*

Le contrôle de la p-fusion par un sous-groupe H de G est équivalent au fait que H contient un p-sous-groupe de Sylow de G et que tout morphisme par conjugaison par un élément de G entre des p-sous-groupes de H peut être donné par la conjugaison par un élément de H. Plus précisement, on a le lemme suivant.

Lemme 1.2.7 *Soit H un sous-groupe de G. Alors H contrôle la p-fusion, si et seulement si les deux conditions suivantes sont satisfaites :*
i) $p \nmid |G : H|$;
ii) pour tout p-sous-groupe R de H et tout $g \in G$, tel que ${}^gR \leq H$, on a $g = hc$ avec $h \in H$ et $c \in C_G(R)$.

Preuve.
a) Soit $R \in F_p(G)$. L'existence d'un p-sous-groupe Q de H, tel que R est isomorphe à Q, est équivalente à l'existence d'un conjugué R' de R dans H. Ceci est vrai pour tout R si et seulement si H contient un p-sous-groupe de Sylow de G, ce qui est équivalent à $p \nmid |G : H|$.
b) Les morphismes dans $F_p(H)$ sont des conjugaisons par des éléments de H donc ils sont envoyés injectivement sur des morphismes dans $F_p(G)$. Donc $f : F_p(G) \longrightarrow F_p(H)$ est toujours fidèle.
c) Par définition, f est plein si $\mathrm{Hom}_H(R, Q) = \mathrm{Hom}_G(R, Q)$, pour tous $R, Q \in F_p(H)$. En 'traduisant' ceci en langage des conjugaisons, si ${}^gR \leq Q$, il existe un élément h de H tel que $\mathrm{conj}(g) = \mathrm{conj}(h)$. C'est la même chose que de demander que, si R et ${}^gR$ sont des p-sous-groupes de H, alors $gC_G(R) = hC_G(R)$ ou, autrement dit, qu'il existe $c \in C_G(R)$ tel que $g = hc$. □

Exemple 1.2.8 Voici deux exemples de contrôle de fusion.
1) (Burnside) Si un p-sous-groupe de Sylow P de G est abélien, alors $N_G(P)$ contrôle la p-fusion dans G.

Preuve. On utilise les conditions équivalentes de Lemme 1.2.7.

a) Evidemment, p ne divise pas $|G : N_G(P)|$.

b) Soient Q un p-sous-groupe de $N_G(P)$ et $g \in G$ tels que ${}^gQ \leq N_G(P)$. Comme P est normal dans $N_G(P)$, il est l'unique p-sous-groupe de Sylow de $N_G(P)$ et donc $Q, {}^gQ \leq P$. De plus P est abélien et, comme $Q \leq {}^{g^{-1}}P$, on a $P, {}^{g^{-1}}P \leq C_G(Q)$. Maintenant P et ${}^{g^{-1}}P$ sont des p-sous-groupes de Sylow de $C_G(Q)$, donc ils sont conjugués par un élément c de $C_G(Q)$. Autrement dit, ${}^cP = {}^{g^{-1}}P$ ce qui implique qu'il existe $h \in N_G(P)$, tel que $gc = h$. Ceci nous donne $g = hc^{-1}$, avec $h \in N_G(P)$ et $c \in C_G(Q)$. Par le lemme 1.2.7, $N_G(P)$ contrôle la p-fusion dans G. □

2) Si $p \nmid n$ alors S_{n-1} contrôle la p-fusion dans S_n.

Preuve. On utilise de nouveau le Lemme 1.2.7. On fixe $S_{n-1} := \{\gamma \in S_n | \gamma(1) = 1\}$.

a) Comme $|S_n : S_{n-1}| = n$, on a par l'hypothèse que $p \nmid |S_n : S_{n-1}|$.

b) Soient $Q \leq S_{n-1}$ et $\sigma \in S_n$ tels que ${}^\sigma Q \leq S_{n-1}$. On construit explicitement une permutation $\tau \in S_{n-1}$ telle que ${}^\tau\beta = {}^\sigma\beta$, pour tout $\beta \in Q$. Posons

$$\begin{aligned} \tau(1) &:= 1\,, \\ \tau(\sigma^{-1}(1)) &:= \sigma(1) \text{ et} \\ \tau(i) &:= \sigma(i) \text{ pour } i \neq 1, \sigma^{-1}(1)\,. \end{aligned}$$

Clairement, $\tau \in S_{n-1}$ car $\tau(1) = 1$. Vérifions que ${}^\tau\beta = {}^\sigma\beta$, pour tout $\beta \in Q$. Soit $\beta \in Q$.

$$\begin{aligned} \tau\beta\tau^{-1}(1) = 1 \text{ car } \beta \in Q \leq S_{n-1} &\qquad \text{et} \qquad \sigma\beta\sigma^{-1}(1) = 1 \text{ car } {}^\sigma\beta \in {}^\sigma Q \leq S_{n-1}\,; \\ \tau\beta\tau^{-1}(\sigma(1)) = \tau\beta\sigma^{-1}(1) = \tau\sigma^{-1}(1) = \sigma(1) &\qquad \text{et} \qquad \sigma\beta\sigma^{-1}\sigma(1) = \sigma\beta(1) = \sigma(1)\,; \end{aligned}$$

pour $i \neq 1, \sigma(1)$ on a $\tau^{-1}(i) = \sigma^{-1}(i)$ donc $\beta\tau^{-1}(i) = \beta\sigma^{-1}(i) \neq 1, \sigma^{-1}(1)$ ce qui entraîne

$$\tau\beta\tau^{-1}(i) = \sigma\beta\sigma^{-1}(i)\,.$$

Donc ${}^{\tau}\beta = {}^{\sigma}\beta$. Il s'ensuit que $\sigma = \tau\chi$ avec $\chi \in C_{S_n}(Q)$.

Par le lemme 1.2.7, S_{n-1} contrôle la p-fusion dans S_n. □

Définition 1.2.9 *Soit A un sous-groupe normal de G. On dit que A admet un complément dans G s'il existe un sous-groupe K de G tel que $AK = G$ et $A \cap K = \{1\}$.*

Si A admet un complément K dans G alors G est un produit semi-direct de A par K. Le théorème suivant nous donne des conditions suffisantes pour qu'un sous-groupe normal de G admette un complément dans G.

Théorème 1.2.10 (Schur-Zassenhaus) *Soit A un sous-groupe normal de G et supposons que $|A|$ et $|G/A|$ sont deux nombres premiers entre eux. Alors A admet un complément dans G.*

Preuve. [Gr, Thm 6.2.1]

1.3 Groupes p-résolubles et p-nilpotents

En fait, pour l'étude de la catégorie de Frobenius d'un groupe fini, il suffit de se restreindre à la sous-catégorie pleine au-dessous d'un p-sous-groupe de Sylow, comme le montre le résultat suivant. Rappelons qu'une *sous-catégorie pleine* d'une catégorie $\mathcal{F}$ est une catégorie $\mathcal{F}'$ dont les objets sont un sous-ensemble de l'ensemble d'objets de $\mathcal{F}$ et dont les morphismes entre deux objets A et B de $\mathcal{F}'$ sont tous les morphismes entre A et B dans $\mathcal{F}$.

Proposition 1.3.1 *Soient P un p-sous-groupe de Sylow de G et $F_p(G)_{\leq P}$ la sous-catégorie pleine de $F_p(G)$, dont les objets sont les sous-groupes de P. Alors l'inclusion $F_p(G)_{\leq P} \hookrightarrow F_p(G)$ est une équivalence de catégories.*

Preuve. Le foncteur induit par l'inclusion est plein et fidèle par définition. Soit $Q \in F_p(G)$. Comme Q est contenu dans un p-sous-groupe de Sylow de G, disons ${}^{g}P$, on a ${}^{g^{-1}}Q \leq P$. Donc P contient un objet qui est isomorphe à Q dans $F_p(G)$. □

Comme une conséquence de cette proposition on obtient qu'un sous-groupe H, de G, qui contient P, contrôle la p-fusion si et seulement si $F_p(G)_{\leq P} = F_p(H)_{\leq P}$. Le rêve serait de montrer que si H contrôle la p-fusion alors $G = H\mathrm{O}_{p'}(G)$. Dans cette généralité l'affirmation est fausse. Prenons par exemple un groupe simple G, d'ordre divisible par p et supérieur à p, ayant un p-sous-groupe de Sylow P abélien et posons $H = N_G(P)$. Comme G est simple, $\mathrm{O}_{p'}(G)$ est trivial et P n'est pas normal dans G, donc $N_G(P)$ est un sous-groupe propre de G. Maintenant $N_G(P)$ contrôle la p-fusion dans G car P est abélien, mais $N_G(P)\mathrm{O}_{p'}(G) = N_G(P) \neq G$ donc notre rêve n'est pas atteint.

Si G est un groupe *p-résoluble*, c'est-à-dire G admet une série $\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ avec les quotients des p-groupes ou p'-groupes, le rêve se réalise.

Commençons par un petit lemme sur les groupe p-résolubles.

Lemme 1.3.2 (Hall-Higman) *Soit G un groupe fini p-résoluble avec $\mathrm{O}_{p'}(G) = 1$ et posons $P := \mathrm{O}_p(G)$. Alors $C_G(P) \leq P$ (c'est-à-dire $C_G(P) = Z(P)$).*

Preuve. On note $C := C_G(P)$ et on a $P \trianglelefteq G$ et $PC \trianglelefteq G$. On veut montrer que $PC = P$. Soit N/P un sous-groupe normal minimal de G/P, contenu dans PC/P. Maintenant $\mathrm{O}_p(G/P) = 1$ donc N/P est un p'-groupe car G est p-résoluble. Comme $N = P(N \cap C)$ on a $N/P \simeq (N \cap C)/Z(P)$. Donc, par le théorème 1.2.10, on obtient que $Z(P)$ a un complément S dans $N \cap C$. Mais $S \leq C$ donc S et $Z(P)$ se centralisent. Ceci entraîne $N \cap C = S \times Z(P)$ et, par le même raisonnement, $N = P \times S$. Alors $\mathrm{O}_{p'}(N) = S$ est caractéristique dans N, donc normal dans G. Comme $\mathrm{O}_{p'}(G) = 1$, on obtient $S = 1$. On a donc $N = P$, ce qui veut dire que G/P n'a pas de sous-groupes normaux non-triviaux dans PC/P et ainsi $PC/P = 1$. $\square$

Proposition 1.3.3 *Soit G un groupe fini p-résoluble et soit H un sous-groupe de G. Supposons que H contrôle la p-fusion dans G. Alors $G = H\mathrm{O}_{p'}(G)$.*

Preuve. Comme G et $G/\mathrm{O}_{p'}(G)$ ont les mêmes catégories de Frobenius associées, on peut supposer que $\mathrm{O}_{p'}(G) = 1$. Soit $g \in G$ et on pose $Q := \mathrm{O}_p(G) \neq 1$. Par le lemme précédent on a $C_G(Q) \leq Q = {}^gQ$, car $Q \trianglelefteq G$. Ainsi $Q = {}^gQ$ est contenu dans tous les p-sous-groupes de Sylow de G, donc dans un p-sous-groupe de Sylow de H. Par le p-contrôle de fusion on a $g = hc$, avec $h \in H$ et $c \in C_G(Q) \leq Q \leq H$, donc $g \in H$. $\square$

Dans le cas où G est un groupe *p-nilpotent*, c'est-à-dire qu'un p-sous-groupe de Sylow de G admet un complément normal dans G, on peut descendre le contrôle de la p-fusion jusqu'à un p-sous-groupe de Sylow de G.

Proposition 1.3.4 *Si G est p-nilpotent, alors un p-sous-groupe de Sylow P de G contrôle la p-fusion dans G.*

Preuve. On peut donner une preuve rapide en utilisant le lemme 1.2.3. Soit $N := \mathrm{O}_{p'}(G)$ alors $G = N \rtimes P$ et en passant au quotient par N il reste P qui contrôle la p-fusion. Mais on peut aussi donner une preuve directe de la proposition, en prenant $Q, {}^gQ \leq P$. On écrit $g = un$, avec $u \in P$ et $n \in N$. Il suffit de voir que $n \in C_G(Q)$. En effet, $[n, q] \in P \cap N = 1$ car, d'une part, $qnq^{-1}, n \in N$ et, d'autre part, $nqn^{-1} \in {}^nQ \leq P$ et $q \in Q \leq P$. $\square$

La réciproque de cette proposition est aussi vraie. C'est une conséquence du théorème 1.1.10. En effet, si un p-sous-groupe de Sylow P de G contrôle la p-fusion dans G alors, pour tout p-sous-groupe Q de G, contenu dans P, tout automorphisme induit par conjugaison par un élément de G sur Q est donné par conjugaison par un élément de P. Par conséquent, on obtient que $N_G(Q)/C_G(Q) = N_P(Q)/C_P(Q)$ et ainsi $N_G(Q)/C_G(Q)$ est un p-groupe. Par le théorème 1.1.10, le groupe G est p-nilpotent.

Remarque 1.3.5 Tous les résultats de ces deux dernières sections sont bien connus. Ils ont été présentés dans un cours de troisième cycle de Jacques Thévenaz à Lausanne. Une grande partie de ces résultats se trouvent dans un article de Broué [Bru] présenté au Séminaire Chevalley en 1978.

Chapitre 2

Fusion et p-sous-groupes essentiels

Dans ce chapitre on définit la notion de p-sous-groupe essentiel, qui à été introduite par Puig en 1976 dans sa thèse de doctorat. On remarque que les phénomènes de fusion dans la catégorie de Frobenius sont de nature locale, c'est-à dire qu'ils sont controlés par les normalisateurs des p-sous-groupes de G. On énnocera le théorème d'Alperin dans une variante améliorée par Puig, qui utilise des p-sous-groupes essentiels. Ce théorème nous dit que tout morphisme par conjugaison par un élément de G, entre deux sous-groupes d'un p-sous-groupe de Sylow P de G, peut être décomposé en composition de conjugaisons par des éléments du normalisateur de P et des normalisateurs des p-sous-groupes essentiels contenus dans P.

Dans la deuxième partie du chapitre on cherche des p-groupes qui ne peuvent jamais être réalisés comme des p-sous-groupes essentiels dans un groupe fini G. Les premiers exemples de tels groupes, pour $p = 2$, sont les groupes des quaternions, les groupes diédraux et les groupes semi-diédraux. Pour p impair, on trouve une condition suffisante pour qu'un p-groupe ne puisse jamais être réalisé comme p-sous-groupe essentiel et on trouve trois familles différentes de p-groupes qui satisfont ce critère. Ce sont certaines tours d'extensions scindées dans lesquelles le sous-groupe normal est un p-groupe cyclique, un cas spécial de produit semi-direct d'un groupe abélien par un groupe cyclique et les p-groupes métacycliques non-abéliens.

2.1 Théorème de fusion d'Alperin

Dès lors, P sera un p-sous-groupe de Sylow de G. Dans cette section notre but sera de démontrer que les phénomènes de p-fusion dans P sont de nature p-locale, c'est-à-dire qu'ils peuvent être compris à partir des sous-groupes p-locaux $N_G(Q)/C_G(Q)$, où Q parcourt une certaine famille des sous-groupes de P.

Définition 2.1.1 *Soit $\mathcal{S}_p(G)$ l'ensemble des p-sous-groupes non-triviaux de G ordonné par l'inclusion. C'est un poset, c'est-à-dire un ensemble partiellement ordonné pour l'inclusion. On dit que $Q, R \in \mathcal{S}_p(G)$ sont liés s'ils existent des groupes $S_i \in \mathcal{S}_p(G)$, $i = 1, \ldots, n$ avec $Q \leq S_1 \geq S_2 \leq S_3 \geq \cdots \geq S_{n-1} \leq S_n \geq R$. Ceci définit une relation d'équivalence sur $\mathcal{S}_p(G)$. Les classes d'équivalence sont appelées les composantes connexes. On dit que $\mathcal{S}_p(G)$ est connexe s'il y a une seule composante connexe.*

On peut aussi voir $\mathcal{S}_p(G)$ comme un complexe, dont les sommets sont les p-sous-groupes non-triviaux de G et les symplexes sont les chaînes des groupes emboîtés les uns dans le autres.

Exemple 2.1.2 1) Si $O_p(G) \neq 1$ alors $\mathcal{S}_p(G)$ est connexe car $O_p(G)$ est un p-sous-groupe normal de G, donc il est contenu dans tous les p-sous-groupes de Sylow de G.
2) Si $O_p(G) = 1$ et un p-sous-groupe de Sylow P de G est cyclique ou quaternion généralisé, alors $\mathcal{S}_p(G)$ n'est pas connexe. En effet, soit Z l'unique p-sous-groupe de P d'ordre p. De plus Z n'est pas normal dans G car tout p-sous-groupe normal est contenu dans $O_p(G)$. Une composante connexe est constituée des p-sous-groupes de G contenant un des conjugués de Z.
3) Soit $G = \mathrm{PSL}(2, \mathbf{F}_q)$. Alors $P = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ est un p-sous-groupe de Sylow de G et il n'est pas unique. Dans ce cas on a $P \cap {}^gP = 1$ pour tout $g \notin N_G(P)$, donc $\mathcal{S}_p(G)$ n'est pas connexe.
4) Soit $G = S_{2p}$, où p est un nombre premier impair. Un p-sous-groupe de Sylow de G est $P := < (1, 2, \ldots, p) > \times < (p+1, p+2, \ldots, 2p) >$. Le complexe $\mathcal{S}_p(S_{2p})$ n'est pas connexe ; une composante connexe est, par exemple, $\mathcal{S}_p(S_p \times S_p)$.

Remarque 2.1.3 G agit par conjugaison sur les composantes connexes de $\mathcal{S}_p(G)$. Cette action est transitive car elle l'était déjà sur les p-sous-groupes de Sylow.

Définition 2.1.4 *Si $\mathcal{S}_p(G)$ n'est pas connexe, alors le stabilisateur d'une composante connexe est appelé un sous-groupe fortement p-plongé dans G.*

Proposition 2.1.5 *Si H est un sous-groupe de G, fortement p-plongé dans G, alors $H \cap {}^gH$ est un p'-groupe, pour tout $g \in G \setminus H$. Un tel H contient $N_G(Q)$, pour tout $Q \in \mathcal{S}_p(H)$.*

Preuve. Soient $g \in G$ et $\mathcal{C}$ la composante connexe stabilisée par H. Supposons que $H \cap {}^gH$ contient un p-sous-groupe de G, non-trivial, Q. De plus, H contient tous les éléments de $\mathcal{C}$ et tous les p-sous-groupes non-triviaux de H sont contenus dans $\mathcal{C}$. Il en est de même pour ${}^gH$ et ${}^g\mathcal{C}$. Donc $\mathcal{C} \cap {}^g\mathcal{C} \neq \emptyset$ ce qui entraîne $\mathcal{C} = {}^g\mathcal{C}$. Ainsi g stabilise $\mathcal{C}$ et par conséquent $g \in H$. De même, pour tout $Q \in \mathcal{S}_p(H)$ et tout $g \in N_G(Q)$, on a $Q = {}^gQ \in H \cap {}^gH$ et il s'ensuit que $g \in H$. □

Définition 2.1.6 *Soit Q un p-sous-groupe de G. On dit que Q est faiblement essentiel si $\mathcal{S}_p(N_G(Q)/Q)$ n'est pas connexe.*

Exemple 2.1.7 Si Q est d'indice p dans un p-sous-groupe de Sylow P et Q est contenu dans au moins deux p-sous-groupes de Sylow, alors Q est faiblement essentiel. En effet, P normalise Q car le normalisateur d'un sous-groupe propre de P grossit dans P et $\mathcal{S}_p(N_G(Q)/Q)$ est constitué des éléments du type S/Q, où S est un conjugué P dans $N_G(Q)$. Chacun de ces éléments constitue une composante connexe de $\mathcal{S}_p(N_G(Q)/Q)$ et il y en a au moins deux, par hypothèse.

Si Q est faiblement essentiel alors $N_G(Q)$ agit transitivement sur les composantes connexes de $\mathcal{S}_p(N_G(Q)/Q)$. Pour l'analyse des morphismes dans $F_p(G)$, de Q dans P, on passe encore au quotient par l'action de $C_G(Q)$.

Définition 2.1.8 *On dit que Q est un p-sous-groupe essentiel de G s'il est faiblement essentiel et si $C_G(Q)$ n'agit pas transitivement sur les composantes connexes de $\mathcal{S}_p(N_G(Q)/Q)$.*

Définition 2.1.9 *Soit Q un p-sous-groupe de G. On dit que Q est centrique si $Z(Q)$ est un p-sous-groupe de Sylow de $C_G(Q)$.*

Remarque 2.1.10 Cette condition est équivalente au fait que $Z(P) = C_P(Q)$ pour tout p-sous-groupe de Sylow P de G contenant Q. On trouve dans la littérature la même notion sous le nom de p-auto-centralisant [Th, p. 324].

On peut donner une caractérisation équivalente d'un p-sous-groupe essentiel de G. Cette caractérisation a l'avantage de sortir en évidence le fait qu'une condition nécessaire pour qu'un p-sous-groupe de G soit essentiel est le fait d'être centrique, propriété qui est, en général, beaucoup plus facile à vérifier que la connexité de $\mathcal{S}_p(N_G(Q)/Q)$.

Proposition 2.1.11 *Q est un p-sous-groupe essentiel de G si et seulement si Q est centrique et $\mathcal{S}_p(N_G(Q)/QC_G(Q))$ n'est pas connexe.*

La preuve a été faite dans un cadre plus général dans [Th, Thm. 48.8]. En remplaçant groupe pointé local par p-sous-groupe, $\mathcal{N}_{>Q}$ par $\mathcal{S}_p(N_G(Q))_{>Q}$ et $\mathcal{O}G$ par G on obtient la preuve dans notre cas.

Définition 2.1.12 *On dit que Q est complètement normalisé dans P par rapport à G si $N_P(Q)$ est un p-sous-groupe de Sylow de $N_G(Q)$. D'une manière équivalente, on dit que Q est complètement centralisé dans P par rapport à G si $C_P(Q)$ est un p-sous-groupe de Sylow de $C_G(Q)$.*

Le phénomène de fusion est de nature locale. Le théorème suivant, dû à Alperin [Al] en 1967 et raffiné par Puig [Pu1] en 1976, en est la preuve.

Théorème 2.1.13 (Alperin) *Tout morphisme de la catégorie $F_p(G)_{\leq P}$ peut être décomposé comme une suite de morphismes de deux types :*

i) conjugaison par un élément de $N_G(E)$, où E est un p-sous-groupe essentiel de G contenu dans P et complètement normalisé dans P.

ii) conjugaison par un élément de $N_G(P)$,

suivies d'une inclusion. Plus précisément si Q et ${}^gQ$ sont des sous-groupes de P alors il existe une décomposition $g = g_{n+1}g_n \dots g_2g_1c$, où

a) $g_i \in N_G(E_i)$, où E_i est un p-sous-groupe essentiel de G, contenu dans P et complètement normalisé dans P, pour tout $i = 1, \dots, n$,

b) $g_{n+1} \in N_G(P)$,

c) $c \in C_G(Q)$.

La preuve est aussi donnée dans [Th] dans le même cadre général des groupes pointés locaux. En remplaçant groupe pointé local par p-sous-groupe, $\mathcal{L}_G(b)_{\leq P}$ par $F_p(G)_{\leq P}$ et groupe de défaut par p-sous-groupe de Sylow, on spécialise cette preuve à notre cas.

Les notions de p-contrôle de fusion et p-sous-groupe essentiel sont fortement liées. Par le théorème précédent, si G ne contient pas de p-sous-groupes essentiels alors le normalisateur de P dans G contrôle la p-fusion. En fait, comme le montre le résultat suivant, la réciproque est aussi vraie.

Proposition 2.1.14 *Le normalisateur $N_G(P)$ contrôle la p-fusion si et seulement s'il n'y a pas de p-sous-groupes essentiels dans G.*

Preuve. Clairement, par le théorème d'Alperin, la condition est suffisante. Prouvons le fait qu'elle est aussi nécessaire. Soit Q un p-sous-groupe centrique de G. Sans restreindre la généralité on peut supposer que Q est un sous-groupe de P. En fait, Q est sous-groupe de tout p-sous-groupe de Sylow de $N_G(Q)$. Soit $T := N_P(Q)$ et R un p-sous-groupe de Sylow de $N_G(Q)$ qui contient T. Un autre p-sous-groupe de Sylow, R', contenu dans $N_G(Q)$ est conjugué à R par un élément $h \in N_G(Q)$. Comme $Q = {}^hQ < N_G(P)$, la conjugaison par h est un morphisme dans $F_p(N_G(P))$. Par le fait que $N_G(P)$ contrôle la p-fusion dans G, on a $h = gc$ avec $g \in N_G(P)$ et $c \in C_G(Q)$. Ainsi $h, c \in N_G(Q)$, donc $g = hc^{-1} \in N_G(P) \cap N_G(Q) \subset N_G(T)$. Comme, par la proposition 1.1.5, Q est un sous-groupe propre de T et $C_P(Q) \leq Q$ (Q est centrique) l'image $\overline{T}$ de T dans $N_G(Q)/Q$ est un groupe non trivial. Donc, les images de R et ${}^gR$ dans $N_G(Q)/Q$ sont connectées par $\overline{T}$. D'autre part, on peut passer de ${}^hR$ à ${}^gR$ en utilisant la conjugaison par $c \in C_G(Q)$. Ceci implique que $C_G(Q)$ agit transitivement sur les composantes connexes de $\mathcal{S}_p(N_G(Q)/Q)$ et ainsi Q n'est pas un p-sous-groupe essentiel de G. □

2.2 Y a-t-il des p-sous-groupes essentiels ?

Concernant le groupe d'automorphismes d'un p-groupe Q, Martin [Ma] et après, Henn et Priddy [HP] ont démontré que, pour presque tout p-groupe Q, le groupe d'automorphismes, $\mathrm{Aut}(Q)$, est un p-groupe. Rappelons ce que 'presque tout' veut dire dans ce contexte. Pour ceci on a besoin de définir la série de Frattini d'un p-groupe Q.

Définition 2.2.1 *Soit Q un p-groupe.*

Le sous-groupe de Frattini de Q est le sous-groupe de Q engendré par les commutateurs et les puissances p-ièmes des éléments.

La série, définie par $Q_1 = Q$ et, pour $i \geq 1$, $Q_{i+1} = (Q_i)^p[Q, Q_i]$, où, par $[\cdot,\cdot]$ on note les commutateurs des groupes entre les parenthèses, s'appelle la série de Frattini de Q.

Le nombre entier n tel que $Q_{n+1} = 1 \neq Q_n$ s'appelle la longueur de Frattini de Q.

Notons $A_{n,d}$ l'ensemble (fini) des classes d'isomorphisme des p-groupes de longueur de Frattini n et engendrés par d éléments. Étant donnée une propriété S des groupes, invariante par isomorphisme, on pose $S_{n,d} \subset A_{n,d}$ le sous-ensemble formé des éléments ayant la propriété S.

Définition 2.2.2 *On dit que presque tous les p-groupes de longueur de Frattini n ont la propriété S si*

$$\lim_{d \longrightarrow \infty} \frac{|S_{n,d}|}{|A_{n,d}|} = 1.$$

D'autre part, Gorenstein et Lyons [GL] et Aschbacher [As] ont trouvé la liste complète des groupes finis ayant un sous-groupe fortement p-plongé. Il est vrai que le fait que la liste est complète se base entièrement sur la classification des groupes finis simples.

Théorème 2.2.3 (24-1 [GL], (6.1),(6,2) [As]) *Soit G un groupe fini de centre trivial et p un nombre premier divisant l'ordre de G. Supposons que $O_{p'}(G) = 1$. Alors $\mathcal{S}_p(G)$ est non-connexe si et seulement si G a un p-sous-groupe de Sylow cyclique d'ordre p, qui n'est pas normal dans G, ou bien G est un des groupes suivants.*
a) Groupe simple de type de Lie, de rang 1 et caractéristique p.
b) A_{2p} avec $p \geq 5$.
c) ${}^2G_2(3)$, $L_3(4)$ ou M_{11} avec $p = 3$.
d) $\mathrm{Aut}(Sz(32))$, ${}^2F_4(2)'$, Mc ou $M(22)$ avec $p = 5$.
e) J_4 avec $p = 11$.

On remarque, donc, qu'il y a des conditions très restrictives imposées par l'existence d'un groupe fortement p-plongé et aussi qu'en général, si Q est un p-groupe, $\mathrm{Out}(Q)$ est un p-groupe. Ceci nous pousse, plutôt, à chercher des familles de p-groupes qui ne peuvent jamais être des p-sous-groupes essentiels. Les premiers exemples pour $p = 2$ sont les groupes des quaternions, les groupes diédraux et les groupes semi-diédraux.

Exemple 2.2.4 Les groupes d'automorphismes des groupes des quaternions Q_{2^m}, pour $m > 3$, des groupes diédraux D_{2^n}, pour $n > 2$ et des groupes semi-diédraux SD_{2^s}, pour $s > 2$ sont des 2-groupes. En effet, en étudiant les images des générateurs par un automorphisme quelconque, on obtient $|\mathrm{Aut}(Q_{2^m})| = 2^{2m-3}$, $|\mathrm{Aut}(D_{2^n})| = 2^{2n-3}$ et $|\mathrm{Aut}(SD_{2^s})| = 2^{2s-4}$, pour $m > 3$, $n > 2$ et $s > 2$. Donc, si Q est un p-groupe d'un des trois types plus haut, pour tout $X \leq \mathrm{Out}(Q)$ on a que $\mathcal{S}_p(X)$ n'a qu'une seule composante connexe, donc il est connexe. Un tel p-groupe Q ne peut pas être réalisé comme p-sous-groupe essentiel d'un groupe G car $N_G(Q)/QC_G(Q)$ est un sous-groupe de $\mathrm{Out}(Q)$.

Dans ce qui suit on donne une condition suffisante pour qu'un p-groupe ne puisse pas être réalisé comme p-sous-groupe essentiel. Pour ceci, on a besoin de quelques propriétés du sous-groupe de Frattini d'un p-groupe.

Notation 2.2.5 On denote le sous-groupe de Frattini de Q par $\Phi(Q)$.

Le sous-groupe de Frattini de Q est caractéristique dans Q. Le quotient de Q par $\Phi(Q)$ est un p-groupe abélien (car on passe au quotient par les commutateurs) élémentaire (car on passe au quotient par les puissances p-ièmes) de rang n (où n est le cardinal minimal d'un système de générateurs de Q). Donc on peut regarder $Q/\Phi(Q)$ comme un espace vectoriel de dimension n sur le corps $\mathbf{F}_p$. Par conséquent, $\mathrm{Aut}(Q/\Phi(Q))$ peut être interprété comme le groupe $\mathrm{GL}(n, \mathbf{F}_p)$ des matrices inversibles de dimension n, à coefficients dans $\mathbf{F}_p$. On a la propriété suivante.

Proposition 2.2.6 *Soit $\phi : \mathrm{Aut}(Q) \longrightarrow \mathrm{Aut}(Q/\Phi(Q))$ l'application canonique induite par la projection $Q \longrightarrow Q/\Phi(Q)$. Alors $\mathrm{Ker}\phi$ est un p-groupe.*

Preuve. Un résultat de Burnside, dont une preuve se trouve dans le livre de Gorenstein [Gr, Thm. 5.1.4], affirme que tout p'-automorphisme de Q qui induit l'identité sur $Q/\Phi(Q)$ est, en fait, l'identité sur Q. Donc $\mathrm{Ker}(\phi)$ ne contient pas de p'-éléments, ce qui entraîne que $\mathrm{Ker}(\phi)$ est un p-groupe. □

Voici quelques rappels sur le sous-groupe des matrices triangulaires inférieures dans $\mathrm{GL}(n, \mathbf{F}_p)$.

Les matrices triangulaires inférieures sont de la forme $B := \left\{ \begin{pmatrix} * & 0 & \dots & 0 \\ * & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & * \end{pmatrix} \right\}$; le nombre d'éléments de B est $\#B = p^{\frac{n(n-1)}{2}}(p-1)^n$. Donc $P := \left\{ \begin{pmatrix} 1 & 0 & \dots & 0 \\ * & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & 1 \end{pmatrix} \right\}$, qui a $p^{\frac{n(n-1)}{2}}$ éléments, est un p-sous-groupe de Sylow de B. Il est unique car il est normal dans B.

Soient G un groupe, $H, N \triangleleft G$ et $K := G/N$. Si P est l'unique p-sous-groupe de Sylow de G, alors $P \cap H$ est l'unique p-sous-groupe de Sylow de H et $P/(P \cap N)$ est l'unique p-sous-groupe de Sylow de K. Si N est un p-groupe on a une bijection entre les p-sous-groupes de Sylow de G et de K.

La proposition 2.2.6 nous aide à trouver des informations sur $\mathrm{Aut}(Q)$, à partir de l'image de ϕ, comme l'indique le lemme suivant.

Lemme 2.2.7 *Soient p un nombre premier, Q un p-groupe, $\Phi(Q)$ son sous-groupe de Frattini et n le rang du groupe abélien élémentaire $Q/\Phi(Q)$. Supposons que l'image du morphisme canonique $\phi : \mathrm{Aut}(Q) \longrightarrow \mathrm{Aut}(Q/\Phi(Q))$ induite par la projection canonique est isomorphe à un sous-groupe du groupe multiplicatif B des matrices inversibles triangulaires inférieures, de dimension n, à coefficients dans $\mathbf{F_p}$. Alors Q ne peut pas être réalisé comme p-sous-groupe essentiel dans un groupe fini G.*

Preuve. On note $\mathrm{Im}\phi$ l'image et $\mathrm{Ker}\phi$ le noyau du morphisme ϕ. Alors $\mathrm{Im}\phi$ est isomorphe à un sous-groupe de B, donc il a un unique p-sous-groupe de Sylow. Comme $\mathrm{Im}\phi \simeq \mathrm{Aut}(Q)/\mathrm{Ker}\phi$ et $\mathrm{Ker}\phi$ est un p-groupe, $\mathrm{Aut}(Q)$ a aussi un unique p-sous-groupe de Sylow et il en est de même pour $\mathrm{Out}(Q)$, car il est le quotient de $\mathrm{Aut}(Q)$ par le groupe des automorphismes intérieurs de Q, qui est un p-groupe. D'autre part, $N_G(Q)/QC_G(Q)$ est un sous-groupe de $\mathrm{Out}(Q)$ donc il a un unique p-sous-groupe de Sylow. Ainsi $\mathcal{S}_p(N_G(Q)/QC_G(Q))$ est connexe et Q ne peut jamais être réalisé comme p-sous-groupe essentiel dans un groupe fini G. □

Ce résultat nous aide à trouver d'autres familles de p-groupes, pour p impair, qui ne sont pas réalisables comme p-sous-groupes essentiels. On construit une des familles comme des tours d'extension scindées, dans lesquelles le groupe normal est cyclique.

Proposition 2.2.8 *Soient p un nombre premier impair, n un entier positif, $\alpha_1, \alpha_2, \dots, \alpha_n$ une suite d'entiers positifs avec $\alpha_i \neq \alpha_j$, pour $1 \leq i \neq j \leq n$ et M_1, $M_2, \dots, M_n$ une suite de p-groupes tels que $M_1 = C_{p^{\alpha_1}}$ et M_{i+1} est obtenu à partir de M_i à l'aide d'une extension scindée :*

$$1 \longrightarrow C_{p^{\alpha_{i+1}}} \rightarrowtail M_{i+1} \longrightarrow M_i \longrightarrow 1 \quad . \tag{1}$$

Alors le groupe M_n ne peut pas être réalisé comme un p-sous-groupe essentiel d'un groupe G.

Au premier abord, l'hypothèse que les α_i sont distincts est incontournable car dans le groupe $\mathrm{GL}(3, \mathbf{F}_p)$ il y a des p-sous-groupes essentiels isomorphes à $C_p \times C_p$, comme on verra dans la proposition 3.2.9.

Remarque 2.2.9 Une conséquence directe de ce théorème est le fait que si un p-groupe abélien se décompose en produit de groupes cycliques d'ordres distincts, alors ce p-groupe ne peut jamais être réalisé comme p-sous-groupe essentiel d'un groupe fini.

Définition 2.2.10 *Soit p un nombre premier et n, α des nombres entiers positifs. On dit que p^α divise exactement n ou que n est exactement divisible par p^α si p^α divise n et $p^{\alpha+1}$ ne divise pas n.*

Pour la preuve de la proposition on aura besoin du lemme technique suivant

Lemme 2.2.11 *Soient p un nombre premier impair, b un nombre entier tel que $b \equiv 1 \pmod p$ et n un nombre entier positif. Alors la somme $\sum_{k=0}^{p^n-1} b^k$ est exactement divisible par p^n.*

Preuve. Par récurrence sur n. Le lemme est vrai pour $n = 1$, car, en posant $b = mp + 1$, on obtient

$$\sum_{k=0}^{p-1} b^k = \sum_{k=0}^{p-1} (mp+1)^k \equiv \sum_{k=0}^{p-1} (kmp+1) \pmod{p^2} \equiv$$

$$\equiv \frac{p(p-1)}{2} mp + p \pmod{p^2} \equiv p \pmod{p^2}.$$

Pour $n \geq 2$, on a

$$\sum_{k=0}^{p^n-1} b^k = \Big(\sum_{i=0}^{p^{n-1}-1} b^i\Big)\Big(\sum_{j=0}^{p-1} (b^{p^{n-1}})^j\Big).$$

Par récurrence, p^{n-1} divise exactement le premier facteur de droite et p divise exactement le deuxième facteur de droite, donc p^n divise exactement la somme de gauche. □

Preuve de la proposition 2.2.8 Premièrement, on démontre, par récurrence sur l'indice de ces sous-groupes, que M_i admet un système minimal de générateurs $\{\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,i}\}$ avec l'ordre de $\beta_{i,j}$ égal à p^{α_j}, pour tout $j = 1, \ldots, i$ et satisfaisant la condition $(*)$: pour tout $k = 1, \ldots, i-1$, la conjugaison par un élément de $< \beta_{i,1}, \ldots, \beta_{i,k-1} >$ donne un automorphisme de $< \beta_{i,k} >$. On a $M_1 = C_{p^{\alpha_1}}$ et on choisit un générateur $b_{1,1}$ de ce groupe, qui a donc l'ordre p_1^α et la condition $(*)$ est vide dans ce cas. Il est évident que $\{b_{1,1}\}$ est un système minimal de générateurs de $C_{p^{\alpha_1}}$. Par récurrence, soient $\{\beta_{i,1}, \ldots, \beta_{i,i}\}$ un système minimal de générateurs de M_i tel que l'ordre de $\beta_{i,j}$ est p^{α_j}, satisfaisant la condition $(*)$ et β_{i+1} un générateur de $C_{p^{\alpha_{i+1}}}$. Comme l'extension (1) est scindée, il existe une section $M_i \rightarrowtail M_{i+1}$. Soient $\beta_{i+1,1}, \ldots, \beta_{i+1,i}$ dans M_{i+1}, les images de $\beta_{i,1}, \ldots, \beta_{i,i}$ par la section s, qui gardent donc les mêmes ordres. Soit, de plus, $\beta_{i+1,i+1}$ l'image de β_{i+1} par l'inclusion $C_{p^{\alpha_{i+1}}} \rightarrowtail M_{i+1}$. On obtient ainsi un système de générateurs $\beta_{i+1,1}, \ldots, \beta_{i+1,i+1}$ de M_{i+1} tel que l'ordre de $\beta_{i+1,j}$ soit α_j. Vérifions maintenant la condition $(*)$: pour tout $k = 1, \ldots, i$, la conjugaison par un élément de $< \beta_{i+1,1}, \ldots, \beta_{i+1,k-1} >$ donne un automorphisme de $< \beta_{i+1,k} >$. Pour $k = i$ la condition est satisfaite car $< \beta_{i+1,i+1} >$ est un sous-groupe normal de M_{i+1}. Comme la section s induit un isomorphisme entre M_i et

$< \beta_{i+1,1}, \ldots, \beta_{i+1,i} >$ et que les $\beta_{i,1}, \ldots, \beta_{i,i}$ satisfont la condition $(*)$ dans M_i, la condition est satisfaite aussi dans M_{i+1} pour $k < i$. De plus les commutateurs de $\beta_{i+1,i+1}$ avec $\beta_{i+1,j}$, pour tout $1 \leq j \leq i$, sont contenus dans $< \beta_{i+1,i+1} >$, donc $\{\beta_{i+1,1}, \ldots, \beta_{i+1,i+1}\}$ est un système minimal de générateurs de M_{i+1}.

Deuxièmement, posons $0 < k \leq n$ un nombre entier. Pour simplifier les notations, on pose $\beta_j := \beta_{n,j}$, pour tout $j = 1, \ldots n$. Soit $\sigma \in \mathrm{Aut}(M_n)$. Considérons la décomposition de $\sigma(\beta_k)$ suivant les générateurs de M_n

$$\sigma(\beta_k) = \beta_n^{m_n} \beta_{n-1}^{m_{n-1}} \ldots \beta_1^{m_1} .$$

où $m_1, \ldots, m_n$ sont des entiers positifs.

Soit u un nombre entier positif. On va montrer que

$$(\sigma(\beta_k))^u = \beta_n^{m_n \sum_{j=0}^{u-1} b_n^j} \beta_{n-1}^{m_{n-1} \sum_{j=0}^{u-1} b_{n-1}^j} \ldots \beta_2^{m_2 \sum_{j=0}^{u-1} b_2^j} \beta_1^{m_1 u} ,$$

pour certains nombres entiers $b_2, \ldots, b_n$, tels que $b_l \equiv 1 \pmod p$, pour tout $l = 2, \ldots, n$.

On pose $\beta := \beta_{n-1}^{m_{n-1}} \ldots \beta_2^{m_2} \beta_1^{m_1}$. Comme la condition $(*)$ est satisfaite, il existe un entier positif b_n tel que $\beta \beta_n \beta^{-1} = \beta_n^{b_n}$. Notons $b := b_n$. Alors,

$$(\sigma(\beta_k))^u = (\beta_n^{m_n} \beta)^u = \beta_n^{m_n \sum_{j=0}^{u-1} b^j} \beta^u .$$

On a $b \equiv 1 \pmod p$. En effet, $\beta^n \beta_n \beta^{-n} = \beta_n^{b^n}$. Soit p^γ l'ordre de β. Alors $\beta^{p^\gamma} = 1$ ce qui entraîne $\beta_n^{b^{p^\gamma}} = \beta_n$. Donc, $b^{p^\gamma} \equiv 1 \pmod{p^{\alpha_n}}$ et par conséquent $b^{p^\gamma} \equiv 1 \pmod p$. Puisque $b^p \equiv b \pmod p$, on obtient $b^{p^\gamma} \equiv b \pmod p \equiv 1 \pmod p$.

En utilisant de nouveau la condition $(*)$, on factorise β^u par le même procédé que celui utilisé pour $\sigma(\beta)^u$ et on obtient $\beta^u = \beta_{n-1}^{m_{n-1} \sum_{j=0}^{u-1} b_{n-1}^j} \beta'^u$. Après un nombre fini de pas on obtient une décomposition de $(\sigma(\beta_k))^u$ en puissances des générateurs $\beta_n, \ldots, \beta_1$:

$$(\sigma(\beta_k))^u = \beta_n^{m_{k,n} \sum_{j=0}^{u-1} b_n^j} \ldots \beta_2^{m_{k,2} \sum_{j=0}^{u-1} b_2^j} \beta_1^{m_{k,1} u} ,$$

avec $b_l \equiv 1 \pmod p$, pour tout $2 \leq l \leq n$.

On est maintenant en mesure de démontrer que M_n ne peut pas être réalisé comme p-sous-groupe essentiel. Le cas $n = 1$ est trivial car $M_1/\Phi(M_1) \simeq C_p$ donc $\mathrm{Aut}(M_1/\Phi(M_1))$ est un p'-groupe et donc M_1 satisfait les conditions du lemme 2.2.7.

Soit $n \geq 2$. Soit $\tau \in S_n$ une permutation, telle que $\alpha_{j_1} > \alpha_{j_2}$ si $\tau(j_1) < \tau(j_2)$.

Soit, de plus, $1 \leq k \leq n$. Considérons la décomposition de $(\sigma(\beta_k))^u$ pour $u = p^{\alpha_k}$. Maintenant, σ préserve l'ordre, donc l'ordre de $\sigma(\beta_k)$ est p^{α_k}. On a :

$$1 = (\sigma(\beta_k))^{p^{\alpha_k}} = \beta_n^{m_{k,n} \sum_{j=0}^{p^{\alpha_k}-1} b_n^j} \ldots \beta_2^{m_{k,2} \sum_{j=0}^{p^{\alpha_k}-1} b_2^j} \beta_1^{m_{k,1} p^{\alpha_k}} ,$$

avec $b_j \equiv 1 \pmod p$, pour tout $1 \leq j \leq n$. Ceci implique que, pour tout $1 \leq l \leq n$, on a $\beta_l^{m_{k,l} \sum_{j=0}^{p^{\alpha_k}-1} b_l^j} = 1$ car $\{\beta_1, \beta_2, \ldots, \beta_n\}$ est un système minimal de générateurs. Par le lemme 2.2.11, p^{α_k} divise exactement $\sum_{j=0}^{p^{\alpha_k}-1} b_n^j$, donc, si $\alpha_l > \alpha_k$, alors $p | m_{k,l}$. Ainsi les coefficients $m_{k,l}$ sont divisibles par p, pour tout k, l tels que $\tau(k) > \tau(l)$. Comme les éléments dans M_n qui apparaissent à des puissances divisibles par p sont tous dans le noyau de l'application $\phi : M_n \longrightarrow M_n/\Phi(M_n)$, et que l'image par ϕ de $\{\beta_1, \beta_2, \ldots, \beta_n\}$ est une base de $M_n/\Phi(M_n)$, l'image de σ dans $\mathrm{Aut}(M_n/\phi(M_n)) \simeq \mathrm{GL}(n, \mathbf{F}_p)$ est conjuguée par τ à une matrice triangulaire inférieure.

Il s'ensuit que l'image de $\mathrm{Aut}(M_n)$ est conjuguée par τ à un sous-groupe des matrices triangulaires inférieures. Par le lemme 2.2.7, M_n ne peut pas être réalisé comme p-sous-groupe essentiel. $\square$

La question naturelle qu'on se pose en ce moment est si on peut faire la même construction à l'inverse, c'est-à-dire faire des extensions successives avec, cette fois-ci, le groupe quotient qui est cyclique. Les vérifications s'avèrent beaucoup plus difficiles et on ne les a faites que dans un cas particulier, celui d'un produit semi-direct $(C_{p^{a_1}} \times C_{p^{a_2}} \times \ldots \times C_{p^{a_n}}) \rtimes C_{p^{a_{n+1}}}$ où $a_1 > a_2 > \ldots > a_{n+1}$ est une suite des nombres entiers positifs. Le but est toujours de démontrer que l'image des automorphismes de Q dans $\mathrm{Aut}(Q/\Phi(Q))$, par la projection canonique, est isomorphe à un sous-groupe du groupe multiplicatif des matrices triangulaires inférieures à coefficients dans $\mathbf{F}_p$. Pour ceci, on a besoin de quelques lemmes techniques. Par $\binom{n}{k}$ on note le coefficient binomial, avec la convention que $\binom{n}{k} = 0$ si $n < k$.

Lemme 2.2.12 *Soit* $M = (b_{i,j})_{1 \le i,j \le n} \in \mathrm{GL}(n, \mathbf{F}_p)$ *une matrice triangulaire inférieure de la forme*

$$M = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ b_{2,1} & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_{n1,} & \ldots & b_{n,n-1} & 1 \end{pmatrix}$$

et s un nombre entier positif. Alors $M^s = (b_{i,j}^{(s)})_{1 \le i,j \le n}$ *est aussi une matrice triangulaire inférieure et, de plus,*

$$M^s = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ b_{2,1}^{(s)} & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_{n,1}^{(s)} & \ldots & b_{n,n-1}^{(s)} & 1 \end{pmatrix}$$

avec

$$b_{i,j}^{(s)} = \binom{s}{1}\Gamma_{i,j}^{(1)} + \binom{s}{2}\Gamma_{i,j}^{(2)} + \ldots + \binom{s}{i-j}\Gamma_{i,j}^{(i-j)},$$

où $\Gamma_{i,j}^{(1)} = b_{i,j}$ *et* $\Gamma_{i,j}^{(k)} = \sum_{i > i_{k-1} > \ldots i_2 > i_1 > j} b_{i,i_{k-1}} b_{i_{k-1},i_{k-2}}, \ldots, b_{i_1,j}$, *pour tout* $2 \le k \le i-j$.

Preuve. Par récurrence sur s. Les cas "$s = 0$" et "$s = 1$" sont évidents. Supposons l'énoncé satisfait pour $s = m$ et démontrons-le pour $s = m + 1$. On a

$$M^{m+1} = M^m M = \begin{pmatrix} 1 & 0 & \dots & 0 \\ b_{2,1} & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_{n,1} & \dots & b_{n,n-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \dots & 0 \\ b_{2,1}^{(m)} & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_{n,1}^{(m)} & \dots & b_{n,n-1}^{(m)} & 1 \end{pmatrix},$$

donc $b_{i,j}^{(m+1)} = \sum_{k=j}^{i} b_{i,k}^{(m)} b_{k,j}$. Pour $i < j$, on a $b_{i,j}^{(m+1)} = 0$, pour $i = j$, on a $b_{i,i}^{(m+1)} = 1$ et, pour $i > j$, on a

$$\begin{aligned}
b_{i,j}^{(m+1)} &= b_{i,j}^{(m)} + \sum_{l=j+1}^{i-1} b_{i,l}^{(m)} b_{l,j} + b_{i,j} \\
&= \Big(\binom{m}{1} \Gamma_{i,j}^{(1)} + \binom{m}{2} \Gamma_{i,j}^{(2)} + \dots + \binom{m}{i-j} \Gamma_{i,j}^{(i-j)} \Big) + \\
&+ \sum_{l=j+1}^{i-1} \Big(\binom{m}{1} \Gamma_{i,l}^{(1)} + \binom{m}{2} \Gamma_{i,l}^{(2)} + \dots + \binom{m}{i-l} \Gamma_{i,l}^{(i-l)} \Big) b_{l,j} + b_{i,j} \\
&= \Big(b_{i,j} + \binom{m}{1} \Gamma_{i,j}^{(1)} \Big) + \Big(\binom{m}{2} \Gamma_{i,j}^{(2)} + \Big(\sum_{l=j+1}^{i-1} \binom{m}{1} \Gamma_{i,l}^{(1)} \Big) b_{l,j} \Big) + \dots + \\
&+ \Big(\binom{m}{i-j} \Gamma_{i,j}^{(i-j)} + \Big(\binom{m}{i-j-1} \Gamma_{i,j+1}^{(i-j-1)} \Big) b_{j+1,j} \Big) \\
&= \Big(1 + \binom{m}{1} \Big) \Gamma_{i,j}^{(1)} + \Big(\binom{m}{1} + \binom{m}{2} \Big) \Gamma_{i,j}^{(2)} + \dots + \\
&+ \Big(\binom{m}{i-j-1} + \binom{m}{i-j} \Big) \Gamma_{i,j}^{(i-j)} \\
&= \binom{m+1}{1} \Gamma_{i,j}^{(1)} + \binom{m+1}{2} \Gamma_{i,j}^{(2)} + \dots + \binom{m+1}{i-j} \Gamma_{i,j}^{(i-j)}.
\end{aligned}$$

Dans les calculs, on utilise l'identité binomiale $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ et le fait que $\Gamma_{i,l}^{(k)} b_{l,j} = \Gamma_{i,j}^{(k+1)}$ pour tous $1 \leq i < l < j \leq n$ et $1 \leq k \leq i - l$. Une remarque utile est le fait que $\Gamma_{i,j}^{(i-j)} = b_{i,i-1} b_{i-1,i-2} \dots b_{j+1,j}$. □

Lemme 2.2.13 *Considérons les deux matrices :*

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 1 & 0 & \dots & 0 \\ b_{2,1} & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_{n,1} & \dots & b_{n,n-1} & 1 \end{pmatrix}$$

On pose $A_1 := A$ et, par récurrence, pour $k > 0$, $A_{k+1} := A_k B + B^k A$. Soit $s \geq 1$. Si on considère que $A_s = \left(a_{i,j}^{(s)}\right)_{(i,j)\in\{1,\ldots,n\}\times\{1,\ldots,n\}}$, alors

$$a_{i,j}^{(s)} = \binom{s}{1} a_{i,j} + \sum_{\substack{0 < k+l \leq s-1 \\ k,l \geq 0}} \binom{s}{k+l+1} \Lambda_{i,j}(k,l)\,,$$

où $\Lambda_{i,j}(k,l) = \displaystyle\sum_{\substack{i > i_1 > \ldots > i_k \geq 1 \\ n \geq j_1 > \ldots > j_l > j}} b_{i,i_1} b_{i_1,i_2} \ldots b_{i_{k-1},i_k} a_{i_k,j_1} b_{j_1,j_2} \ldots b_{j_{l-1},j_l} b_{j_l,j}\,.$

Preuve. Par récurrence sur s. Le cas "$s = 1$" est évident. Supposons l'énoncé satisfait pour $s = m$ et démontrons-le pour $s = m+1$. On utilise les notations du lemme précédent.

$$A_{m+1} = \begin{pmatrix} a_{1,1}^{(m)} & \ldots & a_{1,n}^{(m)} \\ \vdots & \ldots & \vdots \\ a_{n,1}^{(m)} & \ldots & a_{n,n}^{(m)} \end{pmatrix} \begin{pmatrix} 1 & 0 & \ldots & 0 \\ b_{2,1} & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_{n,1} & \ldots & b_{n,n-1} & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & \ldots & 0 \\ b_{2,1}^{(m)} & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_{n,1}^{(m)} & \ldots & b_{n,n-1}^{(m)} & 1 \end{pmatrix} \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ldots & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{pmatrix}$$

donc $a_{i,j}^{(m+1)} = \displaystyle\sum_{r=j}^{n} a_{i,r}^{(m)} b_{r,j} + \sum_{r=1}^{i} b_{i,r}^{(m)} a_{r,j}$. Les coefficients $a_{i,r}^{(m)}$ sont donnés par récurrence et les coefficients $b_{i,r}^{(m)}$ par le lemme 2.2.12, avec la convention supplémentaire que $b_{i,i}^{(m)} = 1$. Développons :

$$\begin{aligned} a_{i,j}^{(m+1)} &= a_{i,j}^{(m)} + \sum_{r=j+1}^{n} a_{i,r}^{(m)} b_{r,j} + \sum_{r=1}^{i-1} b_{i,r}^{(m)} a_{r,j} + a_{i,j} \\ &= \Big(\binom{m}{1} a_{i,j} + \sum_{\substack{0 < k+l \leq m-1 \\ k,l \geq 0}} \binom{m}{k+l+1} \Lambda_{i,j}(k,l) \Big) + \\ &+ \sum_{r=j+1}^{n} \Big(\binom{m}{1} a_{i,r} + \sum_{\substack{0 < k+l \leq m-1 \\ k,l \geq 0}} \binom{m}{k+l+1} \Lambda_{i,r}(k,l) \Big) b_{r,j} + \\ &+ \sum_{r=1}^{i-1} \Big(\binom{m}{1} \Gamma_{i,r}^{(1)} + \binom{m}{2} \Gamma_{i,r}^{(2)} + \ldots + \binom{m}{i-r} \Gamma_{i,r}^{(i-r)} b_{i,m_1} \Big) a_{r,j} + a_{i,j}\,. \end{aligned}$$

Pour continuer le calcul on tient compte des identités remarquables suivantes :

$$\begin{aligned}
\Lambda_{i,j}(k,l+1) &= \sum_{r=j+1}^{n} \Lambda_{i,r}(k,l) b_{r,j} \\
\Lambda_{i,j}(0,1) &= \sum_{r=j+1}^{n} a_{i,r} b_{r,j} \\
\Lambda_{i,j}(k,0) &= \sum_{r=1}^{i-1} \Gamma_{i,r}^{(k)} a_{r,j} \,.
\end{aligned}$$

On remplace dans notre équation.

$$\begin{aligned}
a_{i,j}^{(m+1)} = {} & \Big(\binom{m}{1} a_{i,j} + \sum_{\substack{0 < k+l \leq m-1 \\ k,l \geq 0}} \binom{m}{k+l+1} \Lambda_{i,j}(k,l) \Big) + \\
& + \Big(\binom{m}{1} \Lambda_{i,j}(0,1) + \sum_{\substack{0 < k+l \leq m-1 \\ k,l \geq 0}} \binom{m}{k+l+1} \Lambda_{i,j}(k,l+1) \Big) + \\
& + \Big(\binom{m}{1} \Lambda_{i,j}(1,0) + \sum_{1<k\leq i-1} \binom{m}{k} \Lambda_{i,j}(k,0) \Big) + a_{i,j}
\end{aligned}$$

A présent, on met en évidence les termes $\Lambda_{i,j}(k,l)$ et on obtient

$$\begin{aligned}
a_{i,j}^{(m+1)} &= \Big(\binom{m}{1} + 1 \Big) a_{i,j} + \Big(\binom{m}{1} + \binom{m}{2} \Big) \Lambda_{i,j}(0,1) + \\
&\quad + \Big(\binom{m}{2} + \binom{m}{1} \Big) \Lambda_{i,j}(1,0) + \sum_{\substack{1 < k+l \leq m \\ k,l \geq 0}} \Big(\binom{m}{k+l} + \binom{m}{k+l+1} \Big) \Lambda_{i,j}(k,l) \\
&= \binom{m+1}{1} a_{i,j} + \sum_{\substack{0 < k+l \leq m \\ k,l \geq 0}} \binom{m+1}{k+l+1} \Lambda_{i,j}(k,l)
\end{aligned}$$

qui est la forme qu'on cherchait. □

Lemme 2.2.14 *Soient p un nombre premier impair et $0 \leq k < p-1$ un nombre entier. Alors $\sum_{j=1}^{p-1} \binom{j}{k}$ est divisible par p.*

Preuve. Notons $S_k := \sum_{j=1}^{p-1} \binom{j}{k}$. On utilise le fait que

$$(x+1)^p - 1 = ((x+1)-1)(1 + (x+1) + (x+1)^2 + \ldots + (x+1)^{p-1}) \,.$$

Comparons les coefficient de x^{k+1}. A gauche ce coefficient est $\binom{p}{k+1}$, tandis qu'à droite, il est S_k. Donc $S_k = \binom{p}{k+1}$ est divisible par p pour tous les $0 \leq k < p-1$. □

Remarque 2.2.15 Pour $k = p-1$, le lemme n'est pas vérifié car, dans ce cas $S_k = 1$. Comme ce lemme est un des ingrédients de la preuve du théorème 2.2.20, les restrictions de ce lemme vont nous imposer des restrictions sur la taille du groupe dans le théorème. On reviendra sur ce fait dans le lemme 2.2.19.

Définition 2.2.16 *Soit la matrice $M = (m_{i,j})_{1 \leq i,j \leq n}$ à coefficients dans $\mathbf{Z}$. On dit que M est p^k-triangulaire inférieure si $m_{i,j} \equiv 0 \pmod{p^k}$ pour $i < j$, p^{k-1} divise exactement $m_{i,i}$ et $m_{i,j} \equiv 0 \pmod{p^{k-1}}$ pour $i > j$.*

Remarque 2.2.17 Le nom de p^k-triangulaire inférieure donné à M vient du fait que la matrice $\frac{1}{p^{k-1}}M$, vue modulo p, est une matrice triangulaire inférieure.

On a la propriété suivante des matrices p^k-triangulaires inférieures :

Lemme 2.2.18 *Soient $A \in \mathrm{GL}(n, \mathbf{Z})$ une matrice p^k-triangulaire inférieure et $B \in \mathrm{GL}(n, \mathbf{Z})$ une matrice p^l-triangulaire inférieure. Alors le produit AB est une matrice p^{k+l-1}-triangulaire inférieure.*

Preuve. On pose $A' := \frac{1}{p^{k-1}}A$ et $B' := \frac{1}{p^{l-1}}B$. Alors A' et B' sont deux matrices p-triangulaires inférieures. Leurs images dans $\mathrm{GL}(n, \mathbf{F}_p)$ sont des matrices triangulaires inférieures. Donc le produit $A'B'$, vu dans $\mathrm{GL}(n, \mathbf{F}_p)$, est une matrice triangulaire inférieure. Ceci est equivalent avec le fait que $A'B'$ est une matrice p-triangulaire inférieure. Donc $AB = p^{k+l-2}A'B'$ est une matrice p^{k+l-1}-triangulaire inférieure. □

Lemme 2.2.19 *Soient p un nombre premier impair, a un nombre entier positif et n un nombre entiel tel que $0 \leq n < \frac{p-1}{2}$. Considérons la matrice $M = (m_{i,j})_{1 \leq i,j \leq n}$, à coefficients dans $\mathbf{Z}$, avec $m_{i,j} \equiv 0 \pmod{p}$ pour $i < j$ et $m_{i,i} \equiv 1 \pmod{p}$. Alors la matrice définie par $S := \sum_{s=0}^{p^a-1} M^s$ est une matrice p^{a+1}-triangulaire inférieure.*

Preuve. Par récurrence sur a.

Cas $a = 1$. Le lemme 2.2.13 nous donne les coefficients de $M^s \pmod{p^2}$ car, si on écrit $M = pA + B$ avec B triangulaire inférieure avec des 1 sur la diagonale et A quelconque, alors $M^s \equiv pA_s + B^s \pmod{p^2}$. Donc $S \equiv \sum_{s=0}^{p-1}(pA_s + B^s) \pmod{p^2}$. Par le lemme 2.2.12 on a les coefficients de B^s et par le lemme 2.2.13 les coefficients de A_s. Récapitulons

$$b_{i,j}^{(s)} = \binom{s}{1}\Gamma_{i,j}^{(1)} + \binom{s}{2}\Gamma_{i,j}^{(2)} + \ldots + \binom{s}{i-j}\Gamma_{i,j}^{(i-j)}$$

$$a_{i,j}^{(s)} = \binom{s}{1}a_{i,j} + \sum_{\substack{0 < k+l \leq s-1 \\ k,l \geq 0}} \binom{s}{k+l+1}\Lambda_{i,j}(k,l)\,.$$

Donc

$$\sum_{s=0}^{p-1} b_{i,j}^{(s)} = \sum_{s=0}^{p-1} \binom{s}{1} \Gamma_{i,j}^{(1)} + \sum_{s=0}^{p-1} \binom{s}{2} \Gamma_{i,j}^{(2)} + \ldots + \sum_{s=0}^{p-1} \binom{s}{i-j} \Gamma_{i,j}^{(i-j)}$$

$$\sum_{s=0}^{p-1} a_{i,j}^{(s)} = \sum_{s=0}^{p-1} \binom{s}{1} a_{i,j} + \sum_{\substack{0 < k+l \leq p-2 \\ k,l \geq 0}} \sum_{s=k+l+1}^{p-1} \binom{s}{k+l+1} \Lambda_{i,j}(k,l)$$

$$= \sum_{s=0}^{p-1} \binom{s}{1} a_{i,j} + \sum_{\substack{0 < k+l \leq p-2 \\ k,l \geq 0}} \sum_{s=0}^{p-1} \binom{s}{k+l+1} \Lambda_{i,j}(k,l) .$$

Ainsi tous les termes dans les développements de droite contiennent des facteurs de type $\sum_{s=0}^{p-1} \binom{s}{t}$ avec $t \leq 2n < p-1$ car les termes $\Gamma_{i,j}^{(k)}$ et $\Lambda_{i,j}(k,l)$ sont nuls si k ou l est plus grand que n. Par le lemme 2.2.14, ces facteurs sont divisibles par p. Il s'ensuit que S est p^2-triangulaire inférieure.

Supposons maintenant le problème résolu pour $a \leq k$ et démontrons le pour $a = k+1$. On a

$$S = \sum_{l=0}^{p^{k+1}-1} M^l = (\sum_{l=0}^{p^k-1} M^l)(\sum_{l=0}^{p-1} (M^{p^k})^l)$$

Par récurrence, $\sum_{l=0}^{p^k-1} M^l$ est une matrice p^{k+1}-triangulaire inférieure. De plus M^k hérite de M la propriété d'être une matrice p-triangulaire inférieure, car, par le lemme 2.2.18, le produit de deux matrices p-triangulaires inférieures est une matrice p-triangulaire inférieure. Le cas $a = 1$ nous donne que $\sum_{l=0}^{p-1} (M^{p^k})^l$ est p^2-triangulaire inférieure. Toujours par le lemme 2.2.18, le produit d'une matrice p^{k+1}-triangulaire inférieure avec une matrice p^2-triangulaire inférieure donne une matrice p^{k+2}-triangulaire inférieure. Donc S est p^{k+2}-triangulaire inférieure. □

Théorème 2.2.20 *Soient p un premier impair, $1 \leq n < \frac{p-1}{2}$ un entier et $a_1 > a_2 > \ldots > a_{n+1}$ une suite de nombres entiers positifs. Alors le p-groupe*

$$P = (C_{p^{a_1}} \times C_{p^{a_2}} \times \ldots \times C_{p^{a_n}}) \rtimes C_{p^{a_{n+1}}}$$

ne peut pas être réalisé comme p-sous-groupe essentiel d'un groupe fini G.

Preuve. Par le lemme 2.2.7 il suffit de démontrer que l'image du groupe d'automorphismes de P dans $\mathrm{Aut}(P/\Phi(P))$ est isomorphe à un sous-groupe du groupe multiplicatif des matrices inversibles triangulaires inférieures à coefficients dans $\mathbf{F}_p$.

On note y_i les générateurs de $C_{p^{a_i}}$ pour $1 \leq i \leq n$ et par y_{n+1} le générateur de $C_{p^{a_{n+1}}}$. Posons $R := C_{p^{a_1}} \times C_{p^{a_2}} \times \ldots \times C_{p^{a_n}}$. Comme $R \triangleleft P$, l'action par conjugaison de y_{n+1} sur R donne un automorphisme de R. Maintenant $\{y_1, y_2, \ldots, y_{n+1}\}$ est un système de générateurs de P. On va en extraire un système de générateurs minimal X. Comme les commutateurs de y_{n+1} avec tous les autres générateurs sont dans R, on en déduit que $y_{n+1} \in X$. On a aussi que $X \cap \{y_1, \ldots, y_n\} = \{y_{i_1}, \ldots, y_{i_t}\}$, où $t \leq n$ est un entier positif et $1 \leq i_1 < i_2 < \ldots < i_t \leq n$. En posant $x_j := y_{i_j}$, pour tout $1 \leq j \leq t$ et $x_{t+1} := y^{n+1}$, on obtient que $X = \{x_1, \ldots, x_{t+1}\}$.

A l'aide des générateurs dans X on peut écrire

$$ {}^{x_{t+1}}x_i = \prod_{j=1}^{t} x_j^{m_{j,i}}, $$

où $m_{i,j}$, $i, j \in \{1, \ldots, t\}$ sont des entiers positifs. On obtient ainsi une matrice à coefficients dans $\mathbf{Z}$, $M := (m_{i,j})_{(i,j)\in\{1,\ldots,t\}\times\{1,\ldots,t\}}$. Etant donné que les ordres de x_i et ${}^{x_{n+1}}x_i$ sont égaux et que l'ordre de x_{t+1} est une puissance de p, on a que $m_{i,j} \equiv 0 \pmod p$ pour $i < j$ et $m_{i,i} \equiv 1 \pmod p$ pour tous $i, j \in \{1, \ldots, t\}$. Donc M est une matrice p-triangulaire inférieure.

Soit maintenant $\sigma \in \mathrm{Aut}(P)$. On peut écrire à l'aide des générateurs dans X

$$ \sigma(x_i) = (\prod_{j=1}^{t} x_j^{u_{j,i}}) x_{t+1}^{u_{t+1,i}} $$

avec $u_{i,j}$ des entiers positifs, pour tous $i, j \in \{1, \ldots, t+1\}$.

Le but sera de montrer que $p|u_{i,j}$ pour $i < j$ et donc que l'image de σ dans $\mathrm{Aut}(P/\Phi(P))$ est dans le groupe des matrices triangulaires inférieures, car l'image de X dans $P/\Phi(P)$ est une base de $P/\Phi(P)$ vu comme espace vectoriel sur $\mathbf{F}_p$, étant donné que X est un système de générateurs minimal de P. Pour simplifier l'écriture, on va noter $\prod_{j=1}^{t} x_j^{u_{j,i}} =: \widetilde{x}^{\widetilde{u}_i}$ où $\widetilde{x}$ et $\widetilde{u}_i$ sont les transposés des vecteurs $(x_1, x_2, \ldots, x_t)$ et $(u_{1,i}, u_{2,i}, \ldots, u_{t,i})$. Calculons :

$$ {}^{x_{t+1}}(\widetilde{x}^{\widetilde{u}_i}) = ({}^{x_{t+1}}x_1)^{u_{1,i}} ({}^{x_{t+1}}x_2)^{u_{2,i}} \ldots ({}^{x_{t+1}}x_n)^{u_{t,i}} = \widetilde{x}^{M\widetilde{u}_i} $$

Si on répète le calcul, on obtient ${}^{x_{t+1}^w}(\widetilde{x}^{\widetilde{u}_i}) = \widetilde{x}^{M^w\widetilde{u}_i}$, pour tout entier $w \geq 1$. A l'aide de ces calculs préliminaires on peut obtenir les puissances s-ièmes de σ, pour tout entier positif s :

$$ (\sigma(x_i))^s = (\widetilde{x}^{(I_t+M^{u_{t+1,i}}+M^{2u_{t+1,i}}+\ldots+M^{(s-1)u_{t+1,i}})\widetilde{u}_i}) x_{t+1}^{su_{t+1,i}} = \widetilde{x}^{(\sum_{j=0}^{s-1} M^{ju_{t+1,i}})\widetilde{u}_i} x_{t+1}^{su_{t+1,i}} $$

Comme M est une matrice p-triangulaire inférieure, par le lemme 2.2.18, ses puissances le sont aussi. En particulier $M^{u_{i,t+1}}$ est p-triangulaire inférieure pour tout $i \in \{1, \ldots, t+1\}$. Par le lemme 2.2.19, la matrice $V^{(a,i)} := \sum_{j=0}^{p^a-1} M^{ju_{t+1,i}}$ est p^{a+1}-triangulaire inférieure.

Maintenant σ est un automorphisme de P, donc il préserve les ordres des éléments de P. Autrement dit, $\sigma(x_i)$ et x_i ont le même ordre, pour tout $1 \leq i \leq t$. Il s'ensuit que $(\sigma(x_i))^{p^{a_i}} = 1$. Comme les ordres des x_j pour tout $j < i$ sont strictement plus grands que p^{a_i}, il faut que, pour tout $j < i$, le j-ième élément du vecteur $V^{(a_i,i)}\widetilde{u}_i$ soit divisible par p^{a_i+1}, car celui-ci représente la puissance à laquelle sera élevé x^j dans la décomposition de $(\sigma(x_i))^{p^{a_i}}$. Et le facteur correspondant à x^j dans la décomposition de $(\sigma(x_i))^{p^{a_i}}$ doit être égal à 1 car X est un système minimal de générateurs. Ceci entraîne que $p|u_{j,i}$ pour tout $j < i$.

En effet, le premier élément de $V^{(a_i,i)}\widetilde{u}_i$ est $v_{1,1}u_{1,i} + \sum_{k=2}^{t} v_{1,k}u_{k,i}$. Comme $p^{a_i+1}|v_{1,k}$ pour $k > 1$ et comme p^{a_i} divise exactement $v_{1,1}$, car $V^{(a_i,i)}$ est p^{a_i+1}-triangulaire inférieure, il faut, si $i > 1$, que $u_{1,i}$ soit divisible par p. Soit $j < i$. On peut supposer maintenant, par récurrence, que $u_{k,i}$ est divisible par p pour tout $1 \leq k < j$ et on va montrer que $u_{j,i}$ l'est aussi. Pour ceci on calcule le j-ième élément de $V^{(a_i,i)}\widetilde{u}_i$, qui est $\sum_{k=1}^{j-1} v_{j,k}u_{k,i} + v_{j,j}u_{j,i} + \sum_{k=j+1}^{t} v_{j,k}u_{k,i}$. Pour $k < j$, $p^{a_i}|v_{j,k}$ car $V^{(a_i,i)}$, est p^{a_i+1} triangulaire inférieure et $p|u_{k,i}$ par hypothèse de récurrence donc $p^{a_i+1}|v_{j,k}u_{k,i}$. Pour $k > j$ $p^{a_i+1}|v_{j,k}$ car $V^{(a_i,i)}$ est p^{a_i+1} triangulaire inférieure. Donc $p|u_{j,i}$ car p^{a_i} divise exactement $v_{j,j}$ et $p^{a_i+1}|\sum_{k=1}^{j-1} v_{j,k}u_{k,i} + v_{j,j}u_{j,i} + \sum_{k=j+1}^{t} v_{j,k}u_{k,i}$.

Ainsi $p|u_{i,j}$ pour tout $i < j$. Cette propriété reste vraie pour tout morphisme $\sigma \in \mathrm{Aut}(P)$ car σ a été pris au hasard. Donc l'image de $\mathrm{Aut}(P)$ dans $\mathrm{Aut}(P/\Phi(P))$ est contenue dans le sous-groupe des matrices triangulaires inférieures, ce qui entraîne que P ne peut pas être réalisé comme p-sous-groupe essentiel dans un groupe fini G. □

Remarque 2.2.21 Le théorème reste vrai dans le cas plus général où l'ordre de x_{n+1} est seulement différent des ordres des x_i pour $1 \le i \le n$ et pas nécessairement plus petit. Dans ce cas il suffit juste conjuguer par une matrice de permutations pour arriver dans les matrices triangulaires inférieures.

2.3 Groupes métacycliques

Définition 2.3.1 *On dit qu'un p-groupe est métacyclique s'il est l'extension d'un p-groupe cyclique par un autre p-groupe cyclique. S'il existe une telle extension scindée on dit que le p-groupe métacyclique est scindé, sinon on dit qu'il est non-scindé.*

Autrement dit, un p-groupe Q est métacyclique s'il possède un sous-groupe normal cyclique tel que le quotient par ce groupe est aussi cyclique. Il est bien connu (voir [Hu]) qu'une présentation par générateurs et relations d'un p-groupe métacyclique est donnée par

$$< x, y | x^{p^m} = 1, y^{p^n} = x^{p^q}, {}^{y}x = x^{p^l+1} >$$

On dit alors que Q est du type (m, n, q, l).

En utilisant les travaux de Burnside [Bu], J. Dietz [Dz] classifie les présentations des p-groupes métacycliques non-abéliens et obtient que Q est non-scindé si et seulement si $q \neq m$ et $l < q < n$. Dans ce qui suit on va démontrer que les groupes métacycliques, non-abéliens, ne peuvent pas être réalisés comme p-sous-groupes essentiels.

Théorème 2.3.2 *Soit $Q =< x, y >$ un p-groupe métacyclique, non-abélien. Alors Q ne peut pas être réalisé comme p-sous-groupe essentiel.*

Preuve. Supposons que Q est de type (m, n, q, l) et choisissons x et y de sorte que $q = m$ si Q est scindé. Soit σ un automorphisme de Q. On a $\sigma(x) = x^a y^b$ et $\sigma(y) = x^c y^d$. Par le lemme 2.2.7, une condition suffisante, pour que Q ne puisse pas être réalisé comme p-sous-groupe essentiel, est que l'image du groupe d'automorphismes de Q dans $\mathrm{Aut}(Q/\Phi(Q))$ soit plongée dans le groupe des matrices triangulaires inférieures. Donc il suffit de montrer que, pour tout $\sigma \in \mathrm{Aut}(Q)$, comme avant, p divise b ou p divise c. Les relations dans Q imposent que

$$\begin{array}{ll} (1) & (\sigma(x))^{p^m} = 1\,, \\ (2) & (\sigma(y))^{p^n} = (\sigma(x))^{p^q} \quad \text{et} \\ (3) & {}^{\sigma(y)}\sigma(x) = (\sigma(x))^{p^l+1}\,. \end{array}$$

On écrit maintenant, à l'aide des générateurs, des puissances de $\sigma(x)$ et de $\sigma(y)$, et ${}^{\sigma(y)}\sigma(x)$, en posant $\sigma(x) = x^a y^b$ et $\sigma(y) = x^c y^d$. Ces développements nous seront utils par la suite. Soient r

et s deux entiers positifs.

$$\begin{aligned}
(\sigma(x))^s &= (x^a y^b)^s = x^{a\sum_{i=0}^{s-1}(p^l+1)^{ib}} y^{bs}\,, \\
(\sigma(y))^r &= (x^c y^d)^r = x^{c\sum_{i=0}^{r-1}(p^l+1)^{id}} y^{dr}\,, \\
{}^{\sigma(y)}\sigma(x) &= (x^c y^d)(x^a y^b)(x^c y^d)^{-1} = x^c y^d x^a y^b y^{-d} x^{-c} \\
&= x^{c+a(p^l+1)^d-c(p^l+1)^b} y^b\,.
\end{aligned}$$

On distingue deux cas.

Si $l \geq n$, alors Q est forcément scindé et, en remplaçant dans la relation (2) par les développements calculés et en tenant compte du fait que $q = m$, par le choix fait au début, on obtient

$$x^{c\sum_{i=0}^{p^n-1}(p^l+1)^{id}} y^{dp^n} = (\sigma(x))^{p^m}\,.$$

Mais $(\sigma(x))^{p^m} = 1$, donc $y^{dp^n} = 1$ et $x^{c\sum_{i=0}^{p^n-1}(p^l+1)^{id}} = 1$. La deuxième égalité est équivalente à $c\sum_{i=0}^{p^n-1}(p^l+1)^{id} \equiv 0 \pmod{p^m}$. Comme $(p^l+1)^d \equiv 1 \pmod{p}$, par le lemme 2.2.11, la somme $\sum_{i=0}^{p^n-1}(p^l+1)^{id}$ est exactement divisible par p^n. Maintenant Q est non-abélien, donc $l < m$, ce qui entraîne, au vu de la supposition que $l \geq n$, que $n < m$. Ceci force c à être un multiple de p.

Si $l < n$, on remplace dans la relation (3) par les développements calculés et on obtient

$$x^{c+a(p^l+1)^d-c(p^l+1)^b} y^b = x^{a\sum_{i=0}^{p^l}(p^l+1)^{ib}} y^{b(p^l+1)}\,.$$

Ceci implique que $y^{b(p^l+1)}y^{-b} \in < x >$, ce qui est équivalent à $bp^l \equiv 0 \pmod{p^n}$. Et donc b est un multiple de p.

Ces calculs nous montrent que, dans les deux cas, l'image du groupe d'automorphismes de Q dans $\mathrm{Aut}(Q/\Phi(Q))$ est plongée dans un groupe isomorphe au groupe des matrices triangulaires inférieures, car si Q est un p-groupe métacyclique non-cyclique, alors $\{x, y\}$ est un système minimal de générateurs. Le théorème en découle. $\square$

Chapitre 3

Groupes résistants

Dans ce chapitre on part à la recherche des p-groupes dont, quelle que soit leur réalisation comme p-sous-groupes de Sylow dans un groupe fini G, leur normalisateur dans G contrôle la p-fusion. On appellera ces groupes des p-groupes résistants. Le critère utilisé ici pour la recherche des p-groupes résistants est une conséquence du théorème d'Alperin, démontré dans le chapitre précédent, qui nous dit que le normalisateur d'un p-sous-groupe de Sylow contrôle la p-fusion dans G si et seulement si le p-sous-groupe de Sylow ne contient pas de p-sous-groupes essentiels de G.

Burnside a vu que les p-groupes abéliens sont résistants. Le but est de trouver d'autres exemples de p-groupes résistants. On généralise un résultat de Green et Minh [GM], en démontrant que presque tous les p-groupes extraspéciaux généralisés sont résistants. On donne aussi une autre preuve du fait, découvert par Dietz et Glauberman [MP], que les p-groupes métacycliques, pour p-impair, sont résistants.

3.1 Définition et propriétés de base

On a vu jusqu'à présent quelques exemples de groupes qui ne peuvent jamais être réalisés comme des p-sous-groupes essentiels. Dans le chapitre précédent on a vu que presque tout p-groupe a comme groupe d'automorphismes un p-groupe et qu'il y a des conditions très fortes imposées par l'existence d'un sous-groupe fortement p-plongé ; autrement dit, il y a peu de p-sous-groupes essentiels. Ceci nous fait nous pencher sur une autre question. Est-ce qu'il y a des classes de p-groupes P tels que pour toute réalisation de P comme p-sous-groupe de Sylow dans un groupe fini G, il n'y a pas de p-sous-groupe essentiel dans G ? Par la proposition 2.1.14 ceci est équivalent à demander que pour toute réalisation de P comme p-sous-groupe de Sylow dans un groupe fini G, le normalisateur $N_G(P)$ contrôle la p-fusion dans G.

Définition 3.1.1 *Un p-groupe P est appelé résistant (à la fusion) si pour tout groupe fini G tel que P est un p-sous-groupe de Sylow de G, le normalisateur $N_G(P)$ contrôle la p-fusion dans G.*

Par un théorème de Mislin [Mi], qui dit qu'un sous-groupe H d'un groupe fini G contrôle la p-fusion dans G si et seulement si l'inclusion $H \longrightarrow G$ induit un isomorphisme entre les anneaux $H^*(G, \mathbf{F}_p)$ et $H^*(H, \mathbf{F}_p)$ de cohomologie à coefficients dans $\mathbf{F}_p$, la notion de groupe résistant est équivalente à ce que Martino et Priddy [MP] appellent groupe de Swan. On rappelle que l'homomorphisme induit par l'inclusion $H \longrightarrow G$ en cohomologie est la restriction d'une classe de cohomologie de G à une classe de cohomologie de H, notée res_H^G et que P est un groupe de Swan si, pour tout G comme avant, l'inclusion $N_G(P) \longrightarrow G$ induit un isomorphisme $\mathrm{res}_{N_G(P)}^G : H^*(G, \mathbf{F}_p) \longrightarrow H^*(N_G(P), \mathbf{F}_p)$.

Le fait que, si P est résistant, alors $\mathrm{res}_{N_G(P)}^G : H^*(G, \mathbf{F}_p) \longrightarrow H^*(N_G(P), \mathbf{F}_p)$ est un isomorphisme, est un corollaire de l'énoncé suivant ([Be, Prop 3.8.4]).

Proposition 3.1.2 *Soit G un groupe fini et H un sous-groupe de G qui contrôle la p-fusion dans G. Alors $\mathrm{res}_H^G : H^*(G, \mathbf{F}_p) \longrightarrow H^*(H, \mathbf{F}_p)$ est un isomorphisme.*

Avant de donner la preuve, fixons une notion dont on aura besoin. Pour un élément $g \in G$, on note c_g^* le morphisme en cohomologie induit par la conjugaison par g.

Définition 3.1.3 *Soit G un groupe fini et $H \leq G$. On dit qu'une classe de cohomologie α dans $H^n(H, A)$ est stable par rapport à $g \in G$ si $\mathrm{res}_{H \cap {}^gH}^{{}^gH} \mathrm{c}_g^*(\alpha) = \mathrm{res}_{H \cap {}^gH}^{H}(\alpha)$.*

Preuve de la proposition 3.1.2. Soit P un p-sous-groupe de Sylow de G contenu dans H. On a le diagramme commutatif suivant

$$\begin{tikzcd} H^n(G, \mathbf{F}_p) \arrow[r, tail, "\mathrm{res}_H^G"] \arrow[dr, tail, "\mathrm{res}_P^G"'] & H^n(H, \mathbf{F}_p) \arrow[d, tail, "\mathrm{res}_P^H"] \\ & H^n(P, \mathbf{F}_p) \end{tikzcd}$$

avec res_P^G et res_P^H des injections comme indiqué. Donc le fait que res_H^G est un isomorphisme est équivalent à $\mathrm{res}_P^G(H^n(G, \mathbf{F}_p)) = \mathrm{res}_P^H(H^n(H, \mathbf{F}_p))$. Mais $\mathrm{res}_P^G(H^n(G, \mathbf{F}_p))$ (respectivement

$\mathrm{res}_P^H(H^n(H,\mathbf{F}_p)))$ sont les classes de cohomologie de $H^n(P,\mathbf{F}_p)$ stables relativement à G (respectivement à H) [Brw, Thm.3.10.3]. Il faut donc montrer que si une classe de cohomologie $\beta \in H^n(P,\mathbf{F}_p)$ est stable relativement à H, alors elle est stable relativement à G. Soit $g \in G$ et posons $Q = P \cap {}^gP$. Alors on a ${}^{g^{-1}}Q, Q \leq P$ et, comme H contrôle la p-fusion dans G, $g^{-1} = kd$, avec $k \in H$, $d \in C_G(Q)$. Posons maintenant $c := d^{-1}$ et $h := k^{-1}$. Ainsi, $Q = {}^dQ < {}^{dg}P = {}^hP$ ce qui nous permet de calculer

$$\mathrm{res}^{gP}_{P\cap {}^gP}\mathrm{c}_g^*(\beta) = \mathrm{c}_c^*\mathrm{res}^{hP}_Q\mathrm{c}_h^*(\beta) = \mathrm{c}_c^*\mathrm{res}^P_Q(\beta) = \mathrm{res}^P_Q(\beta)\,.$$

Ici on a utilisé que la conjugaison en cohomologie par un élément du centralisateur d'un groupe agit trivialement sur les classes de cohomologie de ce groupe et qu'en général on a pour $K \leq L$ et $x \in L$ que $\mathrm{res}^L_{{}^xK}\mathrm{c}_x^* = \mathrm{c}_x^*\mathrm{res}^L_K$. Donc β est stable relativement à G. □

On passe maintenant à la recherche des classes de p-sous-groupes résistants.

3.2 Groupes extraspéciaux généralisés

Une des classes de groupes résistants, hors mis quelques petites exceptions, est la classe des p-groupes extraspéciaux généralisés. Green et Minh ont démontré [GM] que presque tous les p-groupes extraspéciaux sont de Swan. Dans ce qui suit, on va généraliser ce résultat tout en évitant, dans la mesure du possible, les outils cohomologiques.

Définition 3.2.1 *Un p-groupe P est appelé extraspécial généralisé si son sous-groupe de Frattini, $\Phi(P)$, a l'ordre p, $\Phi(P) = [P,P] \simeq C_p$ et $Z(P) \geq \Phi(P)$. Si, de plus, $Z(P) = \Phi(P)$, alors P est appelé extraspécial.*

Soit P un p-groupe extraspécial généralisé. On peut regarder $V := P/\Phi(P)$ comme un espace vectoriel sur $\mathbf{F}_p$ car il est un p-groupe abélien élémentaire. En identifiant le groupe C_p avec $\mathbf{F}_p$ on définit forme bilinéaire symplectique

$$\begin{aligned} \beta : V \times V &\longrightarrow \mathbf{F}_p\,. \\ (x,y) &\mapsto [x,y] \end{aligned}$$

On décompose $V = \mathrm{Ker}\beta \oplus U$, et ainsi $\beta|_{U\times U}$ est une forme bilinéaire symplectique, non-dégénérée. En fait, on a $U \simeq P/Z(P)$. Par la classification des formes non-dégénérées symplectiques [Di, I.16], U a dimension paire sur $\mathbf{F}_p$, disons $2n$, et possède une base symplectique $\{u_1,\dots,u_n,v_1,\dots,v_n\}$. On rappelle qu'une base symplectique $\{u_1,\dots,u_n,v_1,\dots,v_n\}$ est telle que $\beta(u_i,v_j) = \delta_{i,j}$ et $\beta(u_i,u_j) = \beta(v_i,v_j) = 0$ pour tous $1 \leq i,j \leq n$.

Dans le cas des p-groupes extraspéciaux généralisés on peut choisir cette base symplectique encore plus soigneusement. On étudie séparement les cas p impair et $p = 2$.

Cas p impair. On définit une forme λ sur U par $\lambda(x) = x^p$. Cette forme est linéaire car $\lambda(x^ay^{-b}) = (x^ay^{-b})^p = x^{pa}y^{-pb}$, étant donné que les éléments de U commutent. Il y a deux possibilités. Si λ est nulle, alors tous les éléments de P sont d'ordre p et on choisit n'importe quelle base symplectique $\{u_1,\dots,u_n,v_1,\dots,v_n\}$ de U. Sinon on prend une préimage u_1 de 1 et tous les autres éléments de la base dans $\mathrm{Ker}\lambda$.

Cas $p = 2$. L'application $\rho : U \longrightarrow \mathbf{F}_p$ donnée par $\rho(x) = x^2$ est une forme quadratique, avec forme bilinéaire associée β. Cela veut dire $\rho(xy) + \rho(x) + \rho(y) = \beta(x, y)$. On a deux possibilités dépendant de l'éxistence d'une paire (u_i, v_i) dans la base telle que $\rho(u_i) = \rho(v_i) = 1$. S'il y a une telle paire, on suppose, sans restreindre la généralité, que $i = 1$ et on peut choisir les autres éléments de la base tels que $\rho(u_i) = \rho(v_i) = 0$, $i > 1$. Sinon, on peut choisir tous les éléments de la base satisfaisant $\rho(u_i) = \rho(v_i) = 0$, pour tout $1 \leq i \leq n$.

Une fois la base de U construite, on prend $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ un choix des représentants de $\{u_1, \ldots, u_n, v_1, \ldots, v_n\}$ dans P. On a donc que P est engendré par $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ et son centre Z. Dès lors on ne considérera que des systèmes de générateurs de P qui contiennent un choix de représentants de $\{u_1, \ldots, u_n, v_1, \ldots, v_n\}$ et tous les éléments de Z. On appelle un tel système un système générateur symplectique de P.

Remarque 3.2.2 Soient $u, v \in U$ et prenons $e, f \in P$ des représentants de u et v, respectivement. Alors il existe $z \in \Phi(P)$ d'ordre p tel que

1. si $\beta(u, v) = 1$ alors $[e, f] = z$,
2. si $\beta(u, v) = 0$ alors $[e, f] = 1$,
3. si $\lambda(u) = 1$ (ou $\rho(u) = 1$) alors $e^p = z$,
4. si $\lambda(u) = 0$ (ou $\rho(u) = 0$) alors $e^p = 1$.

Si tous les éléments de P sont d'ordre p, on dit que P est d'exposant p, autrement P est d'exposant p^2. Soit $\{e_1, \ldots, e_n, f_1, \ldots, f_n, Z\}$ un système de générateurs symplectique de P. On a vu que les relations entre les générateurs sont $(e_i)^p = (f_j)^p = 1$, pour tous $2 \leq i, j \leq n$, $[e_i, f_j] = z^{\delta_{i,j}}$ et $[e_i, e_j] = [f_i, f_j] = 1$, pour tous $1 \leq i, j \leq n$ où $z \in \Phi(P)$. Suivant les relations qui font intervenir e_1 et f_1 il y a quatre classes de p-groupes extraspéciaux généralisés, deux pour p impair et deux pour $p = 2$.

Cas p impair :

a) $(e_1)^p = (f_1)^p = 1$ (ex. $(C_p \times C_p) \rtimes C_p$) ; P est d'exposant p ;

b) $(e_1)^p = z, (f_1)^p = 1$ (ex. $(C_{p^2}) \rtimes C_p$) ; P est d'exposant p^2.

Cas $p = 2$:

a) $(e_1)^2 = (f_1)^2 = 1$ (ex. le groupe diédral D_8) ;

b) $(e_1)^2 = (f_1)^2 = z$ (ex. le groupe des quaternions Q_8).

Tous ces résultats sur les p-groupes extraspeciaux généralises sont bien connus ; voir, par exemple l'article récent de Dietz [Dz2]. Le lemme suivant donne la structure d'un p-groupe extraspécial généralisé.

Lemme 3.2.3 *Soit P un p-groupe extraspécial généralisé. Alors, ou bien $Z(P)$ est isomorphe à $\Phi(P) \times A$ et P est isomorphe à $E \times A$, ou bien $Z(P)$ est isomorphe à $C_{p^2} \times A$ et P est isomorphe à $(E * C_{p^2}) \times A$, où E est un p-groupe extraspécial, A est un p-groupe abélien élémentaire et $E * C_{p^2} = (E \times C_{p^2})/\{(u, f(u)) | u \in \Phi(E)\}$ où f est un morphisme injectif de $\Phi(E)$ dans C_{p^2}.*

Preuve. Comme $\Phi(P)$ est un sous-groupe cyclique d'ordre p, le centre $Z(P)$ admet au plus un facteur isomorphe à C_{p^2} dans sa décomposition en sous-groupes cycliques, et, si ce facteur existe, il contient $\Phi(P)$. Soit A un sous-groupe abélien élémentaire de $Z(P)$ tel que $Z(P) \simeq \Phi(P) \times A$, quand il n'y a pas de facteur de type C_{p^2} dans $Z(P)$, et $Z(P) \simeq C_{p^2} \times A$, dans le cas contraire. On a, dans les deux cas, $[P, P] \cap A = 1$ et $[P, A] = 1$ donc A est un facteur direct de P. Il s'ensuit que le complément de A dans P est isomorphe ou bien à E (s'il n'y a pas de facteur de type C_{p^2} dans $Z(P)$), ou bien à $E * C_{p^2}$ (dans le cas contraire). □

On rappelle qu'un sous-espace vectoriel isotrope de U par rapport à β est un sous-espace sur lequel β est identiquement nulle. Un sous-espace maximal isotrope de U a dimension égale à la moitié de la dimension de U. Comme $\dim U = 2n$, la dimension d'un sous-espace maximal isotrope de U est n.

Lemme 3.2.4 *Soit Q un sous-groupe centrique de P. Alors Q contient $Z(P)$ et $Q/Z(P)$ contient un sous-espace isotrope maximal de $P/Z(P)$.*

Preuve. Un sous-groupe centrique de P contient le centre $Z := Z(P)$ de P. Supposons que $Q/Z(P)$ ne contient pas un sous-espace isotrope maximal de $P/Z(P)$. En ce cas $V := Q/Z(P)$, vu comme un espace vectoriel, ne contient pas un sous-espace isotrope maximal de $U := P/Z(P)$ par rapport à β. Ceci veut dire qu'il existe $u \in U \setminus V$ avec $\beta(u, x) = 0$, pour tout $x \in V$. En prenant un représentant e de u dans P on a $e \in P \setminus Q$ et e commute avec tous les éléments de Q. Donc $e \in C_P(Q) \setminus Q \neq \emptyset$, ce qui est une contradiction avec le fait que Q est centrique. □

Voici maintenant le résultat annoncé sur les p-groupes extraspéciaux généralisés.

Théorème 3.2.5 *Soit P un p-groupe extraspécial généralisé. Alors P est résistant à l'exception du cas où $P = E \times A$ avec A abélien élémentaire et E diédral d'ordre 8 (quand $p = 2$) ou d'ordre p^3 et exposant p (quand p est impair).*

Corollaire 3.2.6 *Si P satisfait les conditions du théorème, alors P est un groupe de Swan.*

Preuve. Le fait que P soit résistant est équivalent au contrôle de la p-fusion par son normalisateur dans tout groupe G où P est réalisé comme p-sous-groupe de Sylow. Par la proposition 3.1.2, ceci veut dire que res^G_H induit un isomorphisme entre $H^n(G, \mathbf{F}_p)$ et $H^n(N_G(P), \mathbf{F}_p)$, pour tout $n \geq 0$, donc P est un groupe de Swan. □

Preuve du théorème 3.2.5. On va montrer que, si P peut être réalisé comme p-sous-groupe de Sylow d'un groupe G qui contient un p-sous-groupe essentiel, alors P est une des exceptions au théorème décrites précédemment.

Soit Q un sous-groupe centrique de P. Par le lemme 3.2.4, ceci force Q à contenir $Z(P)$ et, a fortiori, $\Phi := \Phi(P)$. Désignons par R le sous-groupe de $N := (N_G(Q) \cap N_G(\Phi))/C_G(Q)$ qui agit trivialement sur Φ et Q/Φ. Alors R est un sous-groupe de $\mathrm{Aut}(Q)$ qui centralise les quotients de la série centrale $1 \triangleleft \Phi \triangleleft Q$ donc il est un p-sous-groupe de N, par la proposition 1.1.9. De plus R est normal dans N car N fixe Q et Φ. Maintenant R contient $P/C_P(Q)$, étant donné que P agit trivialement sur Φ et Q/Φ. Comme P est un p-sous-groupe de Sylow de G, qui normalise Q, il s'ensuit que P est un p-sous-groupe de Sylow de $N_G(Q)$, donc $P/C_P(Q)$ est un p-sous-groupe de Sylow de N. Ainsi on a $R = P/C_P(Q)$, et, comme R est normal dans N, il est l'unique p-sous-groupe de Sylow de N.

Supposons que Q est un p-sous-groupe essentiel de G. Alors $\mathcal{S}_p(N_G(Q)/QC_G(Q))$ est non-connexe. Ceci force $N_G(Q) \not\leq N_G(\Phi)$ car, dans le cas contraire, on aurait $N_G(Q)/C_G(Q) = N$, donc $N_G(Q)/QC_G(Q)$ aurait un unique p-sous-groupe de Sylow et $\mathcal{S}_p(N_G(Q)/QC_G(Q))$ serait connexe. Comme $\Phi(Q)$ est un sous-groupe caractéristique de Q, on a $N_G(Q) \leq N_G(\Phi(Q))$ et en tenant compte du fait que $N_G(Q) \not\leq N_G(\Phi)$ on obtient que $\Phi(Q) \neq \Phi$. Mais Φ est un groupe d'ordre p et $\Phi(Q) \leq \Phi$. On en déduit que $\Phi(Q)$ est trivial, ce qui entraîne que Q est abélien élémentaire. Comme Q est centrique, car essentiel, $C_P(Q) = Q$ et donc $R = P/Q$.

Prenons un élément $x \in N_G(Q) \setminus N_G(\Phi)$. Le groupe R n'est pas contenu dans ${}^xN$, sinon N et ${}^xN$ auraient le même p-sous-groupe de Sylow, R. Ceci impliquerait que $P/Q = {}^x(P/Q)$ et donc x normaliserait P et, par conséquent, Φ, ce qui est en contradiction avec le choix de x. Ainsi on obtient que $P \not\leq N_G({}^x\Phi)$ et, par conséquent, P ne centralise pas ${}^x\Phi$. Maintenant ${}^x\Phi$ est un sous-groupe de P d'ordre p qui n'est pas contenu dans le centre de P.

Soit u un générateur de ${}^x\Phi$ et considérons l'application $g : U \to \mathbf{F}_p$ donnée par $g(y) = [y, u]$, où $U = P/Z(P)$. C'est une application linéaire, car $[yz, u] = [y, u][z, u]$. Comme le noyau de g ne peut pas être trivial, étant donné que P ne centralise pas ${}^x\Phi$, il doit être un espace de codimension 1 de U. Donc $|P : C_P({}^x\Phi)| = p$.

Si Q est un sous-groupe propre de $C_P({}^x\Phi)$ alors $C_P({}^x\Phi)$ est non-abélien car Q est centrique. On en déduit que $\Phi(C_P({}^x\Phi))$ est non-trivial et, comme il est contenu dans Φ, on a $\Phi = \Phi(C_P({}^x\Phi))$. Maintenant, ${}^{x^{-1}}(C_P({}^x\Phi)) < C_{N_G(Q)}(\Phi)$ et, comme P est un p-sous-groupe de Sylow de $C_{N_G(Q)}(\Phi)$, il existe $c \in C_{N_G(Q)}(\Phi)$ tel que ${}^{cx^{-1}}(C_P({}^x\Phi)) < P$. De plus, le sous-groupe de Frattini de ${}^{cx^{-1}}(C_P({}^x\Phi))$ est ${}^{cx^{-1}}\Phi$, qui est non-trivial. Ceci implique que ${}^{cx^{-1}}\Phi = \Phi$ ce qui est équivalent à $\Phi = {}^x\Phi$ et on obtient de nouveau une contradiction.

Donc on a $Q = C_P({}^x\Phi)$ et $|P : Q| = p$. Mais Q est centrique, donc, par le lemme 3.2.4, $Q/Z(P)$ est un sous-espace isotrope maximal de $P/Z(P)$. Ainsi $|P/Z(P)| = |P : Q|^2 = p^2$. De plus ${}^x\Phi \not\leq Z(P)$, et, en faisant le même raisonnement pour x^{-1} on obtient que ${}^{x^{-1}}\Phi \not\leq Z(P)$, donc $\Phi \not\leq {}^xZ(P)$.

Finalement posons $T := Z(P) \cap {}^x(Z(P))$. Comme $|Q : Z(P)| = |Q : {}^x(Z(P))| = p$ et $Z(P) \neq {}^x(Z(P))$, car $\Phi \leq Z(P)$ mais $\Phi \not\leq {}^xZ(P)$, on obtient que $|Z(P) : T| = p$ et $\Phi \not\leq T$. Comme Q est abélien élémentaire, $Z(P)$ l'est aussi et, par le lemme 3.2.3, on a $Z(P) = \Phi \times T$ et $P = E \times T$ avec E extraspécial d'ordre p^3. De plus $|Q : T| = |Q : Z(P)||Z(P) : T| = p^2$, donc Q/T est isomorphe à $C_p \times C_p$. Ainsi, pour $p = 2$, E n'est pas isomorphe au groupe des quaternions car Q_8 n'a pas de sous-groupes isomorphes à $C_2 \times C_2$.

Pour p impair, soit $H := < P/Q, {}^x(P/Q) >$. C'est un groupe isomorphe à un sous-groupe de $N_G(Q)/C_G(Q)$ qui fixe T, donc on peut le voir comme un sous-groupe de $\mathrm{Aut}(Q/T)$. Et, étant donné que Q/T est isomorphe à $C_p \times C_p$, il s'ensuit que H peut être vu comme un sous-groupe de $\mathrm{GL}(2, \mathbf{F}_p)$. Maintenant, P/Q et ${}^x(P/Q)$ sont deux p-sous-groupes de Sylow distincts de H.

Soit $h \in H$ tel que $P/Q = {}^h(P/Q)$. En prenant g un représentant de h dans $N_{C_G(T)}(Q)$ qui normalise P, il s'ensuit que g induit la conjugaison par h sur Q/T et P/Q. On est maintenant dans les hypothèses du lemme 3.2.7, plus bas. Il s'ensuit que la suite exacte courte $1 \longrightarrow Q/T \longrightarrow E \longrightarrow P/Q \longrightarrow 1$ peut être étendue à $1 \longrightarrow Q/T \longrightarrow L \longrightarrow H \longrightarrow 1$. Et on conclut pour p impair car, par le même lemme 3.2.7, le groupe E n'est pas isomorphe à $C_{p^2} \rtimes C_p$.

Il nous reste seulement les cas $P = E \times T$, où E est diédral d'ordre 8 ou extraspécial d'ordre p^3 et exposant p (pour p impair). $\square$

Lemme 3.2.7 *Soient p un premier impair, Q un p-groupe abélien élémentaire d'ordre p^2 et H un sous-groupe du groupe d'automorphismes de Q. Supposons que H possède un p-sous-groupe de Sylow R non-trivial et qu'on se donne le p-groupe P tel que la suite $1 \longrightarrow Q \longrightarrow P \longrightarrow R \longrightarrow 1$ soit exacte.*

a) Si, pour tout morphisme $\phi \in N_H(R)$, il existe un automorphisme ψ de P, tel que $\psi(u) = \phi(u)$, pour tout $u \in Q$ et $\psi\rho\psi^{-1} = \phi\rho\phi^{-1}$ pour tout $\rho \in R$, alors on peut étendre l'extension $1 \longrightarrow Q \longrightarrow P \longrightarrow R \longrightarrow 1$ à une exension $1 \longrightarrow Q \longrightarrow L \longrightarrow H \longrightarrow 1$.

b) Si H a au moins deux p-sous-groupes de Sylow distincts et on peut étendre l'extension $1 \longrightarrow Q \longrightarrow P \longrightarrow R \longrightarrow 1$ à une exension $1 \longrightarrow Q \longrightarrow L \longrightarrow H \longrightarrow 1$ alors P n'est pas isomorphe à $C_{p^2} \rtimes C_p$.

Preuve. a) Pour voir que l'extension $1 \longrightarrow Q \longrightarrow P \longrightarrow R \longrightarrow 1$ s'étend à l'extension $1 \longrightarrow Q \longrightarrow L \longrightarrow H \longrightarrow 1$, il suffit de vérifier [Brw, pp.84-85] que la classe de cohomologie $h(P)$, déterminée par P dans $H^2(R,Q)$, est H-stable, c'est-à-dire que pour tout $\phi \in H$ on a

$$\mathrm{res}^{R}_{R\cap {}^{\phi}R} h(P) = \mathrm{res}^{{}^{\phi}R}_{R\cap {}^{\phi}R} \mathrm{c}^*_{\phi}(h(P)) \quad (*)\,.$$

Ici res est la restriction en cohomologie et c^*_{ϕ} est le morphisme induit par la conjugaison par ϕ en cohomologie. Si $R \neq {}^{\phi}R$ alors $R \cap {}^{\phi}R = 1$, car R est un p-groupe d'ordre p, et la relation $(*)$ est clairement est satisfaite. Supposons que $R = {}^{\phi}R$. Par l'hypothèse, il existe un automorphisme ψ de P tel que $\psi(u) = \phi(u)$, pour tout $u \in Q$ et $\psi\rho\psi^{-1} = \phi\rho\phi^{-1}$ pour tout $\rho \in R$. Ceci implique que $h(P) = \mathrm{c}^*_{\phi}(h(P))$ et $(*)$ est de nouveau satisfait. En effet, soit $1 \longrightarrow Q \longrightarrow P' \longrightarrow R \longrightarrow 1$ une suite exacte représentant la classe $\mathrm{c}^*_{\phi}(h(P)) \in H^2(R,Q)$. Par la définition de c^*_{ϕ} (voir [Brw, pp.80]), il existe un isomorphisme $f : P \longrightarrow P'$ tel que le diagramme suivant commute

$$\begin{tikzcd}
h(P) & 1 \arrow[r] & Q \arrow[r] \arrow[d, "\phi"'] & P \arrow[r] \arrow[d, "f"'] & R \arrow[r] \arrow[d, "\mathrm{conj}(\phi)"'] & 1 \\
\mathrm{c}^*_{\phi}(h(P)) & 1 \arrow[r] & Q \arrow[r] & P' \arrow[r] & R \arrow[r] & 1
\end{tikzcd}$$

D'autre part la condition sur l'existence de ψ nous donne le diagramme commutatif suivant.

$$\begin{tikzcd}
h(P) & 1 \arrow[r] & Q \arrow[r] \arrow[d, "\phi"'] & P \arrow[r] \arrow[d, "\psi"'] & R \arrow[r] \arrow[d, "\mathrm{conj}(\phi)"'] & 1 \\
h(P) & 1 \arrow[r] & Q \arrow[r] & P \arrow[r] & R \arrow[r] & 1
\end{tikzcd}$$

En prenant $g := f\psi^{-1} : P \longrightarrow P'$ on obtient

$$\begin{tikzcd}
h(P) & 1 \arrow[r] & Q \arrow[r] \arrow[d, "\mathrm{id}"'] & P \arrow[r] \arrow[d, "f\psi^{-1}"'] & R \arrow[r] \arrow[d, "\mathrm{id}"'] & 1 \\
\mathrm{c}^*_{\phi}(h(P)) & 1 \arrow[r] & Q \arrow[r] & P' \arrow[r] & R \arrow[r] & 1
\end{tikzcd}$$

ce qui entraîne que $h(P) = \mathrm{c}^*_{\phi}(h(P))$.

b) La preuve de la deuxième partie du lemme est due à Jacques Thévenaz. Elle est basée sur le fait que $H^2(\mathrm{SL}(2,\mathbf{F}_p),Q)=0$, qui sera prouvé plus bas. Maintenant, par la première partie de la preuve, $h(P)$ s'étend à une classe de cohomologie dans $H^2(H,Q)$. De plus H contient $\mathrm{SL}(2,\mathbf{F}_p)$, étant donne que H a au moins deux p-sous-groupes de Sylow, et n'importe quels deux p-sous-groupe de Sylow de $\mathrm{GL}(2,\mathbf{F}_p)$ engendrent $\mathrm{SL}(2,\mathbf{F}_p)$. Donc $h(P)$ s'étend à une classe de cohomologie dans $H^2(\mathrm{SL}(2,\mathbf{F}_p),Q)$, ce qui entraîne que $h(P)$ est triviale. Ainsi P n'est pas isomorphe à $C_{p^2}\rtimes C_p$ car la classe de cohomologie induite par $C_{p^2}\rtimes C_p$ dans $H^2(Q,R)$ n'est pas triviale (autrement dit, $C_{p^2}\rtimes C_p$ n'est pas un produit semi-direct de $C_p\times C_p$ par C_p).

Montrons que $H^2(\mathrm{SL}(2,\mathbf{F}_p),Q)=0$. Soit $U:=\left\{\begin{pmatrix}1&*\\0&1\end{pmatrix}\right\}$ un p-sous-groupe de Sylow de $\mathrm{SL}(2,\mathbf{F}_p)$. Posons $S:=\mathrm{SL}(2,\mathbf{F}_p)$ et $N(U):=N_{\mathrm{SL}(2,\mathbf{F}_p)}(U)$. La restriction en cohomologie à U donne un monomorphisme $\mathrm{res}^S_U: H^2(S,Q)\longrightarrow H^2(U,Q)^{N(U)}$ où $H^2(U,Q)^{N(U)}$ est le groupe des points fixes sous l'action naturelle de $N(U)$. Maintenant $U=<u>$ est un groupe cyclique d'ordre p, donc, [Be, p. 60] sa cohomologie est

$$H^2(U,Q)=Q^U/\{(\sum_{i=0}^{p-1}u^i)v|v\in Q\}\,.$$

Par un calcul simple, on obtient que $Q^U=<z>$, où z est un générateur de $\Phi(P)$, et que $\{(\sum_{i=0}^{p-1}u^i)v|v\in Q\}=0$ donc $H^2(U,Q)=<z>$. Comme z n'est pas fixé par $N(U)$, on a $H^2(U,Q)^{N(U)}=0$ et, ainsi, $H^2(S,Q)=0$. □

On montre maintenant que les cas restants sont vraiment des exceptions au théorème 3.2.5. Commençons par une propriété des groupes résistants.

Proposition 3.2.8 *Soit P un p-groupe et A un p-groupe abélien. Si P n'est pas résistant alors le produit direct $P\times A$ ne l'est pas non plus.*

Preuve. Soit G un groupe fini ayant P comme p-sous-groupe de Sylow et soit Q un p-sous-groupe essentiel de G contenu dans P. Un tel G existe car on suppose que P n'est pas résistant. En ce cas $\widetilde{P}:=P\times A$ est un p-sous-groupe de Sylow de $\widetilde{G}:=G\times A$. Comme Q est centrique dans P, il en est de même pour $\widetilde{Q}:=Q\times A$ dans $\widetilde{P}$. De plus, on a $N_{\widetilde{G}}(\widetilde{Q})/\widetilde{Q}C_{\widetilde{G}}(\widetilde{Q})\simeq N_G(Q)/QC_G(Q)$. Comme $\mathcal{S}_p(N_G(Q)/QC_G(Q))$ est non-connexe, ceci veut dire que $\mathcal{S}_p(N_{\widetilde{G}}(\widetilde{Q})/\widetilde{Q}C_{\widetilde{G}}(\widetilde{Q}))$ est aussi non-connexe. Alors $\widetilde{Q}$ est un p-sous-groupe essentiel de $\widetilde{G}$ et $\widetilde{P}$ n'est pas résistant. □

Proposition 3.2.9 *Soit $P=E\times A$ où A est abélien élémentaire et E est diédral d'ordre 8 (si $p=2$) ou est de ordre p^3 et exposant p (si p est impair). Alors P n'est pas résistant.*

Preuve. Considérons E comme dans l'énoncé. On réalise E comme p-sous-groupe de Sylow de $\mathrm{GL}(3,\mathbf{F}_p)$ en prenant $E=\left\{\begin{pmatrix}1&*&*\\0&1&*\\0&0&1\end{pmatrix}\right\}$. Alors les groupes $Q_1=\left\{\begin{pmatrix}1&0&*\\0&1&*\\0&0&1\end{pmatrix}\right\}$ et $Q_2=\left\{\begin{pmatrix}1&*&*\\0&1&0\\0&0&1\end{pmatrix}\right\}$ sont des p-sous-groupes essentiels de G. En effet, Q_i est centrique et $N_G(Q_i)/Q_iC_G(Q_i)\simeq\mathrm{SL}(2,\mathbf{F}_p)$, pour $i=1,2$. Comme $\mathcal{S}(\mathrm{SL}(2,\mathbf{F}_p))$ est non-connexe, on obtient que Q_i est un p-sous-groupe essentiel de G, pour $i = 1, 2$. Donc E n'est pas résistant. Comme P est isomorphe à $E \times A$, où A est abélien élémentaire, par Proposition 3.2.8, P n'est pas non plus résistant. $\square$

3.3 Groupes métacycliques

On retourne vers les p-groupes métacycliques, cette fois pour les regarder du point du vue des p-groupes résistants.

Théorème 3.3.1 *Soient p un nombre premier impair et P un p-groupe métacyclique. Alors P est un p-groupe résistant.*

Pour la notion équivalente de groupe de Swan, ce résultat à été démontré par Dietz et Glauberman. La preuve a été publiée dans un article de Martino et Priddy [MP]. La preuve qu'on donne ici est basée sur la recherche des p-sous-groupes essentiels dans P pour toute réalisation de ce dernier comme un p-sous-groupe de Sylow dans un groupe G.

Preuve. Par le théorème 2.3.2 et la remarque 2.2.9, les seuls sous-groupes de P candidats à être essentiels sont les produits directs de deux groupes cycliques de même ordre $Q \simeq C_{p^\alpha} \times C_{p^\alpha}$.

Soit G un groupe fini ayant P comme p-sous-groupe de Sylow. Supposons par l'absurde qu'il existe un p-sous-groupe essentiel, Q, de G. Comme Q est centrique, complètement normalisé dans G, le groupe $N_G(Q)/C_G(Q)$ a $N_P(Q)/Q$ comme p-sous-groupe de Sylow et $C_G(Q) = Q \times M$, où $M = O_{p'}(C_G(Q))$. De plus $\mathcal{S}_p(N_G(Q)/C_G(Q))$ est non-connexe donc $N_G(Q)/C_G(Q)$ n'admet pas de p-sous-groupe normal non-trivial.

Soit $\Phi(Q)$ le sous-groupe de Frattini de Q. Par la proposition 2.2.6, le noyau de l'application canonique $\phi : N_G(Q)/C_G(Q) \longrightarrow \mathrm{Aut}(Q/\Phi(Q))$ est un p-sous-groupe normal de $N_G(Q)/C_G(Q)$. Par la conclusion de l'alinéa précédent, ce noyau est trivial. Il s'ensuit que ϕ est injectif. On a aussi que l'image de ϕ contient un sous-groupe isomorphe à $\mathrm{SL}(2, \mathbf{F}_p)$, sinon elle serait contenue dans le normalisateur d'un p-sous-groupe de Sylow, donc isomorphe à un sous-groupe du groupe des matrices triangulaires inférieures de $\mathrm{GL}(2, \mathbf{F}_p)$. Par le lemme 2.2.7 on contredirait le fait que Q est un p-sous-groupe essentiel de G. En résumé, $N_G(Q)/C_G(Q)$ est isomorphe à l'image de ϕ, donc contient un sous-groupe isomorphe à $\mathrm{SL}(2, \mathbf{F}_p)$ et a un p-sous-groupe de Sylow d'ordre p.

Maintenant $\Phi(Q)$ est caractéristique dans Q, donc il est normal dans $N_G(Q)$. On travaille dans $N_G(Q)/\Phi(Q)$. Un p-sous-groupe de Sylow de $N_G(Q)/\Phi(Q)$ est $N_P(Q)/\Phi(Q)$, qui est un p-groupe métacyclique non-abélien d'ordre p^3. Mais il y a un unique p-groupe métacyclique non-abélien d'ordre p^3 et celui-ci est isomorphe à $C_{p^2} \rtimes C_p$.

On se retrouve dans les hypothèses de la partie b) du lemme 3.2.7, avec $Q/\Phi(Q)$ comme groupe abélien élémentaire de rang 2, $N_G(Q)/C_G(Q)$ comme sous-groupe du groupe d'automorphismes de $Q/\Phi(Q)$ et $N_P(Q)/Q$ un p-sous-groupe de Sylow de $N_G(Q)/C_G(Q)$. En effet, l'extension $1 \longrightarrow Q/\Phi(Q) \longrightarrow N_P(Q)/\Phi(Q) \longrightarrow N_P(Q)/Q \longrightarrow 1$ s'étend à l'extension $1 \longrightarrow Q/\Phi(Q) \longrightarrow N_G(Q)/(M \times \Phi(Q)) \longrightarrow N_G(Q)/C_G(Q) \longrightarrow 1$ et donc, on obtient que $N_P(Q)/\Phi(Q)$ n'est pas isomorphe à $C_{p^2} \rtimes C_p$, ce qui est une contradiction. Ainsi, Q ne peut pas être un p-sous-groupe essentiel de G.

En conclusion, P ne contient pas de p-sous-groupes essentiels de G, quelle que soit la réalisation de P comme p-sous-groupe de Sylow d'un groupe fini G. Donc il est résistant. $\square$

Chapitre 4

Systèmes complets de Frobenius

Le but de ce chapitre est de généraliser les résultats du chapitre 3 aux systèmes complets de Frobenius sur un p-groupe P. Dans la première partie on définit la notion de paire de Brauer dans une algèbre de groupe kG où k est un corps de caractéristique p. On continue avec les notions de catégorie de Brauer et système complet de Frobenius sur un p-groupe P. On démontre que la sous-catégorie de Brauer pleine au-dessous d'une paire maximale (P, e), est un système complet de Frobenius sur P. Par ailleurs, la catégorie de Brauer associée au bloc principal de kG est équivalente à la catégorie de Frobenius de G.

Sur les systèmes complets de Frobenius on définit les notion de contrôle de la p-fusion et de sous-groupe essentiel. On démontre, par la suite, une généralisation d'un théorème de Gilotti et Serena dans le cadre d'un système complet de Frobenius $\mathcal{F}$, qui donne des conditions nécessaires et suffisantes sur un sous-groupe Q de P pour que les morphismes dans $\mathcal{F}$ qui normalisent Q contrôlent la p-fusion dans $\mathcal{F}$. En utilisant ce théorème on démontre que les mêmes groupes qu'au chapitre 3 sont résistants dans le cadre des systèmes complets de Frobenius.

4.1 Terminologie et premières propriétés

Pour trouver des nouvelles informations sur la table des caractères des groupes finis simples, Richard Brauer, dans les années '40, a eu l'idée originale d'étudier les représentations des groupes sur des corps de caractéristique p, où p est un nombre premier divisant d'ordre du groupe. Ce fut une approche couronnée de beaucoup de résultats profonds. Ce nouvel outil mathématique a été appelé la théorie de la représentation modulaire. Un des buts de cette théorie est d'obtenir une classification des représentations irréductibles sur un corps k de caractéristique p.

Se donner une représentation (irréductible) d'un groupe G sur un corps k de caractéristique p est équivalent à se donner un module (simple) sur l'algèbre de groupe kG. On rappelle qu'une algèbre de groupe sur un corps k est la donnée d'un espace vectoriel sur k de base les éléments de G et d'une loi de multiplication engendrée par la multiplication dans G.

L'algèbre de groupe kG peut être décomposée en produit direct d'algèbres indécomposables $kG \simeq \prod_{j=1}^{n} B_j$, uniques à isomorphisme d'algèbres près. A chaque B_j correspond un idempotent b_j du centre $Z(kG)$ tel que b_j se projette sur 1 dans B_j et sur zéro dans les autres facteurs. Autrement dit, on a une décomposition orthogonale $1 = \sum_{j=1}^{n} b_j$. On a l'isomorphisme $B_j \simeq kGb_j$. On dit que kGb_j est une algèbre de bloc et b_j est un idempotent de bloc, ou tout simplement un bloc. Les blocs sont très importants, car toute la théorie de la représentation sur k se décompose naturellement sur les algèbres de bloc.

Si une algèbre de bloc kGb est isomorphe à une algèbre de matrices, on dit que b est un bloc de défaut zéro. Et ceci arrive pour tous les blocs de kG si p ne divise pas l'ordre de G. Quand p divise l'ordre de G, on a besoin de considérer des blocs avec des degrés de complexité plus élevés. Le premier invariant qui mesure cette complexité est le groupe de défaut du bloc. C'est un p-sous-groupe de G, unique à conjugaison près, dont la définition sera donnée plus bas. Le groupe de défaut d'un bloc est trivial si et seulement si le bloc est de défaut zéro. A l'autre extrémité se situé le cas où le groupe de défaut d'un bloc b est un p-sous-groupe de Sylow de G. Soit b_0 l'unique bloc qui contient la représentation triviale de dimension 1. Dans ce cas le groupe de défaut de b_0 est un p-sous-groupe de Sylow de G. On appelle b_0 le bloc principal de kG.

On associerra d'une façon naturelle, à chaque bloc de kG, des familles de p-sous-groupes de G et on étudiera les morphismes donnés par les éléments de G entre ces p-sous-groupes de G. Pour cela, on introduit le concept de paire de Brauer. Les fondements de toute la théorie sont parus dans un article d'Alperin et Broué en 1979 [AB].

Définition 4.1.1 *Soit k un corps de caractéristique p et G un groupe fini. Une paire de Brauer sur kG est une paire (P, e), où P est un p-sous-groupe de G et e est un bloc de $kC_G(P)$, c'est-à-dire un idempotent primitif de $Z(kC_G(P))$.*

Le groupe G agit par conjugaison sur l'ensemble des paires de Brauer. En effet, si (P, e) est une paire de Brauer sur G, alors, pour tout $g \in G$, ${}^g e$ est un bloc de $kC_G({}^g P) = k\,{}^g(C_G(P))$. On peut donc définir ${}^g(P, e) := ({}^g P, {}^g e)$. On note $N_G(P, e)$ le normalisateur de la paire (P, e). C'est l'ensemble des éléments $g \in N_G(P)$ tels que $e = {}^g e$. C'est un sous-groupe de $N_G(P)$ qui contient $PC_G(P)$.

Définition 4.1.2 *La catégorie de Brauer de kG est une catégorie ayant comme objets les paires* *de Brauer de kG et comme morphismes, les morphismes entre le paires de Brauer donnés par conjugaison par les éléments de G.*

Sur l'ensemble des paires de Brauer on peut mettre un ordre partiel. Pour pouvoir le faire, on doit définir le morphisme de Brauer. On note $(kG)^P$ l'ensemble d'éléments de kG qui sont fixes par l'action de P.

Définition 4.1.3 *Soit P un p-sous-groupe de G. Le morphisme de Brauer relatif à P est une application surjective k-linéaire*

$$br_P : (kG)^P \longrightarrow kC_G(P)\,,$$

qui envoie tout élément de $C_G(P)$ sur lui-même, vu comme un élément de la base de $kC_G(P)$, et qui envoie sur 0 toute somme d'éléments d'une classe non-triviale de P-conjugaison.

Remarque 4.1.4 Le morphisme de Brauer est bien défini car les éléments de $C_G(P)$ ensemble avec les sommes d'éléments d'une classe non-triviale de P-conjugaison, pour toutes les classes non-triviales de P-conjugaison, forment une k-base de $(kG)^P$.

La relation d'ordre sur les paires de Brauer est engendrée par les relations entre deux paires de Brauer (Q, f) et (P, e), quand $Q \trianglelefteq P$. Dans ce cas, on dit que $(Q, f) \leq (P, e)$ si $f \in (kC_G(Q))^P$ et e apparaît dans la décomposition de $br_P(f)$ dans $kC_G(P)$ et on écrit $(Q, f) \trianglelefteq (P, e)$. Dans le cas général, pour un sous-groupe Q de P, on dit que $(Q, f) \leq (P, e)$ s'il existe une suite sous-normale $Q = Q_0 \trianglelefteq Q_1 \trianglelefteq \ldots \trianglelefteq Q_n = P$ et des blocs f_i de $kC_G(Q_i)$ pour $i = 0, \ldots, n$ tels que $f_0 = f$, $f_n = e$ et $(Q_{i-1}, f_{i-1}) \trianglelefteq (Q_i, f_i)$ pour tout $i = 1, \ldots, n$.

La proposition suivante clarifie la structure du treillis ordonné des paires de Brauer de kG.

Proposition 4.1.5 ([Th], Cor. 40.9, Cor. 40.11) *Soit (P, e) une paire de Brauer de kG et Q un sous-groupe de P.*
a) Il existe un unique bloc f de $kC_G(Q)$ tel que $(P, e) \geq (Q, f)$.
b) L'application $Q \mapsto (Q, f)$ est un isomorphisme entre le poset des sous-groupes de (P, e) et le poset des paires de Brauer contenues dans P (ordonnées par l'inclusion).
c) $N_P(Q, f) = N_P(Q)$.

Donc, si $(Q, f) < (P, e)$ et g est l'unique bloc de $kC_G(N_P(Q))$ tel que $(N_P(Q), g) \leq (P, e)$ alors $(Q, f) \triangleleft (N_P(Q), g) \leq (P, e)$ et $(N_P(Q), g) \neq (Q, f)$.

Définition 4.1.6 *Soit b un bloc de kG. On dit que la paire de Brauer (P, e) est associée à b si $(P, e) \geq (1, b)$.*

Par la proposition précédente, il existe un unique bloc b de kG avec cette propriété, donc la notion est bien définie. La relation d'ordre qu'on a construite sur le treillis des paires de Brauer, nous permet de trouver, pour chaque bloc b de kG, des paires maximales associées à b. Les premiers arguments de ces paires sont les groupes de défaut du bloc b. Mais, on a dit que le groupe de défaut est unique à isomorphisme près. On a même davantage. On a l'équivalent du théorème de Sylow dans le cas de la catégorie de Frobenius de G.

Proposition 4.1.7 ([Th], Prop. 40.13) *Les paires de Brauer maximales de G associées à b sont conjuguées dans G.*

Cette proposition a comme conséquence immédiate le fait que tous les groupes de défaut de b sont conjugués entre eux par des éléments de G.

Soit Q un p-sous-groupe de G. Une propriété utile des p-groupes est le fait que tous les p-sous-groupes maximaux qui normalisent Q sont conjugués sous $N_G(Q)$. Cette propriété reste valide pour les paires de Brauer.

Proposition 4.1.8 ([Th], Prop. 40.15) *Soit (Q, f) une paire de Brauer de kG. Alors*
a) (Q, f) est aussi une paire de Brauer pour $kN_G(Q, f)$. De plus l'ensemble des paires de Brauer de G qui normalisent (Q, f) coïncide avec l'ensemble des paires de Brauer de $N_G(Q, f)$ qui contiennent (Q, f).
b) toutes les paires de Brauer de G, qui sont maximales par rapport à la propriété de normaliser (Q, f), sont conjuguées dans $N_G(Q, f)$.

Donc, de la même façon qu'on pouvait considérer la catégorie de Frobenius de $N_G(Q)$ comme une sous-catégorie de la catégorie de Frobenius de G, on peut maintenant considérer la catégorie de Brauer de $kN_G(Q, f)$ comme une sous-catégorie de la catégorie de Brauer de kG.

Soit (Q, f) une paire de Brauer de kG et soit $N \leq G$. Si $QC_G(Q) \leq N$, alors (Q, f) est aussi une paire de Brauer de kN. En effet, on a $C_N(Q) = C_G(Q)$ et Q est un p-sous-groupe de N.

Définition 4.1.9 *Soit (P, e) une paire maximale de kG et $(Q, f) \leq (P, e)$. Posons $N := N_P(Q)$ et soit f_N l'unique bloc de $kC_G(N)$ tel que $(N, f_N) \leq (P, e)$. On dit que la paire (Q, f) est complètement normalisée dans (P, e) par rapport à kG si (N, f_N) est une paire de Brauer maximale de $kN_G(Q, f)$.*

Dans les années '90, Puig, convaincu de la richesse des p-structures locales, comme la catégorie de Frobenius ou la catégorie de Brauer, en donne une description axiomatique. Les notes dans lesquels Puig introduit ces nouveaux concepts sont restées dans l'état manuscript, jusqu'à récemment, quand l'auteur en a écrit un papier [Pu2]. Les nouveaux concepts que Puig introduit sont les systèmes complets de Frobenius sur un p-groupe P. Commençons par une définition plus générale.

Définition 4.1.10 *Une catégorie sur P est une catégorie dont les objets sont les sous-groupes de P et les morphismes entre les sous-groupes Q et R de P, sont un ensemble de morphismes injectifs de groupe de Q dans R, qui contient les morphismes par conjugaison par les éléments de P.*

Un système complet de Frobenius $\mathcal{F}$ sur P est une catégorie sur P dont les morphismes satisfont les trois axiomes suivants.

A1 *Si Q et R sont des sous-groupes de P, alors, pour tout morphisme $\phi \in \mathcal{F}(Q, R)$ il existe un morphisme $\psi \in \mathcal{F}(\phi(Q), Q)$, tel que $\psi(\phi(u)) = u$, pour tout $u \in Q$.*

Si $Q \leq R$, l'inclusion de Q dans R est aussi dans $\mathcal{F}(Q, R)$ car elle est induite par conjugaison par 1. En particulier les morphismes dans un système complet de Frobenius sur P sont déterminés par les ensembles $\mathcal{F}(Q, P)$, où Q parcourt tous les sous-groupes de P. Une autre remarque importante est le fait que si on a un morphisme $\phi \in \mathcal{F}(Q, R)$ et $T \leq Q$ alors la restriction de ϕ à T est un morphisme de $\mathcal{F}(T, R)$. En effet, soit $\iota \in \mathcal{F}(T, Q)$, l'inclusion de T dans Q. Alors $\phi\iota$ est un morphisme dans $\mathcal{F}(T, R)$. C'est la restriction de ϕ à T.

Avant d'énoncer l'axiome 2 on donne quelques notations. Soit Q un sous-groupe de P. On désigne par $\mathcal{F}(Q) := \mathcal{F}(Q, Q)$ l'ensemble des automorphismes de Q, qui appartiennent à $\mathcal{F}$.

Au vu de l'axiome A1, $\mathcal{F}(Q)$ est un groupe. Soit $R \leq P$ et notons $\mathcal{I}_R(Q) := N_R(Q)/C_R(Q)$ l'ensemble des morphismes de Q, donnés par la conjugaison par les éléments de R. Comme tous les morphismes par conjugaison par les éléments de P sont dans $\mathcal{F}$, il s'ensuit que $\mathcal{I}_R(Q) \leq \mathcal{F}(Q)$. Finalement, posons $\mathcal{I}(Q) := \mathcal{I}_Q(Q)$, qui est le groupe d'automorphismes intérieurs de Q.

A2 *Le groupe $\mathcal{I}(P)$, d'automorphismes intérieurs de P, est un p-sous-groupe de Sylow de $\mathcal{F}(P)$.*

On donne maintenant une définition équivalente aux notions de “complètement normalisé” et “complètement centralisé” dans un p-groupe pour les systèmes complets de Frobenius. Pour le faire en même temps pour les deux notions, on note $N_P^K(Q)$ le K-normalisateur de Q dans P, qui est l'image inverse de K dans $N_P(Q)$, où K est un sous-groupe de $\mathrm{Aut}(Q)$. Pour tout morphisme $\phi \in \mathcal{F}(Q \cdot N_P^K(Q), P)$, on a $\phi(N_P^K(Q)) \leq N_P^{{}^\phi K}(\phi(Q))$, où ${}^\phi K = \{\phi\theta\phi^{-1} | \theta \in K\}$ est un sous-groupe de $\mathrm{Aut}(\phi(Q))$.

Définition 4.1.11 *On dit que Q est K-complètement normalisé dans $\mathcal{F}$ si, pour tout morphisme $\phi \in \mathcal{F}(Q \cdot N_P^K(Q), P)$, on a $\phi(N_P^K(Q)) = N_P^{{}^\phi K}(\phi(Q))$.*

Si $K = 1$ ou $K = \mathrm{Aut}(Q)$, on dira que Q est complètement centralisé ou, respectivement, complètement normalisé dans $\mathcal{F}$. Par ailleurs, on a la propriété suivante.

Lemme 4.1.12 *Soient R un sous-groupe de $Q \cdot N_P^K(Q)$ contenant Q et $\phi \in \mathcal{F}(R, P)$, satisfaisant que, pour tout autre morphisme $\phi' \in \mathcal{F}(R, P)$, on a*

$$|N_P^{{}^{\phi'} K}(\phi'(Q))| \leq |N_P^{{}^\phi K}(\phi(Q))| . \qquad (*)$$

Alors $\phi(Q)$ est ${}^\phi K$-complètement normalisé dans $\mathcal{F}$.

Preuve. Notons $Q' := \phi(Q)$ et $K' := {}^\phi K$. Pour tout morphisme $\psi \in \mathcal{F}(Q' \cdot N_P^{K'}(Q'), P)$, on a le morphisme $\phi' \in \mathcal{F}(R, P)$ qui envoie $v \in R$ sur $\psi(\phi(v))$. Notons $Q'' := \phi'(Q)$ et $K'' := {}^{\phi'} K$. Par $(*)$, on obtient que $|N_P^{K''}(Q'')| \leq |N_P^{K'}(Q')|$. Mais on a toujours $\psi(N_P^{K'}(Q')) \leq N_P^{K''}(Q'')$. Comme

$$|\psi(N_P^{K'}(Q'))| = |N_P^{K'}(Q')| \geq |N_P^{K''}(Q'')| ,$$

on conclut que $\psi(N_P^{K'}(Q')) = N_P^{K''}(Q'')$. Donc Q' est K'-complètement normalisé. □

En particulier, il existe toujours un morphisme $\phi \in \mathcal{F}(Q, P)$ tel que $\phi(Q)$ soit ${}^\phi K$-complètement normalisé dans $\mathcal{F}$.

On peut enfin donner l'axiome qui nous permet d'avoir l'équivalent du théorème de Sylow, dans le cadre des systèmes complets de Frobenius.

A3 *Pour tout sous-groupe Q de P, pour tout sous-groupe K de $\mathrm{Aut}(Q)$ et pour tout morphisme $\phi \in \mathcal{F}(Q, P)$, tel que $\phi(Q)$ est ${}^\phi K$-complètement normalisé dans P, il existe un morphisme $\psi \in \mathcal{F}(Q \cdot N_P^K(Q), P)$ et $\chi \in K$, tels que $\psi(u) = \phi(\chi(u))$ pour tout $u \in Q$.*

Le lien entre l'axiome A3 et le théorème de Sylow est un peu caché, c'est vrai. On voit qu'être K-complètement normalisé pour un sous-groupe Q de P est équivalent à dire que Q est le mieux placé parmi toutes ses images par des morphismes dans $\mathcal{F}(Q, P)$. Le théorème de Sylow est équivalent à dire qu'on peut ramener tout p-sous-groupe d'un groupe G, par conjugaison par un élément de G, à l'intérieur d'un p-sous-groupe de Sylow de G. Dans les systèmes complets de Frobenius, l'axiome A3 nous premet de ramener le K-normalisateur dans P d'une des images de Q par un morphisme de $\mathcal{F}$, à l'intérieur de $N_P^K(Q)$, si Q est K-complètement normalisé dans $\mathcal{F}$.

D'ailleurs, la propriété suivante, qui sera très utile par la suite, nous montre que, derrière le fait qu'un groupe est K-complètement normalisé se cache, quelque part, un p-sous-groupe de Sylow.

Proposition 4.1.13 ([Pu2], Prop. 2.7) *Soit Q un sous-groupe de P et K un sous-groupe de $\mathrm{Aut}(Q)$. Alors Q est K-complètement normalisé dans $\mathcal{F}$ si et seulement si Q est complètement centralisé dans $\mathcal{F}$ et $K \cap \mathcal{I}_P(Q)$ est un p-sous-groupe de Sylow de $K \cap \mathcal{F}(Q)$.*

Preuve. Si Q est complètement centralisé dans $\mathcal{F}$ et $\phi \in \mathcal{F}(Q \cdot N_P^K(Q), P)$, alors la restriction de ϕ à $Q \cdot C_P(Q)$ est dans $\mathcal{F}(Q \cdot C_P(Q), P)$, donc on a $\phi(C_P(Q)) = C_P(\phi(Q))$. Si, de plus, $K \cap \mathcal{I}_P(Q) = N_P^K(Q)/C_P(Q)$ est un p-sous-groupe de Sylow de $K \cap \mathcal{F}(Q)$, on obtient

$$\begin{aligned}|N_P^K(Q)| &= |C_P(Q)| \cdot |K \cap \mathcal{I}_P(Q)| = |C_P(Q)| \cdot |K \cap \mathcal{F}(Q)|_p = \\ &= |C_P(\phi(Q))| \cdot |{}^{\phi}K \cap \mathcal{F}(\phi(Q))|_p \geq |C_P(\phi(Q))| \cdot |{}^{\phi}K \cap \mathcal{I}_P(\phi(Q))| = |N_P^{\phi K}(\phi(Q))|\,.\end{aligned}$$

où par $|G|_p$ on a noté l'ordre d'un p-sous-groupe de Sylow de G. Mais on a toujours que $\phi(N_P^K(Q)) \leq N_P^{\phi K}(\phi(Q))$, ce qui entraîne $|N_P^K(Q)| = |\phi(N_P^K(Q))| \leq |N_P^{\phi K}(\phi(Q))|$. Ainsi on obtient $\phi(N_P^K(Q)) = N_P^{\phi K}(\phi(Q))$ et donc Q est K-complètement normalisé dans $\mathcal{F}$.

Supposons maintenant que Q est K-complètement normalisé dans $\mathcal{F}$. Premièrement, on va prouver que Q est complètement centralisé dans $\mathcal{F}$. Soit $\phi \in \mathcal{F}(Q \cdot C_P(Q), P)$. Par l'axiome A1, il existe $\phi^{-1} \in \mathcal{F}(\phi(Q), Q)$ tel que $\phi^{-1}\phi(u) = u$ pour tout $u \in Q$. Maintenant, le groupe Q est K-complètement normalisé, donc, par l'axiome A3, appliqué à ϕ^{-1}, on obtient qu'il existe $\rho \in \mathcal{F}(\phi(Q) \cdot N_P^{\phi K}(\phi(Q)), P)$ et $\chi \in {}^{\phi}K$ tels que $\rho(v) = \phi^{-1}(\chi(v))$ pour tout $v \in \phi(Q)$. On a $\rho(C_P(\phi(Q))) \leq C_P(\rho\phi(Q)) = C_P(Q)$, car $\rho(\phi(u)) = \phi^{-1}(\chi(\phi(u)) \in Q$ pour tout $u \in Q$. Ceci donne $|C_P(\phi(Q))| \leq |C_P(Q)|$, donc $\phi(C_P(Q)) = C_P(\phi(Q))$. Comme ce résultat est vrai pour tout $\phi \in \mathcal{F}(Q \cdot C_P(Q), P)$, on obtient que Q est complètement centralisé dans $\mathcal{F}$.

On montre maintenant, par récurrence sur l'indice $|P : Q|$, que $K \cap \mathcal{I}_P(Q)$ est un p-sous-groupe de Sylow de $K \cap \mathcal{F}(Q)$. Pour $P = Q$, par l'axiome A2 le groupe $\mathcal{I}(P)$ est un p-sous-groupe de Sylow de $\mathcal{F}(P)$ et, comme $\mathcal{I}(P)$ est un sous-groupe normal de $\mathrm{Aut}(P)$, on obtient que $K \cap \mathcal{I}(P)$ est un p-sous-groupe de Sylow de $K \cap \mathcal{F}(P)$ pour tout $K \leq \mathrm{Aut}(P)$.

Soit maintenant $Q < P$. Prouvons notre assertion premièrement dans le cas où $K = \mathrm{Aut}(Q)$, autrement dit, Q est complètement normalisé. Posons $R := N_P(Q)$ et soit J le sous-groupe de $\mathrm{Aut}(R)$ qui stabilise Q. Il est immédiat que $N_P^J(R) = N_P(Q) \cap N_P(R) = R$. De plus R est J-complètement normalisé dans $\mathcal{F}$. En effet, comme Q est complètement normalisé, pour tout $\phi \in \mathcal{F}(R, P)$ on a $\phi(R) = N_P(\Phi(Q))$. Par ailleurs ${}^{\phi}J$ est le sous-groupe de $\mathrm{Aut}(\phi(R))$ qui stabilise $\phi(Q)$ et donc $N_P^{\phi J}(\phi(R)) = N_P(\phi(Q)) \cap N_P(\phi(R)) = \phi(R)$. On obtient ainsi que, pour tout $\phi \in \mathcal{F}(R \cdot N_P^J(R), P) = \mathcal{F}(R, P)$, on a $N_P^{\phi J}(\phi(R)) = \phi(R) = \phi(N_P^J(R))$, donc R est J-complètement normalisé dans $\mathcal{F}$. Comme Q est un sous-groupe propre de R, par hypothèse de récurrence, on obtient que $J \cap \mathcal{I}_P(R) = \mathcal{I}_R(R)$ est un p-sous-groupe de Sylow de $J \cap \mathcal{F}(R)$.

On a clairement $\mathcal{I}_P(Q) = \mathcal{I}_R(Q)$. Pour montrer que $\mathcal{I}_R(Q)$ un p-sous-groupe de Sylow de $\mathcal{F}(Q)$, il suffit de démontrer que $\mathcal{I}_R(Q)$ est un p-sous-groupe de Sylow de $N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$, car, par la remarque 1.1.6 si un p-sous-groupe d'un groupe fini G est un p-sous-groupe de Sylow de son normalisateur, il est un p-sous-groupe de Sylow de G.

Montrons maintenant que $\mathcal{I}_R(Q)$ est un p-sous-groupe de Sylow de $N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$. Pour ceci, on va montrer que tout morphisme $\phi \in N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$ peut être relevé dans $J \cap \mathcal{F}(R)$, ce qui veut dire que le morphisme de groupes $f : J \cap \mathcal{F}(R) \longrightarrow N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$, donné par la restriction des morphismes dans $J \cap \mathcal{F}(R)$ à Q, est surjectif. Comme, de plus, $f(\mathcal{I}(R)) = \mathcal{I}_R(Q)$ il s'ensuit que $\mathcal{I}_R(Q)$ est un p-sous-groupe de Sylow de $N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$, car l'image d'un p-sous-groupe de Sylow de $J \cap \mathcal{F}(R)$ par le morphisme surjectif f est un p-sous-groupe de Sylow de $N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$.

On va montrer que tout morphisme dans $N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$ peut être relevé dans $J \cap \mathcal{F}(R)$. Soit $\phi \in N_{\mathcal{F}(Q)}(\mathcal{I}_R(Q))$. Par choix de ϕ on a $\phi(Q) = Q$ et ${}^{\phi}(\mathcal{I}_R(Q)) = \mathcal{I}_R(Q)$. De plus, R contient $Q \cdot C_P(Q)$ donc $N_P^{\mathcal{I}_R(Q)}(Q) = R$. On a déjà vu que Q est complètement centralisé dans $\mathcal{F}$. On a aussi que Q est $\mathcal{I}_R(Q)$-complètement normalisé dans $\mathcal{F}$. En effet, pour tout morphisme $\eta \in \mathcal{F}(Q \cdot N_P^{\mathcal{I}_R(Q)}(Q), P) = \mathcal{F}(R, P)$ on a $C_P(\eta(Q)) = \eta(C_P(Q))$ car Q est complètement normalisé et donc $C_P(\eta(Q)) \leq \eta(R)$. Ceci entraîne que $\eta(Q)C_P(\eta(Q)) \leq \eta(R)$ et, par conséquent, $N_P^{\mathcal{I}_{\eta(R)}(\eta(Q))}(\eta(Q)) = \eta(R) = \eta(N_P^{\mathcal{I}_R(Q)}(Q))$ et donc Q est $\mathcal{I}_R(Q)$-complètement normalisé dans $\mathcal{F}$. Par l'axiome A3 appliqué au morphisme ϕ, on obtient qu'il existe un morphisme $\psi \in \mathcal{F}(Q \cdot N_P^{\mathcal{I}_R(Q)}(Q), P) = \mathcal{F}(R, P)$ et $\chi \in \mathcal{I}_R(Q)$ tels que $\psi(u) = \phi\chi(u)$ pour tout $u \in Q$. Soit $\widetilde{\chi}$ un relevé de χ dans $\mathcal{I}_R(R)$. On a alors que $\psi\widetilde{\chi}^{-1}$ est un relevé de ϕ dans $\mathcal{F}(R, P)$. En fait $\psi\widetilde{\chi}^{-1} \in \mathcal{F}(R)$. En effet, ψ et $\widetilde{\chi}$ normalisent $\mathcal{I}_R(Q)$ et $\psi\widetilde{\chi}^{-1}(C_P(Q)) = C_P(\psi\widetilde{\chi}^{-1}(Q))) = C_P(Q)$. Donc, $R/C_P(Q) = \mathcal{I}_R(Q) = {}^{\psi\widetilde{\chi}^{-1}}\mathcal{I}_R(Q) = \psi\widetilde{\chi}^{-1}(R)/C_P(Q)$ ce qui entraîne que $R = \psi\widetilde{\chi}^{-1}(R)$ et, ainsi, $\psi\widetilde{\chi}^{-1} \in \mathcal{F}(R)$. Ceci fini la preuve dans le cas où $K = \mathrm{Aut}(Q)$.

Dans le cas général, soit $\theta \in \mathcal{F}(Q, P)$ tel que $\theta(Q)$ est complètement normalisé dans $\mathcal{F}$. On a vu qu'un tel morphisme θ existe toujours. Maintenant $\theta(Q)$ est complètement normalisé, donc par la preuve dans le cas $K = \mathrm{Aut}(Q)$, appliquée à $\theta(Q)$ à la place de Q, on obtient que $\mathcal{I}_P(\theta(Q))$ est un sous-groupe de Sylow de $\mathcal{F}(\theta(Q))$. Comme ${}^{\theta}(K \cap \mathcal{F}(Q))$ est un sous-groupe de ${}^{\theta}(\mathcal{F}(Q)) = \mathcal{F}(\theta(Q))$, il existe $\rho \in \mathcal{F}(\theta(Q))$ tel que un p-sous-groupe de Sylow de ${}^{\rho\theta}(K \cap \mathcal{F}(Q))$ est contenu dans $\mathcal{I}_P(\theta(Q))$. Donc ${}^{\rho\theta}K \cap \mathcal{I}_P(\theta(Q))$ est un p-sous-groupe de Sylow de ${}^{\rho\theta}(K \cap \mathcal{F}(Q))$.

Si on prend, maintenant, $\theta' := \rho\theta$, $Q' := \theta(Q)$, $K' := {}^{\theta'}K$ et on applique l'axiome A3 à θ'^{-1}, en tenant compte que Q est K-complètement normalisé, il existe $\psi \in \mathcal{F}(Q' \cdot N_P^{K'}(Q'), P)$ et $\chi' \in K'$ tels que $\psi(u) = \theta'^{-1}(\chi'(u))$ pour tout $u \in Q'$. Soit $\chi := {}^{\theta'^{-1}}\chi'$, qui est un élément de K. On a alors $\psi^{-1} = \theta'\chi^{-1}$ ce qui implique que ${}^{\psi^{-1}}K = K'$. Mais $\psi(N_P^{K'}(Q')) \leq N_P^K(Q)$ et, comme Q' est complètement centralisé, $\psi(C_P(Q')) = C_P(Q)$, donc $\psi(K' \cap \mathcal{I}_P(Q')) \leq K \cap \mathcal{I}_P(Q)$. De plus, $K' \cap \mathcal{I}_P(Q')$ est un p-sous-groupe de Sylow de $K' \cap \mathcal{F}(Q')$ et $\phi(K' \cap \mathcal{F}(Q')) = K \cap \mathcal{F}(Q)$. On en déduit que $K \cap \mathcal{I}_P(Q)$ est un p-sous-groupe de Sylow de $K \cap \mathcal{F}(Q)$. $\square$

Soit Q un sous-groupe de P et K un sous-groupe de $\mathrm{Aut}(Q)$. On peut définir, à partir de $\mathcal{F}$, une catégorie $N_{\mathcal{F}}^K(Q)$ sur $N_P^K(Q)$, dont les objets sont les sous-groupes de $N_P^K(Q)$ et les morphismes entre deux sous-groupes R et T de $N_P^K(Q)$ sont les morphismes $\phi \in \mathcal{F}(R, T)$, tels qu'il existe un morphisme $\psi \in \mathcal{F}(Q \cdot R, Q \cdot T)$ et $\chi \in K$ tel que $\chi(u) = \psi(u)$ pour tout $u \in Q$ et $\psi(v) = \phi(v)$ pour tout $v \in R$; autrement dit, tous les morphismes qui se prolongent à $Q \cdot R$ et tels que cette prolongation agisse sur Q par un morphisme de K. Dans le cas où $K = \mathrm{Aut}(Q)$, on note cette catégorie, tout simplement, $N_{\mathcal{F}}(Q)$.

Proposition 4.1.14 ([Pu2], Prop. 2.8) *Soit $\mathcal{F}$ un système complet de Frobenius sur P. Si $Q \leq P$ est K-complètement normalisé dans $\mathcal{F}$, alors, $N_{\mathcal{F}}^K(Q)$ est un système complet de Frobenius sur $N_P(Q)$.*

Pour la preuve de cette proposition on aura besoin du lemme technique suivant :

Lemme 4.1.15 ([Pu2], Lemma 2.9) *Soit $\mathcal{F}$ un système complet de Frobenius sur P, Q un sous-groupe de P et K un sous-groupe de $\mathrm{Aut}(Q)$. Soient R un sous-groupe de $N_P^K(Q)$, L un sous-groupe de $Aut(R)$ et M un sous-groupe de $\mathrm{Aut}(Q \cdot R)$ qui stabilise Q et R et agit sur eux par des morphismes dans K, respectivement L.*

Alors $N_P^M(Q \cdot R) = N_P^K(Q) \cap N_P^L(R)$ et, si R est complètement normalisé dans $N_{\mathcal{F}}^K(Q)$, le groupe $Q \cdot R$ est M-complètement normalisé dans $\mathcal{F}$.

Preuve. La première égalité est immédiate car on a $u \in N_P^M(Q \cdot R)$ si et seulement si $u \in P$ stabilise Q et R et u agit sur Q, respectivement R par des éléments de K, respectivement L ce qui est équivalent avec $u \in N_P^K(Q)$, respectivement $u \in N_P^L(R)$, ou, autrement dit, avec $u \in N_P^K(Q) \cap N_P^L(R)$. On remarque que ceci est vrai indépendamment de l'existence de $\mathcal{F}$.

Pour la deuxième partie du lemme, posons $T := Q \cdot R$, $P' := N_P^K(Q)$ et $\mathcal{F}' := N_{\mathcal{F}}^K(Q)$. Soit $\phi \in \mathcal{F}(T \cdot N_P^M(T), P)$ et on veut montrer que $\phi(N_P^M(Q)) = N_P^{\phi M}(\phi(T))$. Notons $Q' := \phi(Q)$, $T' := \phi(T)$ et $K' := {}^{\phi}K$. Maintenant on a $\phi|_Q \in \mathcal{F}(Q, P)$, donc, par l'axiome A3 appliqué à ϕ^{-1}, en tenant compte que Q est K-complètement normalisé dans $\mathcal{F}$, il existe $\psi \in \mathcal{F}(Q' \cdot N_P^{K'}(Q'), P)$ et $\chi' \in \mathcal{F}(Q')$ tels que $\psi(u) = \phi^{-1}\chi'(u)$ pour tout $u \in Q'$. En particulier $\psi(N_P^{K'}(Q)') \leq N_P^K(Q)$. Maintenant on a $\phi(T \cdot N_P^M(T)) \leq \phi(T) \cdot N_P^{\phi M}(T') \leq Q' \cdot N_P^{K'}(Q')$ donc, si on note $\eta := \psi\phi$, on a $\eta \in \mathcal{F}(T \cdot N_P^M(T), QP') = \mathcal{F}(Q \cdot R \cdot N_P^M(T), QP')$. De plus $\eta(R \cdot N_P^M(T)) \leq P'$, ce qui implique que $\eta|_{R \cdot N_P^M(T)} \in \mathcal{F}'(R \cdot N_P^M(T), P')$, par la définition même de $\mathcal{F}'$.

Par un calcul simple $N_P^M(T) = N_P^K(Q) \cap N_P^L(R) = N_{P'}^L(R)$ (1) et en utilisant le fait que R est L-complètement normalisé dans $\mathcal{F}'$ on obtient $\eta(N_{P'}^L(R)) = N_{P'}^{\eta L}(\eta(R))$ (2). D'autre part on remarque que $\eta(Q) = Q$ et ${}^{\eta}K = K$ et ${}^{\eta}M$ est un sous-groupe du groupe d'automorphismes de $Q \cdot \eta(R)$ qui stabilise Q et $\eta(R)$ et agit Q, respectivement $\eta(R)$ par des morphismes de K, respectivement $\eta(L)$. Donc, $N_P^{\eta M}(Q \cdot \eta(R)) = N_P^K(Q) \cap N_P^{\eta L}(\eta(R)) = N_{P'}^{\eta L}(\eta(R))$ (3), par la première partie du lemme. De (1), (2) et (3) on déduit que $\eta(N_P^M(T)) = N_P^{\eta M}(Q \cdot \eta(R))$. Donc on a

$$\psi(\phi(N_P^M(T))) = \eta(N_P^M(T)) = N_P^{\eta M}(Q \cdot \eta(R)) \geq \psi(N_P^{\phi M}(\phi(T)))$$

On en déduit que $|\phi(N_P^M(T))| \geq |N_P^{\phi M}(\phi(T))|$. Maintenant, comme $\phi(N_P^M(T)) \leq N_P^{\phi M}(\phi(T))$, on obtient que $\phi(N_P^M(T)) = N_P^{\phi M}(\phi(T))$.

Ceci est vrai pour tout $\phi \in \mathcal{F}(T \cdot N_P^M(T), P)$, donc T est M-complètement centralisé dans $\mathcal{F}$. $\square$

Preuve de la proposition 4.1.14. Comme dans le lemme précédent, posons $\mathcal{F}' := N_{\mathcal{F}}^K(Q)$ et $P' := N_P^K(Q)$. On va vérifier les axiomes A1, A2 et A3 pour $\mathcal{F}'$. L'axiome $A1$ est trivialement satisfait.

Vérifions maintenant l'axiome A2. Clairement P' est complètement normalisé dans $\mathcal{F}'$, et en prenant N le sous-groupe de $\mathrm{Aut}(Q \cdot P')$ qui stabilise Q et P' et agit sur Q par des morphismes de K, comme Q est K-complètement normalisé, par le lemme 4.1.15, le groupe $Q \cdot P'$ est N-complètement normalisé dans $\mathcal{F}$. Par la proposition 4.1.13, le groupe $N \cap \mathcal{I}_P(Q \cdot P')$ est un p-sous-groupe de Sylow de $N \cap \mathcal{F}$. Mais, par la définition de $\mathcal{F}'$, tout morphisme de $\mathcal{F}'(P')$ se relève en un morphisme de $\mathcal{F}(Q \cdot P') \cap N$. Donc le morphisme de restriction $N \cap \mathcal{F}(Q \cdot P') \to \mathcal{F}'(P')$ est surjectif. De plus ce morphisme envoie $N \cap \mathcal{I}_P(Q \cdot P')$ surjectivement sur $\mathcal{I}(P')$. Ainsi $\mathcal{I}(P')$ est un p-sous-groupe de Sylow de $\mathcal{F}'(P')$ et l'axiome A2 est satisfait.

Pour vérifier l'axiome A3, soit $R \leq P'$, soit L un sous-groupe de $\mathrm{Aut}(R)$ et $\phi \in \mathcal{F}'(R, P')$ tel que $\phi(R)$ soit ${}^{\phi}L$-complètement normalisé dans $\mathcal{F}'$. Par la construction de $\mathcal{F}'$ on a qu'il existe $\psi \in \mathcal{F}(Q \cdot R, Q \cdot P')$ et $\chi \in K$ tels que $\psi(v) = \phi(v)$ pour tout $v \in R$ et $\psi(u) = \chi(u)$ pour tout $u \in Q$. Reprenons les notations du lemme 4.1.15 : soit $T := Q \cdot R$ et M le sous-groupe de $\mathrm{Aut}(T)$ qui stabilise Q et R et agit sur Q, respectivement R par des morphismes de K, respectivement L. Comme Q est K-complètement normalisé dans $\mathcal{F}$ et $\psi(R)$ est ${}^{\psi}L$-complètement normalisé dans $\mathcal{F}'$, par le lemme 4.1.15, on obtient que $\psi(T)$ est M-complètement normalisé dans $\mathcal{F}$.

On applique l'axiome A3 à $\psi \in \mathcal{F}(T, P)$ et on obtient qu'il existe $\rho \in \mathcal{F}(T \cdot N_P^M(T), P)$ et $\nu \in M$ tels que $\rho(w) = \psi(\nu(w))$, pour tout $w \in T$. En partiqulier on a $\rho(u) = \psi\nu(u)$ et donc ρ détermine un élément de K, car c'était déjà le cas pour ψ et ν. Maintenant R et $N_P^M(T)$ sont des sous-groupes de $N_P^K(Q)$ et comme ρ détermine un élément de K, les images $\rho(R)$ et $\rho(N_P^M(T))$ restent des sous-groupes de $N_P^K(Q)$. D'autre part, l'action de ν sur R détermine un élément λ de L et, par le lemme 4.1.15, on a $N_P^M(T) = N_{P'}^L(R)$. On obtient, pas conséquent, que la restriction de ρ à $R \cdot N_{P'}^L(R)$ est un morphisme de $\mathcal{F}'(R \cdot N_{P'}^L(R), P')$. De plus on a $\rho(v) = \psi(\nu(v)) = \phi(\lambda(v))$ pour tout $v \in R$, donc l'axiome A3 est aussi satisfait. □

Dans ce qui suit on montrera que la catégorie de Brauer au-dessous d'une paire maximale est un système complet de Frobenius.

Proposition 4.1.16 *Soit G un groupe fini et k un corps de caractéristique p. Soit (P, e) une paire de Brauer maximale de kG. Alors la catégorie de Brauer au-dessous de (P, e) est un système complet de Frobenius sur P.*

Preuve. L'axiome A1 est trivialement satisfait. Pour l'axiome A2, il faut montrer que $P/Z(P)$ est un sous-groupe de Sylow de $N_G(P, e)/C_G(P)$. Autrement dit, il faut montrer que l'ordre de $N_G(P, e)/PC_G(P)$ n'est pas divisible par p. Mais ceci est une conséquence directe du premier théorème de Brauer [Th, Thm. 40.14].

Enfin, vérifions l'axiome A3. Soit (Q, f) une paire de Brauer K-complètement normalisée dans (P, e). Posons $N := N_P^K(Q)$ et soient f_N l'unique bloc de $kC_G(Q \cdot N)$ tel que $(N, f_N) \leq (P, e)$ et b l'unique bloc de kG tel que $(1, b) \leq (P, e)$. On va démontrer premièrement que $(Q \cdot N, f_N)$ est une paire de Brauer maximale de $k(Q \cdot N_G^K(Q, f))$.

Soit (S, f_S) une paire de Brauer de $k(Q \cdot N_G^K(Q, f))$ contenant $(Q \cdot N, f_N)$. De plus, on a $C_G(S) = C_{N_G^K(Q,f)}(S)$ car $C_G(S) \leq C_G(Q) \leq N_G^K(Q, f)$, donc (S, f_S) est aussi une paire de Brauer pour G. Soit (P', e') une paire maximale de Brauer de kG contenant (S, f_S). Maintenant les paires (P, e) et (P', e') contiennent les deux (Q, f) donc elles sont associées à b. Par la proposition 4.1.7 il existe un élément $g \in G$ tel que $(P, e) = {}^{g}(P', e')$. Par conséquent, on a ${}^{g}(S, f_S) \leq (P, e)$ et la conjugaison par g nous donne un morphisme de $Q \cdot N$ dans P. Comme ${}^{g}S \leq {}^{g}Q \cdot N_G^{{}^{g}K}({}^{g}Q, {}^{g}f)$ en utilisant que (Q, f) est K-complètement normalisée on obtient que ${}^{g}S = {}^{g}(Q \cdot N)$. On a donc $Q \cdot N = S$ et $(Q \cdot N, f_N)$ est une paire maximale de $k(Q \cdot N_G^K(Q, f))$.

Mettons-nous dans les hypothèses de l'axiome A3. Soit (Q, f), ${}^{g}(Q, f) \leq (P, e)$ tels que ${}^{g}(Q, f)$ soit ${}^{g}K$-complètement normalisé dans P. Soient $(Q \cdot N, f_N)$ construite comme avant, $N' := N_P^{{}^{g}K}({}^{g}Q)$ et $f_{N'}$ l'unique bloc de $kC_G({}^{g}Q \cdot N')$ tel que $({}^{g}Q \cdot N', f_{N'}) \leq (P, e)$. On a vu que dans ce cas $({}^{g}Q \cdot N', f_{N'})$ est une paire de Brauer maximale de $k({}^{g}Q \cdot N_G^{{}^{g}K}({}^{g}Q, {}^{g}f))$. Mais ${}^{g}(Q \cdot N, f_N)$ est aussi une paire de Brauer de $k({}^{g}Q \cdot N_G^{{}^{g}K}({}^{g}Q, {}^{g}f))$. Cette paire de Brauer est contenue dans une paire maximale, donc, par la proposition 4.1.7, il existe $h \in {}^gQ \cdot N_G^{{}^gK}({}^gQ, {}^gf)$ tel que ${}^{hg}(Q \cdot N) \leq {}^gQ \cdot N'$. En passant au quotient par ${}^gQ$, on en déduit qu'il existe un élément $\overline{h} \in N_G^{{}^gK}({}^gQ, {}^gf)/N_{{}^gQ}^{{}^gK}({}^gQ)$, tel que ${}^{\overline{h}}N/N_{{}^gQ}^{{}^gK}({}^gQ) \leq N'/N_{{}^gQ}^{{}^gK}({}^gQ)$. En prenant h' un représentant modulo $N_{{}^gQ}^{{}^gK}({}^gQ)$ de $\overline{h}$ dans $N_G^{{}^gK}({}^gQ, {}^gf)$, on obtient que $\mathrm{conj}(h'g)$ est un morphisme de $Q \cdot N$ dans P tel que

$$\mathrm{conj}(h'g)(u) = \mathrm{conj}(g)\mathrm{conj}(g^{-1}h'g)(u) \qquad \text{pour tout } u \in Q\,.$$

Ceci est la forme voulue dans l'axiome A3 car on a $\mathrm{conj}(g^{-1}h'g) \in K$. Ainsi l'axiome A3 est aussi satisfait.

On peut donc conclure que la sous-catégorie pleine de Brauer, au-dessous d'une paire maximale (P, e), est un système complet de Frobenius sur P. □

Comme la sous-catégorie pleine au-dessous d'un p-sous-groupe de Sylow de G de la catégorie de Frobenius $F_p(G)$ est équivalente à la sous-catégorie de Brauer au-dessous d'une paire maximale associée au bloc principal, la première est aussi un système complet de Frobenius sur le p-sous-groupe de Sylow.

4.2 Le théorème d'Alperin

Dans cette section on donne la preuve du théorème d'Alperin, dans le cadre des systèmes complets de Frobenius. Les idées principales de la preuve sont reprises de [Th]. Dans toute la section P est un p-groupe fini, Q un sous-groupe de P et $\mathcal{F}$ un système complet de Frobenius sur P.

Avant d'énoncer le théorème, juste deux définitions.

Définition 4.2.1 *Soit Q un sous-groupe de P. On dit que Q est centrique si $C_P(\phi(Q)) \subset \phi(Q)$, pour tout $\phi \in \mathcal{F}(Q, P)$.*

Remarque 4.2.2 Un sous-groupe centrique de P est complètement centralisé dans $\mathcal{F}$. En effet, pour tout morphisme $\phi \in \mathcal{F}(Q \cdot C_P(Q), P) = \mathcal{F}(Q, P)$, on a

$$\phi(C_P(Q)) = \phi(Z(Q)) = Z(\phi(Q)) = C_P(\phi(Q))\,.$$

Définition 4.2.3 *Soit Q un sous-groupe de P. On dit que Q est un sous-groupe essentiel de $\mathcal{F}$ si Q est centrique et $\mathcal{S}_p(\mathcal{F}(Q))_{>\mathcal{I}(Q)}$ est non-connexe.*

Remarque 4.2.4 Les mêmes familles de p-groupes, trouvés au chapitre 2, qui ne peuvent jamais être réalisés comme p-sous-groupes essentiels dans un groupe fini, ne peuvent pas non plus être réalisés comme p-sous-groupes essentiels dans un système complet de Frobenius. Et la raison est le fait que, si Q est un de ces p-groupes, alors $\mathcal{S}_p(\mathcal{F}(Q))_{>\mathcal{I}(Q)}$ est connexe pour tout système complet de Frobenius $\mathcal{F}$, étant donné que $\mathcal{F}(Q)$ est un sous-groupe de $\mathrm{Aut}(Q)$, donc il aura un unique p-sous-groupe de Sylow.

Si $\phi \in \mathcal{F}(P)$, on dit que ϕ est un morphisme maximal ; si $\phi \in \mathcal{F}(E)$, où E est un sous-groupe essentiel de $\mathcal{F}$, on dit que ϕ est un morphisme essentiel. On est maintenant en mesure d'énoncer le théorème d'Alperin, dans le cadre des systèmes complets de Frobenius.

Théorème 4.2.5 *Tout morphisme $\phi \in \mathcal{F}(Q,P)$ peut être écrit comme la composition de restrictions à Q de morphismes essentiels, suivies d'un morphisme maximal. Plus précisément, il existe un nombre naturel $n \geq 0$ et, pour tout $1 \leq i \leq n$, des sous-groupes essentiels E_i de $\mathcal{F}$ complètement normalisés dans $\mathcal{F}$ et des morphismes $\psi_i \in \mathcal{F}(E_i)$, $\psi_{n+1} \in \mathcal{F}(P)$ tels qu'on a*

$$\phi(u) = \psi_{n+1}\psi_n \dots \psi_1(u), \text{ pour tout } u \in Q\,.$$

Preuve. La preuve se fait par induction sur l'indice $|P : Q|$. Si $|P : Q| = 1$, alors $P = Q$ et $\phi \in \mathcal{F}(P)$. Supposons maintenant que $|P : Q| > 1$. Soit $\psi \in \mathcal{F}(Q,P)$, tel que $\psi(Q)$ soit complètement normalisé dans $\mathcal{F}$.

Maintenant $\psi \in \mathcal{F}(Q,\psi(Q))$ et $\psi\phi^{-1} \in \mathcal{F}(\phi(Q),\psi(Q))$ ce sont des morphismes qui ont comme but $\psi(Q)$, donc un sous-groupe de P complètement normalisé dans $\mathcal{F}$. Donc il suffit de trouver la décomposition de l'énoncé pour un isomorphisme qui a comme but un sous-groupe de P complètement normalisé dans $\mathcal{F}$ car si on trouve cette décomposition pour ψ et pour $\psi\phi^{-1}$, on la trouve pour ϕ. Il est vrai que les morphismes essentiels et maximaux peuvent ne pas se trouver dans le bon ordre, mais on verra à la fin de la preuve qu'on peut interchanger les places des morphismes maximaux et essentiels.

Donc on s'est réduit au cas où on veut décomposer un morphisme $\psi \in \mathcal{F}(Q,P)$, tel que $\psi(Q)$ est complètement normalisé dans $\mathcal{F}$. Par l'axiome A3 appliqué à ψ, on a un morphisme $\rho \in \mathcal{F}(N_P(Q),P)$ et $\chi \in \mathcal{F}(Q)$ tel que $\rho|_Q = \psi\chi$. Maintenant $|P : N_P(Q)| < |P : Q|$ donc, par récurrence, ρ est de la forme voulue. Pour pouvoir décomposer ψ, il suffit donc de décomposer le morphisme $\psi\chi\psi^{-1} \in \mathcal{F}(\psi(Q))$.

Ainsi, on s'est réduit, quitte à changer de notation, au cas où il faut décomposer $\chi \in \mathcal{F}(Q)$ pour un sous-groupe Q de P complètement normalisé dans $\mathcal{F}$. Par la proposition 4.1.13, Q est complètement centralisé dans $\mathcal{F}$, et, en appliquant l'axiome A3 à χ, il existe $\chi' \in \mathcal{F}(QC_P(Q),P)$ tel que $\chi'(u) = \chi(u)$, pour tout $u \in Q$. Si Q n'est pas centrique, alors $|P : Q| > |P : QC_P(Q)|$ et on obtient la décomposition de χ' par récurrence. On peut donc supposer que Q est centrique.

Si Q est un sous-groupe essentiel de $\mathcal{F}$, alors $\chi \in \mathcal{F}(Q)$ et χ est de la forme voulue, car Q est complètement normalisé dans $\mathcal{F}$. Sinon, $\mathcal{S}_p(\mathcal{F}(Q))_{>\mathcal{I}(Q)}$ est connexe. Soit $T = \mathcal{I}_P(Q)$. C'est un p-sous-groupe de Sylow de $\mathcal{F}(Q)$, par la proposition 4.1.13, car Q est complètement normalisé dans $\mathcal{F}$. Par la connexité de $\mathcal{S}_p(\mathcal{F}(Q))_{>\mathcal{I}(Q)}$, il existe un chemin

$$T \geq S_1 \leq {}^{\chi_1}T \geq S_2 \leq \dots {}^{\chi_{n-1}}T \geq S_n \leq {}^{\chi}T$$

entre T et ${}^{\chi}T$, où $\chi_i \in \mathcal{F}(Q)$ et $S_i > \mathcal{I}(Q)$ pour tout $i = 1,\dots,n$. Autrement dit, en posant $\chi_0 = \mathrm{id}$ et $\chi_n = \chi$, on a, pour tout $1 \leq i \leq n-1$, ${}^{\chi_{i-1}}S_i \leq T \geq {}^{\chi_i}S_i$. Posons $K := {}^{\chi_{i-1}}S_i$. Comme $K \leq T = \mathcal{I}_P(Q)$, on obtient $K \cap \mathcal{I}_P(Q) = K = K \cap \mathcal{F}(Q)$, donc, par la proposition 4.1.13, Q est K-complètement normalisé. Par l'axiome A3, appliqué à $\chi_i\chi_{i-1}^{-1}$, il existe $\rho \in \mathcal{F}(QN_P^K(Q),P)$ et $\sigma \in K$ tel que $\chi_i\chi_{i-1}^{-1}\sigma(u) = \rho(u)$ pour tout $u \in Q$. Comme $\mathcal{I}(Q)$ est un sous-groupe propre de K, le groupe Q est un sous-groupe propre de $N_P^K(Q)$ et, donc, σ est la restriction d'un morphisme par conjugaison par un élément de $\mathcal{F}(N_P^K(Q))$ (donné par la conjugaison par une préimage de σ dans $N_P^K(Q)$). On arrive à décomposer, par récurrence, ρ et σ comme dans l'énoncé du théorème. Ceci entraîne qu'on arrive à décomposer $\chi_i\chi_{i-1}^{-1}$. Donc

$$\chi = (\chi_n\chi_{n-1}^{-1})(\chi_{n-1}\chi_{n-2}^{-1})\dots(\chi_2\chi_1^{-1})$$

se décompose aussi.

Il nous reste à voir que la composée d'un morphisme maximal avec un morphisme essentiel est égale à la composée d'un morphisme essentiel avec un morphisme maximal, ce qui fait qu'on peut mettre tous les morphismes maximaux à gauche dans la décomposition. En effet, si $\nu \in \mathcal{F}(E)$, où E sous-groupe essentiel de $\mathcal{F}$, complètement normalisé dans $\mathcal{F}$ et $\theta \in \mathcal{F}(P)$, on a $\nu\theta(u) = \theta(\theta^{-1}\nu\theta)(u)$, pour tout $u \in \theta^{-1}(E)$ où $(\theta^{-1}\nu\theta) \in \mathcal{F}(\theta^{-1}(E))$ et $\theta^{-1}(E)$ est un sous-groupe essentiel de $\mathcal{F}$, complètement normalisé dans $\mathcal{F}$, car l'image de E par un morphisme $\mu \in \mathcal{F}(R,P)$, pour tout R contenant $N_P(E)$, est un groupe complètement normalisé dans $\mathcal{F}$. En effet on a $\mu(N_P(E)) = N_P(\mu(E))$ car E est complètement normalisé, donc $|N_P(\mu(E))|$ est maximal. □

4.3 Une généralisation du théorème de Gilotti et Serena

Comme dans la section précédente, $\mathcal{F}$ est un système complet de Frobenius sur un p-groupe P. La notion de contrôle de p-fusion dans le cas des p-groupes se traduit dans les systèmes complets de Frobenius par l'égalité des systèmes complets de Frobenius sur P car on travaille directement avec les morphismes. Définissons, en général, la notion de sous-système d'un système complet de Frobenius.

Définition 4.3.1 *Soit $\mathcal{F}$ un système complet de Frobenius sur P. Un sous-système $\mathcal{F}'$ de $\mathcal{F}$ est un système complet de Frobenius sur un sous-groupe Q de P tel que les morphismes de $\mathcal{F}'$ sont un sous-ensemble de morphismes de $\mathcal{F}$.*

On va donner des conditions nécessaires et suffisantes sur un sous-groupe Q de P, complètement normalisé dans $\mathcal{F}$, pour que $N_{\mathcal{F}}(Q)$ soit égal à $\mathcal{F}$. Si $\mathcal{F} = F_p(G)_{\leq P}$, où P est un p-sous-groupe de Sylow d'un groupe fini G, est le système complet de Frobenius sur P, dont les morphismes sont les morphismes à l'intérieur de P, induits par la conjugaison par les éléments de G, le fait que $\mathcal{F} = N_{\mathcal{F}}(Q)$ est équivalent au contrôle de la p-fusion dans G par $N_G(Q)$. En effet, $N_{\mathcal{F}}(Q) = F_p(N_G(Q))_{\leq N_P(Q)}$, car tout morphisme dans $F_p(N_G(Q))_{\leq N_P(Q)}$ entre deux sous-groupes R et T de $N_P(Q)$ donné par la conjugaison par un élément h de $N_G(Q)$ peut être regardé comme un morphisme par conjugaison par h entre $Q \cdot R$ et $Q \cdot T$, étant donné que ${}^hQ = Q$. L'inclusion dans l'autre sens est évidente. Dans le cas des catégories de Frobenius, le contrôle de la p-fusion dans G par $N_G(Q)$ se traduit par $F_p(G)_{\leq P} = F_p(N_G(Q))_{\leq N_P(Q)}$, donc c'est une question naturelle que de se demander si un sous-système $\mathcal{F}'$ d'un sytème complet de Frobenius $\mathcal{F}$ est égal à $\mathcal{F}$.

Débutons par quelques définitions.

Définition 4.3.2 *On dit que Q est fortement fermé dans $\mathcal{F}$ si $\phi(R) \leq Q$, pour tout sous-groupe R de Q et tout morphisme $\phi \in \mathcal{F}(R,P)$.*

Définition 4.3.3 *On dit que Q est faiblement fermé dans $\mathcal{F}$ si $\phi(Q) = Q$, pour tout morphisme $\phi \in \mathcal{F}(Q,P)$.*

Remarque 4.3.4 En fait, Q est fortement fermé dans $\mathcal{F}$ si et seulement si $\mathcal{F}(R,P) = \mathcal{F}(R,Q)$, pour tout sous-groupe R de Q, et faiblement fermé dans $\mathcal{F}$ si et seulement si $\mathcal{F}(Q,P) = \mathcal{F}(Q)$. Il est évident que, si Q est fortement fermé dans $\mathcal{F}$, alors Q faiblement fermé dans $\mathcal{F}$.

Définition 4.3.5 *Une série centrale pour Q est une série $1 = Q_0 \lhd Q_1 \lhd Q_2 \lhd \ldots \lhd Q_n = Q$ telle que $Q_{i+1}/Q_i \leq Z(Q/Q_i)$. Si on a égalité dans la dernière relation alors la série s'appelle centrale ascendante.*

Pour un système complet de Frobenius $\mathcal{F}$ sur P on peut définir le quotient $\overline{\mathcal{F}}$ de $\mathcal{F}$ par un sous-groupe Q de P, fortement fermé dans $\mathcal{F}$.

Définition 4.3.6 *Soit $\mathcal{F}$ un système complet de Frobenius sur P et Q un sous-groupe de P fortement fermé dans $\mathcal{F}$. On définit $\overline{\mathcal{F}} := \mathcal{F}/Q$ comme la catégorie sur P/Q dont les objets sont les sous-groupes de P/Q et les morphismes sont ceux induits par $\mathcal{F}$.*

En fait si G est un groupe fini ayant P comme p-sous-groupe de Sylow, et Q est un sous-groupe de P normal dans G, alors Q est fortement fermé dans $F_p(G)_{\leq P}$ et, de plus $F_p(G)_{\leq P}/Q = F_p(G/Q)_{\leq P/Q}$. Le fait que Q est fortement fermé dans $F_p(G)_{\leq P}$ est immédiat, car tout morphisme dans $F_p(G)_{\leq P}$ donné par conjugaison par un élément g de G qui part d'un sous-groupe R de Q se prolonge en un morphisme par conjugaison par g qui part de Q et on a ${}^gR \leq {}^gQ = Q$ car G normalise Q. L'égalité $F_p(G)_{\leq P}/Q = F_p(G/Q)_{\leq P/Q}$ vient tout simplement du fait que les objets et les morphismes des deux catégories sont trivialement les mêmes.

Démontrons maintenant que $\mathcal{F}/Q$ est un système complet de Frobenius. Ce résultat est aussi dû à Puig. Notons $\overline{} : P \to P/Q$ la projection canonique.

Proposition 4.3.7 ([Pu2], Prop. 2.15) *Soit $\mathcal{F}$ un système complet de Frobenius sur P et Q un sous-groupe de P fortement fermé dans $\mathcal{F}$. Alors $\overline{\mathcal{F}} := \mathcal{F}/Q$ est un système complet de Frobenius.*

Preuve. On va vérifier les trois axiomes pour $\overline{\mathcal{F}}$. Pour vérifier l'axiome A1 il faut montrer que, pour tout $\overline{\phi} \in \overline{\mathcal{F}}(\overline{R}, \overline{T})$, le morphisme $\overline{\psi} : \overline{\phi}(\overline{R}) \to \overline{R}$ définit par $\overline{\psi}(\overline{\phi}(\overline{u})) = u$, pour tout $\overline{u} \in \overline{R}$, est un morphisme de $\overline{\mathcal{F}}(\overline{\phi}(\overline{R}), \overline{R})$. Mais, par la définition de $\overline{\mathcal{F}}$, on a $\phi \in \mathcal{F}(R, T)$. Par l'axiome A1 appliqué à ϕ, il existe $\psi \in \mathcal{F}(\phi(R), R)$ tel que $\psi(\phi(u)) = u$, pour tout $u \in R$, donc $\overline{\psi} \in \overline{\mathcal{F}}(\overline{\phi}(\overline{R}), \overline{R})$ a les propriétés voulues.

Par construction de $\overline{\mathcal{F}}$, le morphisme de passage au quotient $\mathcal{F}(P) \longrightarrow \overline{\mathcal{F}}(\overline{P})$ est surjectif et l'image de $\mathcal{I}(P)$ par ce morphisme est $\mathcal{I}(\overline{P})$. Par l'axiome A2 appliqué à P le groupe $\mathcal{I}(P)$ est un p-sous-groupe de Sylow de $\mathcal{F}(P)$, donc $\mathcal{I}(\overline{P})$ est un p-sous-groupe de Sylow de $\overline{\mathcal{F}}(\overline{P})$, ce qui entraîne que l'axiome $A2$ est satisfait dans $\overline{\mathcal{F}}$.

Vérifions maintenant l'axiome A3. Soit $\overline{\phi} \in \overline{\mathcal{F}}(\overline{R}, \overline{P})$, $\phi \in \mathcal{F}(R, P)$ un représentant de $\overline{\phi}$ dans $\mathcal{F}$ et $\overline{K}$ un sous-groupe de $\mathrm{Aut}(\overline{R})$. On désigne par K l'image inverse de $\overline{K}$ dans le stabilisateur de Q dans $\mathrm{Aut}(R)$. On remarque que, même si K n'est pas forcément envoyé surjectivement sur $\overline{K}$, le groupe $N_{\overline{P}}^{\overline{K}}(\overline{R})$ est l'image de $N_P^K(R)$. Posons $\overline{K}' := {}^{\overline{\phi}}\overline{K}$, $\overline{R}' := \overline{\phi}(\overline{R})$, $K' := {}^{\phi}K$ et $R' := \phi(R)$. Supposons que $\overline{R}'$ est $\overline{K}'$-complètement normalisé. Comme $N_{\overline{P}}^{\overline{K}}(\overline{R})$ est l'image de $N_P^K(R)$, il s'ensuit que $N_{\overline{P}}^{\overline{K}'}(\overline{R}')$ est l'image de $N_P^{K'}(R')$, donc $\overline{\mathcal{F}}(\overline{R}' \cdot N_{\overline{P}}^{\overline{K}'}(\overline{R}'), \overline{P})$ est l'image de $\mathcal{F}(R' \cdot N_P^{K'}(R'), P)$. Donc pour tout $\theta \in \mathcal{F}(R' \cdot N_P^{K'}(R'), P)$ on obtient $\overline{\theta} \in \overline{\mathcal{F}}(\overline{R}' \cdot N_{\overline{P}}^{\overline{K}'}(\overline{R}'), \overline{P})$ et, comme $\overline{R}'$ est $\overline{K}'$-complètement normalisé, on en dèduit que $\overline{\theta}(N_{\overline{P}}^{\overline{K}'}(\overline{R}')) = N_{\overline{P}}^{{}^{\overline{\theta}}\overline{K}'}(\overline{\theta}(\overline{R}'))$, et donc $\theta(N_P^{K'}(R')) = N_P^{{}^{\theta}K'}(\theta(R'))$. On en déduit que R' est K'-complètement normalisé.

Par l'axiome A3 appliqué à ϕ, il existe $\rho \in \mathcal{F}(RN_R^K(P), P)$ et $\chi \in K$ tels que $\rho(u) = \phi(\chi(u))$ pour tout $u \in R$. Comme Q est fortement fermé dans $\mathcal{F}$, on obtient $\rho(Q) = Q$, donc $\overline{\rho}$ est un morphisme de $\overline{\mathcal{F}}(\overline{R} \cdot N_{\overline{P}}^{\overline{K}}(\overline{R}), \overline{P})$. De plus $\chi(Q) = Q$ car $\chi \in K$ et donc $\overline{\chi} \in \overline{K}$. Pour finir on obtient que $\overline{\rho}(\overline{u}) = \overline{\phi}(\overline{\chi}(\overline{u}))$ pour tout $\overline{u} \in \overline{R}$ et l'axiome A3 est vérifié pour $\overline{\mathcal{F}}$. □

Remarque 4.3.8 Soit $\mathcal{F}$ un système complet de Frobenius et Q un sous-groupe normal de P. Alors $N_P(Q) = P$, donc Q est complètement normalisé dans R. Mais Q n'est pas forcément fermé dans $\mathcal{F}$. Par contre, Q est fortement fermé dans $\mathcal{N} := N_{\mathcal{F}}(Q)$. En effet, pour tout sous-groupe $R \leq Q$ et tout $\phi \in \mathcal{N}(R, N_P(Q))$ il existe un morphisme $\psi \in \mathcal{F}(Q \cdot R, P) = \mathcal{F}(Q, P)$ tel que $\psi(u) = \phi(u)$, pour tout $u \in R$ et $\psi(Q) = Q$. Par conséquent, on a $\phi(R) = \psi(R) \leq \psi(Q) = Q$ et comme ceci est vrai pour tout sous-groupe de Q, ce dernier est fortement fermé dans $\mathcal{N}$.

On continue par deux lemmes techniques. Si T est un sous-groupe normal de P, notons $\overline{} : P \to P/T$ la projection canonique.

Lemme 4.3.9 *Soit Q un p-groupe et T un sous-groupe normal de Q. Si la série donnée par $Q = Q_n \geq Q_{n-1} \geq \ldots \geq Q_1$ est une série centrale de Q alors $\overline{Q} = \overline{Q_n} \geq \overline{Q_{n-1}} \geq \ldots \geq \overline{Q_1}$ est une série centrale de $\overline{Q}$. Si, de plus, $Q_1 = T$, alors la réciproque est aussi vraie.*

Preuve. Pour la première partie du lemme on utilise la propriété évidente que $\overline{Z(Q)} \leq Z(\overline{Q})$ et $\overline{Z(Q/Q_i)} \leq Z(\overline{Q}/\overline{Q_i})$. Donc les relations $\overline{Q_1} \leq Z(\overline{Q})$ et $\overline{Q_{i+1}}/\overline{Q_i} \leq Z(\overline{Q}/\overline{Q_i})$ restent toujours satisfaites, étant donné que $\overline{Q_1} \leq \overline{Z(Q)}$ et $\overline{Q_{i+1}}/\overline{Q_i} = \overline{Q_{i+1}/Q_i} \leq \overline{Z(Q/Q_i)}$. On en déduit que $\overline{Q} = \overline{Q_n} \geq \overline{Q_{n-1}} \geq \ldots \geq \overline{Q_1}$ est une série centrale de $\overline{Q}$. Pour la réciproque, T est central dans Q, donc $Q_1 = T \leq Z(Q)$. Les autres vérifications sont immédiates, en utilisant le fait que $Q/Q_i \simeq \overline{Q}/\overline{Q_i}$ et $Q_{i+1}/Q_i \simeq \overline{Q_{i+1}}/\overline{Q_i}$, pour tout $i = 1, \ldots, n-1$. □

Lemme 4.3.10 *Soient P un p-groupe, $\mathcal{F}$ un système complet de Frobenius sur P et T un sous-groupe de P fortement fermé dans $\mathcal{F}$. Soient $\overline{\mathcal{F}} := \mathcal{F}/T$ et soit $Q \leq P$. Si Q est fortement, respectivement faiblement fermé dans $\mathcal{F}$, alors $\overline{Q}$ est fortement, respectivement faiblement fermé dans $\overline{\mathcal{F}}$. Si Q contient T et $\overline{Q}$ est faiblement fermé dans $\overline{\mathcal{F}}$, alors Q est faiblement fermé dans $\mathcal{F}$.*

Preuve. Par définition, Q est fortement fermé dans $\mathcal{F}$ si et seulement si pour tout $R \leq Q$, on a $\mathcal{F}(R, P) = \mathcal{F}(R, Q)$. Ceci implique que $\overline{\mathcal{F}}(\overline{R}, \overline{P}) = \overline{\mathcal{F}}(\overline{R}, \overline{Q})$, car les morphismes dans $\overline{\mathcal{F}}$ sont induits par les morphismes dans $\mathcal{F}$. Comme tout sous-groupe de $\overline{Q}$ a une préimage dans Q, on a l'équivalence avec le fait que $\overline{Q}$ est fortement fermé dans $\overline{\mathcal{F}}$. Le fait que Q est faiblement fermé dans $\mathcal{F}$, par le même argument, implique le fait que $\overline{Q}$ est faiblement fermé dans $\overline{\mathcal{F}}$.

Supposons maintenant que $T \leq Q$ et $\overline{Q}$ est faiblement fermé dans $\overline{\mathcal{F}}$. Soit $\phi \in \mathcal{F}(Q, P)$. Il induit un morphisme $\overline{\phi} \in \overline{\mathcal{F}}(\overline{Q}, \overline{P})$. Comme $\overline{Q}$ est faiblement fermé dans $\overline{\mathcal{F}}$ il s'ensuit que $\overline{\phi} \in \overline{\mathcal{F}}(\overline{Q})$. Ceci entraîne que $\phi \in \mathcal{F}(Q)$, donc Q est faiblement fermé dans $\mathcal{F}$. □

Au milieu des années '80, Gilotti et Serena [GS] donnent des conditions nécessaires et suffisantes pour que le normalisateur d'un p-sous-groupe d'un groupe fini G contrôle la p-fusion dans G. Dans la dernière partie de cette section on va généraliser ce résultat aux systèmes complets de Frobenius.

Théorème 4.3.11 *Soit P un p-groupe fini, Q un sous-groupe de P et $\mathcal{F}$ un système complet de Frobenius sur P. Alors $N_{\mathcal{F}}(Q) = \mathcal{F}$ si et seulement si Q est fortement fermé dans $\mathcal{F}$ et Q admet une série centrale $Q = Q_n \geq Q_{n-1} \geq \ldots \geq Q_1$ où Q_i est faiblement fermé dans $\mathcal{F}$, pour tout $1 \leq i \leq n-1$.*

Preuve. Posons $\mathcal{N} := N_{\mathcal{F}}(Q)$.

$\Longrightarrow$ Supposons que $\mathcal{N} = \mathcal{F}$. Soit R un sous-groupe de Q et $\phi \in \mathcal{F}(R,P)$. Comme $\mathcal{N} = \mathcal{F}$, on obtient $\phi \in \mathcal{N}(R,P)$, donc le morphisme ϕ se prolonge à un morphisme $\psi \in \mathcal{F}(Q)$. Ainsi $\phi(R) = \psi(R) \leq \psi(Q) = Q$, ce qui entraîne que Q est fortement fermé dans $\mathcal{F}$. Considérons la série centrale ascendante $Q = Q_n \geq Q_{n-1} \geq \ldots \geq Q_1$ et, pour un $1 \leq i \leq n-1$, soit $\phi_i \in \mathcal{F}(Q_i, P)$. Comme avant, on a $\phi_i \in \mathcal{N}(Q_i, P)$. Mais, Q_i est caractéristique dans Q, donc $Q_i = \phi_i(Q_i)$, car ϕ peut être relevé en un morphisme dans $\mathcal{F}(Q)$. Ainsi Q_i est faiblement fermé dans $\mathcal{F}$, pour tout $1 \leq i \leq n-1$.

$\Longleftarrow$ Supposons que le groupe Q est fortement fermé dans $\mathcal{F}$ et qu'il admet une série centrale $Q = Q_n \geq Q_{n-1} \geq \ldots \geq Q_1 > 1$ où Q_i est faiblement fermé dans $\mathcal{F}$ pour tout $1 \leq i \leq n-1$. Par le fait que Q_i est faiblement fermé dans $\mathcal{F}$ on a $Q_i \lhd P$, pour tout $1 \leq i \leq n$. En particulier, $N_P(Q) = P$, donc, par la proposition 4.1.14, $\mathcal{N}$ est un système complet de Frobenius sur P. Posons $T := Q_1 \cap Z(P)$. Comme Q_1 est normal dans P, par la proposition 1.1.7, T n'est pas trivial.

On démontre premièrement que $\mathcal{F}(T,P) = \mathcal{N}(T,P)$. En effet, soit $\phi \in \mathcal{F}(T,P)$. Par le fait que Q est fortement fermé dans $\mathcal{F}$ on a $\phi(T) \leq Q$. Comme $Q_1 \leq Z(Q)$, on obtient que $T, \phi(T) \leq C_P(Q_1)$ et, ainsi, que $Q_1 \leq C_P(T)$. Mais T est complètement centralisé dans $\mathcal{F}$, car $C_P(T) = P$. Donc il existe un morphisme $\chi \in \mathcal{F}(C_P(\phi(T)), P)$ tel que $\chi|_{\phi(T)} = \phi^{-1}$. Ainsi $\chi|_{Q_1} \in \mathcal{F}(Q_1, P)$ et, par la fermeture faible de Q_1 dans $\mathcal{F}$, on a $\chi|_{Q_1} \in \mathcal{F}(Q_1)$. Comme $\eta(Q_1) = Q_1$, pour tout $\eta \in \mathcal{F}(Q_1, P)$, on déduit que Q_1 est complètement centralisé dans $\mathcal{F}$. Maintenant $Q \leq C_P(Q_1)$, car $Q_1 \leq Z(Q)$. Ainsi, $\chi|_{Q_1}$ peut être prolongé, par l'axiome A3, à $\widetilde{\chi} \in \mathcal{F}(C_P(Q_1), P)$. On obtient, par restriction à Q, que $\widetilde{\chi}|_Q \in \mathcal{F}(Q,P)$, donc, comme Q est fortement fermé $\mathcal{F}$, on a $\widetilde{\chi}|_Q \in \mathcal{F}(Q)$. Ceci implique que $\widetilde{\chi}|_T$ est un morphisme dans $\mathcal{N}(T,P)$. En résumant, $\phi = \chi^{-1}|_T = \widetilde{\chi}^{-1}|_T$, donc ϕ est dans $\mathcal{N}(T,P)$.

Revenons maintenant au cas général. Par le théorème d'Alperin il suffit de montrer que $\mathcal{F}(U) = \mathcal{N}(U)$, pour U centrique, complètement normalisé dans $\mathcal{F}$. La preuve se fait par induction sur le nombre de morphismes dans $\mathcal{F}$. Si $\mathcal{F} = \{\mathrm{id}\}$ est un système complet de Frobenius sur P, alors P est forcément abélien car $\mathcal{F}(P)$ contient les automorphismes intérieurs de P et dans ce cas le théorème est trivial.

Soit $\mathcal{C} := N_{\mathcal{F}}^{\{\mathrm{id}\}}(T)$ et $\phi \in \mathcal{F}(U)$. Comme $C_P(T) = P$, le groupe T est complètement centralisé dans $\mathcal{F}$, donc, par la proposition 4.1.14, on obtient que $\mathcal{C}$ est un système complet de Frobenius sur P. Posons $\mathcal{N}' := N_{\mathcal{C}}(Q)$, et comme Q est aussi complètement normalisé dans $\mathcal{C}$, il s'ensuit que $\mathcal{N}'$ est un système complet de Frobenius sur P. On a clairement $\mathcal{N}'(R,P) = \mathcal{N}(R,P) \cap \mathcal{C}(R,P)$ pour tout sous-groupe R de P. On distingue deux cas.

Cas 1 : $\mathcal{F} \neq \mathcal{C}$. Comme U est centrique, il contient $Z(P)$, donc, a fortiori, T. Ainsi, on a $\phi|_T \in \mathcal{F}(T,P)$ et, par la première partie de la preuve, on a $\phi|_T \in \mathcal{N}(T,P)$. Par ailleurs, par l'axiome A3 appliqué à $\phi|_T$, en tenant compte du fait que T est complètement centralisé dans P et $C_P(T) = P$, on peut relever $\phi|_T$ en $\widetilde{\phi} \in \mathcal{F}(P)$ tel que $\widetilde{\phi}|_T = \phi|_T$. De plus, $\widetilde{\phi}|_Q \in \mathcal{F}(Q)$ car Q est fortement fermé dans $\mathcal{F}$. On obtient ainsi $\widetilde{\phi}^{-1}\phi \in \mathcal{F}(U,P) \cap \mathcal{C}(T)$. Par l'hypothèse de récurrence appliquée à $\mathcal{C}$, on a $\widetilde{\phi}^{-1}\phi \in \mathcal{N}'(U,P)$. Comme $\mathcal{N}'(U,P) \leq \mathcal{N}(U,P)$ on obtient que $\widetilde{\phi}^{-1}\phi \in \mathcal{N}(U,P)$. Mais, $\widetilde{\phi} \in \mathcal{F}(P) = \mathcal{N}(P)$, ce qui implique que $\phi \in \mathcal{N}(U,P)$ et termine la preuve dans ce cas.

Cas 2 : $\mathcal{F} = \mathcal{C}$. Dans ce cas T est fortement fermé dans $\mathcal{F}$. En effet soit $R \leq T$ et $\phi \in \mathcal{F}(R, P)$. Comme $\mathcal{F} = \mathcal{C}$ le morphisme ϕ se prolonge à $\psi \in \mathcal{F}(T)$ qui fixe T point par point et donc $\phi \in \mathcal{F}(R)$. Ainsi T est fortement fermé dans $\mathcal{F}$.

Prenons $\overline{\mathcal{F}} := \mathcal{F}/T$. Par la proposition 4.1.14, $\overline{\mathcal{F}}$ est un système complet de Frobenius sur $\overline{P}$. De plus, par le lemme 4.3.9, $\overline{Q} = \overline{Q_n} \geq \overline{Q_{n-1}} \geq \ldots \geq \overline{Q_1}$ est une série centrale de $\overline{Q}$ et, par le lemme 4.3.10, il s'ensuit que $\overline{Q}$ est fortement fermé dans $\overline{\mathcal{F}}$ et $\overline{Q}_i$ est faiblement fermé dans $\overline{\mathcal{F}}$, pour tout $1 \leq i \leq n-1$. Comme T n'est pas trivial, par hypothèse de récurrence, on a $\overline{\mathcal{F}} = N_{\overline{\mathcal{F}}}(\overline{Q}) =: \overline{\mathcal{N}}$, donc $\overline{\phi} \in \overline{\mathcal{N}}(\overline{U})$. On relève $\overline{\phi}$ en $\psi \in \mathcal{N}(U)$ car la projection canonique de $\mathcal{N}(U)$ sur $\overline{\mathcal{N}}(\overline{U})$ est surjective. De plus, pour tout $x \in U$ on a $\psi\phi^{-1}(x)x^{-1} \in T$. Posons $K := \{\theta \in \mathcal{F}(U) | \theta(x)x^{-1} \in T, \text{ pour tout } x \in U\}$. Maintenant K est un sous-groupe de $\mathrm{Aut}(U)$ qui centralise U/T par construction et T grâce au fait que tout morphisme de $\mathcal{F}$ centralise T, donc K centralise les quotients de la série normale $1 \triangleleft T \triangleleft U$. Par la proposition 1.1.9, K est un p-groupe. De plus, K est un sous-groupe normal de $\mathcal{F}(U)$, car, pour tous $\chi \in \mathcal{F}(U)$ et $\theta \in K$, on a

$$({}^{\chi}\theta)(x)x^{-1} = \chi\big(\theta(\chi^{-1}(x))(\chi^{-1}(x))^{-1}\big) \in \chi(T) = T \quad \text{pour tout } x \in U\,.$$

Comme U est complètement normalisé dans $\mathcal{F}$, par la proposition 4.1.13, le groupe $\mathcal{I}_P(U)$ est un p-sous-groupe de Sylow de $\mathcal{F}(U)$. De plus, K est un sous-groupe normal de $\mathcal{F}(U)$, donc $K \cap \mathcal{I}_P(U)$ est un p-sous-groupe de Sylow de K. Il s'ensuit que $K = \mathcal{I}_P^K(U)$ car K est un p-groupe. Comme $\psi\phi^{-1} \in K$, il existe $u \in P$ tel que $\psi\phi^{-1}(x) = {}^{u}x$, pour tout $x \in U$. Mais toute conjugaison par un élément de P est dans $\mathcal{F}$ et, de plus, étant donné que Q est normal dans P, on obtient $\mathrm{conj}(u)(Q) = Q$. Ceci entraîne que $\mathrm{conj}(u) \in \mathcal{N}(U)$. Ainsi, on a $\phi = \mathrm{conj}(u^{-1})\psi \in \mathcal{N}(U)$, ce qui prouve le théorème. □

4.4 Groupes résistants

La généralisation du théorème de Gilotti et Serena nous fournit une condition nécessaire et suffisante pour la résistance d'un p-groupe dans le cadre des systèmes complets de Frobenius.

Définition 4.4.1 *On dit qu'un p-groupe P est résistant dans le cadre des systèmes complets de Frobenius si pour tout système complet de Frobenius $\mathcal{F}$ sur P, on a $\mathcal{F} = N_{\mathcal{F}}(P)$.*

Pour qu'un p-groupe P soit résistant il faut et il suffit, par le théorème 4.3.11, que, pour tout système complet de Frobenius $\mathcal{F}$ sur P, il existe une suite centrale de P qui soit formée de sous-groupes faiblement fermés dans $\mathcal{F}$. La condition que P soit fortement fermé dans $\mathcal{F}$ est trivialement satisfaite. On a donc que les p-groupes abéliens sont trivialement résistants dans les systèmes complèts de Frobenius car la suite centrale ascendente est égale à P.

Premièrement on démontre un résultat similaire à celui obtenu dans le cadre des catégories de Frobenius, pour les p-groupes extraspéciaux généralisés.

Théorème 4.4.2 *Soit P un p-groupe extraspécial généralisé. Alors P est résistant dans le cadre des systèmes complets de Frobenius, à l'exception du cas où $P = E \times A$ avec A abélien élémentaire et E diédral d'ordre 8 (quand $p = 2$) ou d'ordre p^3 et exposant p (quand p est impair).*

Preuve. Si P est un tel p-groupe, la suite centrale ascendante se résume à $1 \lhd \Phi(P) \lhd P$. Donc P est résistant si et seulement si $\Phi(P)$ est faiblement fermé dans $\mathcal{F}$, pour tout système de Frobenius complet $\mathcal{F}$ sur P. Par le théorème d'Alperin, tout morphisme dans $\mathcal{F}(\Phi(P), P)$ peut être décomposé en une compostiton de morphismes maximaux et de morphismes essentiels. Comme les morphismes maximaux stabilisent $\Phi(P)$, il nous suffit de voir qu'il en est de même pour les morphismes essentiels.

Soit $\phi \in \mathcal{F}(Q)$, où Q est un sous-groupe essentiel de $\mathcal{F}$, complètement normalisé dans $\mathcal{F}$. Comme Q est centrique, il contient $Z(P)$ et $Q/Z(P)$ est un sous-espace maximal isotrope de $P/Z(P)$ pour la forme symplectique β, définie dans la section 2 du chapitre 3. De plus si Q est non-abélien élémentaire, alors $\Phi(Q) = \Phi(P)$. Tout automorphisme de Q préserve $\Phi(Q)$ et donc ϕ stabilise $\Phi(P)$. On a la même propriété pour ϕ si $|P/Z(P)| > p^2$. En effet, comme $|P : C_P(\phi(\Phi(P)))| \leq p$, car le centralisateur d'un sous-groupe d'ordre p de P est d'indice au plus p dans P, on en déduit que $C_P(\phi(\Phi(P)))/Z(P)$ ne peut pas être contenu dans un sous-espace isotrope maximal de $P/Z(P)$ par rapport à β. Ainsi $C := C_P(\phi(\Phi(P)))$ ne peut pas être abélien élémentaire. Donc $\Phi(C)$ n'est pas trivial et on a $\Phi(C) = \Phi(P)$. En même temps, comme $C_P(\Phi(P)) = P$, il s'ensuit $\Phi(P)$ est complètement centralisé. Par l'axiome A3 appliqué à ϕ, il existe un morphisme $\psi \in \mathcal{F}(C, P)$ tel que $\psi^{-1}|_{\Phi(P)} = \phi$. On en déduit que $\phi(\Phi(P))$ est le sous-groupe de Frattini de C, donc $\phi(\Phi(P)) = \Phi(P)$.

On peut donc se restreindre au cas où Q est abélien élémentaire et $|P : Z(P)| = p^2$. Dans ce cas Q est d'indice p dans P et, par le lemme 3.2.3, on a $P \simeq E \times A$ où E est un p-groupe extraspécial d'ordre p^3 et A un p-groupe abélien élémentaire. De plus $E \simeq P/A$ contient un sous-groupe isomorphe à $Q/A \simeq C_p \times C_p$, car Q est abélien élémentaire, donc E ne peut pas être isomorphe à Q_8. Le seul cas qui nous reste à exclure est le cas $E \simeq C_{p^2} \rtimes C_p$. Soit $K = (P/Q)$ vu comme un sous-groupe de $\mathcal{F}(Q/A)$.

Si $K = {}^{\phi}K$ alors $N_P^{{}^{\phi}K}(Q) = P$, donc Q est ${}^{\phi}K$-complètement normalisé dans $\mathcal{F}$. Par l'axiome $A3$, appliqué à ϕ, il existe $\psi \in \mathcal{F}(P)$ et $\chi \in K$ tel que $\psi(u) = \phi(\chi(u))$ pour tout $u \in Q$. Maintenant ψ et χ fixent Φ, donc il en est de même pour ϕ.

Il nous reste à vérifier le cas où $K \neq {}^{\phi}K$. On regarde K et ${}^{\phi}K$ comme des p-sous-groupes de $\mathrm{Aut}(Q/A) \simeq \mathrm{GL}(2, \mathbf{F}_p)$. Ainsi K et ${}^{\phi}K$ engendrent $\mathrm{SL}(2, \mathcal{F}_p)$.

On montre maintenant que l'extension $1 \longrightarrow Q/A \longrightarrow E \longrightarrow K \longrightarrow 1$ satisfait les hypothèses du lemme 3.2.7. En effet, pour tout morphisme $\phi' \in \mathcal{F}(Q)$ qui fixe K, on a $K = {}^{\phi'}K$, donc Q est ${}^{\phi}K$-complètement normalisé dans $\mathcal{F}$. Par l'axiome $A3$, appliqué à ϕ', il existe $\psi' \in \mathcal{F}(P)$ et $\chi' \in K$ tels que $\phi'(u) = \psi'(\chi')^{-1}(u)$, pour tout $u \in Q$. Mais $K = P/Q$ donc χ' se relève en la conjugaison par une préimage de χ' dans P, qui est un élément de $\mathcal{F}(P)$. En résumé ϕ' se relève dans $\mathcal{F}(P)$.

Ainsi, l'extension $1 \longrightarrow Q/A \longrightarrow E \longrightarrow K \longrightarrow 1$ satisfait les hypothèses du lemme 3.2.7 donc, par ce lemme, elle peut être étendue à $1 \longrightarrow Q/A \longrightarrow L \longrightarrow < K, {}^{\phi}K > \longrightarrow 1$. De plus, K et ${}^{\phi}K$ sont deux p-sous-groupes de Sylow distincts de $< K, {}^{\phi}K >$ donc, par le même lemme 3.2.7, E n'est pas isomorphe à $C_{p^2} \rtimes C_p$. □

La deuxième classe de p-groupes résistants est donnée par les p-groupes métacycliques, pour p impair.

Proposition 4.4.3 *Soit P un p-groupe métacyclique, avec p impair. Alors P est résistant dans le cadre des systèmes complets de Frobenius.*

Preuve. Considérons que P est donné par générateurs et relations

$$P := < u, v | u^{p^m} = 1, v^{p^n} = u^{p^q}, {}^v u = u^{p^l + 1} > \ .$$

Autrement dit, P est du type (m, n, q, l) et correspond à une extension :

$$1 \longrightarrow C_{p^m} \rightarrowtail P \longrightarrow C_{p^n} \longrightarrow 1 \ .$$

Si P est abélien alors il est trivialement résistant. Sinon P est forcément non-cyclique. Dans la cas où P est un p-groupe métacyclique non-cyclique, pour p impair, Nadia Mazza [Mz] a récemment démontré que P a un unique sous-groupe Q isomorphe à $C_p \times C_p$. Entre autres, ceci implique que si P a un sous-groupe isomorphe à $C_{p^\alpha} \times C_{p^\alpha}$, pour un nombre entier positif α, ce sous-groupe est unique.

On va trouver une série centrale de P formée de sous-groupes fortement fermés dans $\mathcal{F}$ par récurrence sur l'ordre de P. Les cas où $|P| \leq p^2$ sont triviaux car P est abélien.

Si on arrive à trouver $1 \neq P_1 \leq Z(P)$ faiblement fermé dans $\mathcal{F}$, alors on peut appliquer l'hypothèse de récurrence à $\overline{\mathcal{F}} := N_{\mathcal{F}}(P_1)/P_1$, qui est un système complet Frobenius sur P/P_1, par la proposition 4.3.7, étant donné que P_1 est fortement fermé dans $N_{\mathcal{F}}(P_1)$. En effet, P/P_1 est un p-groupe métacyclique d'ordre strictement inférieur à P. Par hypothèse de récurrence P/P_1 admet une série centrale $1 = \overline{P}_1 \lhd \overline{P}_2 \lhd \ldots \lhd \overline{P}_n = P/P_1$ avec les $\overline{P}_i$ faiblement fermés dans $\overline{\mathcal{F}}$. Soit $\pi : P \longrightarrow P/P_1$ la projection canonique. Considérons la série sous-normale de P, donnée par $1 = P_0 \lhd P_1 \lhd P_2 \lhd \ldots \lhd P_n = P$ avec $P_i = \pi^{-1}(\overline{P}_i)$ pour $1 \leq i \leq n$. Par la deuxième partie du lemme 4.3.9, c'est une série centrale de P. De plus, par le lemme 4.3.10, P_i est faiblement fermé dans $\mathcal{N} := N_{\mathcal{F}}(P_1)$, pour tout $2 \leq i \leq n$. On va démontrer maintenant que P_i est aussi faiblement fermé dans $\mathcal{F}$, pour tout $2 \leq i \leq n$. En effet, soit $\phi \in \mathcal{F}(P_i, P)$. On a $\phi|_{P_1} \in \mathcal{F}(P_1, P)$. Mais P_1 est faiblement fermé dans $\mathcal{F}$, ce qui entraîne que $\phi(P_1) = P_1$ et, par conséquent que $\phi \in \mathcal{N}(P_i, P)$. Maintenant P_i est faiblement fermé dans $\mathcal{N}$, donc $\phi(P_i) = P_i$ et on obtient que P_i est faiblement fermé dans $\mathcal{F}$.

Partons maintenant à la recherche d'un sous-groupe central non-trivial P_1 de P qui est faiblement fermé dans $\mathcal{F}$.

Si $Q \leq Z(P)$ alors on prend $P_1 := Q$ qui est faiblement fermé dans $\mathcal{F}$, car il est unique. Sinon on a forcément $M := < u^{p^{m-1}} > \leq Z(P)$ et $Z(P) \simeq C_{p^l}$. On veut voir que $< u^{p^{m-1}} >$ est normalisé par les morphismes maximaux et essentiels de P. Les morphismes maximaux normalisent $Z(P)$ et à fortiori $< u^{p^{m-1}} >$ car il est l'unique sous-groupe d'ordre p de $Z(P)$.

Soit maintenant E un sous-groupe de P, centrique et complètement normalisé dans P, candidat à être essentiel dans $\mathcal{F}$. Par élimination des groupes métacycliques qui ne peuvent jamais être réalisés comme sous-groupes essentiels (voir remarque 2.2.9 et théorème 2.3.2), on arrive au fait que E est isomorphe à $C_{p^\alpha} \times C_{p^\alpha}$, où α est un entier positif. Soit $\Phi(E)$ le sous-groupe de Frattini de E. Par la proposition 2.2.6, le noyau de l'application canonique $\phi : \mathcal{F}(E) \longrightarrow \mathrm{Aut}(E/\Phi(E))$ est un p-groupe. Mais, comme E est un sous-groupe essentiel dans $\mathcal{F}$ et $\mathcal{I}(E) = 1$, le complexe $\mathcal{S}_p(\mathcal{F}(E))$ est non-connexe, donc $O_p(\mathcal{F}(E))$ est trivial ce qui entraîne que le noyau de ϕ est aussi trivial. On en déduit qu'un p-sous-groupe de Sylow de $\mathcal{F}(E)$ est d'ordre p, car $\mathrm{Aut}(E/\Phi(E)) \simeq \mathrm{GL}(2, \mathbf{F}_p)$.

D'autre part, E est l'unique sous-groupe de P isomorphe à $C_{p^\alpha} \times C_{p^\alpha}$, donc il est caractéristique dans P. Ainsi $N_P(E) = P$ et E est complètement normalisé dans $\mathcal{F}$. Comme, de plus, E est centrique, P/E est un p-sous-groupe de Sylow de $\mathcal{F}(E)$. Mais on a vu qu'un p-sous-groupe de Sylow de $\mathcal{F}(E)$ est d'ordre p, donc $|P : E| = p$.

Donc P est un sous-groupe métacyclique, d'ordre $p^{2\alpha+1}$, ayant un sous-groupe E isomorphe à $C_{p^\alpha} \times C_{p^\alpha}$ et un centre $Z(P)$ cyclique. Ceci se traduit par le fait que u ne commute pas avec $v^{p^{n-1}}$ et que $u^{p^{m-\alpha}}$ commute avec $v^{p^{n-\alpha}}$.

Mais $v^{p^{n-1}}uv^{-p^{n-1}} = u^{(p^l+1)^{p^{n-1}}}$ et si on veut que $u^{(p^l+1)^{p^{n-1}}} \neq u$ il faut que $n+l-1 < m$. D'autre part

$$u^{p^{m-\alpha}} = v^{p^{n-\alpha}}u^{p^{m-\alpha}}v^{-p^{n-\alpha}} = u^{p^{m-\alpha}(p^l+1)^{p^{n-\alpha}}}$$

et, en tenant compte du fait que $(p^l+1)^{p^{n-\alpha}} - 1$ est exactement divisible par $p^{l+n-\alpha}$, il s'ensuit que $(m-\alpha)+(l+n-\alpha) \geq m$. Comme $m+n = 2\alpha+1$, on obtient que $1+l \geq m$. En fait, on a $m = l+1$ car $l < m$. Revenons maintenant à l'inégalité $n+l-1 < m$ dans laquelle on remplace $m = l+1$ de sorte qu'on obtient $n < 2$. Donc $n = 1$ ce qui entraîne $\alpha = 1$ et $m = 2$. On arrive à la conclusion que P doit être un p-groupe extraspécial d'ordre p^3 et exposant p^2, cas où on a vu, dans le théorème précédent, que tout morphisme dans $\mathcal{F}(E)$ fixe le centre de P.

Donc, si le centre de P est cyclique, $< u^{p^{m-1}} >$ est faiblement fermé dans P par rapport à $\mathcal{F}$ et on peut prendre $P_1 =< u^{p^{m-1}} >$. $\square$

On remarque ainsi que les p-groupes qu'on avait trouvés être résistants dans la catégorie de Frobenius restent résistants dans les systèmes de Frobenius. Est-ce juste le hasard ou y a-t-il quelque chose de profond qui se cache derrière ?

Bibliographie

[Al] J. L. Alperin, Sylow intersections and fusion, *J. Algebra* **6** (1967), 222–241.

[AB] J. L. Alperin et M. Broué. Local methods in block theory, *Ann. of Math* **110** (1979), 143–157.

[As] M. Aschbacher, Simple connectivity on p-group complexes, *Israel J. of Math.* **83** nos. 1–3 (1993), 1–43.

[Be] D. J. Benson, "Representations and cohomology I," Cambridge Studies in Advanced Math. 30, Cambridge Univ. Press, 1991.

[Bru] M. Broué, Contrôle – Isométries – Groupes de Frobenius, Publ. math. Univ. Paris VII. Séminaire sur les groupes finis. Tome I, 1979, 51–59.

[Brw] K. Brown, "Cohomology of groups," Springer-Verlag ed., 1982.

[Bu] W. Burnside, "Theory of groups of finite order," Cambridge Univ. Press, London 1897.

[CR] C. W. Curtis et I. Reiner. "Representation Theory of Finite Groups and Associative Algebras," Wiley-Interscience Publications, 1988.

[Di] J. A. Dieudonné, "La géométrie des groupes classiques," Springer-Verlag, Berlin, third edition, 1971.

[Dz] J. Dietz, Stable splitting of classifying spaces of metacyclic p-groups, p odd, *J. Pure and Appl. Algebra* **90** (1993), 115–136.

[Dz2] J. Dietz, Automorphisms of p-groups, given as cyclic-by-elementary abelian central extension, *J. Algebra* **242** (2001), 417–432.

[Gl] D. M. Goldschmidt, A conjugation family for finite groups, *J. Algebra* **16** (1970), 138–142.

[Gr] D. Gorenstein, "Finite groups," Harper's Series in Modern Math., U.S.A., 1968.

[GL] D. Gorenstein et R. Lyons. The local structure of finite groups of characteristic 2 type, *Mem. Amer. Math. Soc.* **42** no. 276 (1983).

[GM] D. J. Green et P. A. Minh. Almost all Extraspecial p-groups are Swan Groups, *Bull. Austral. Math. Soc.* **62** (2000), no. 1, 149–154.

[GS] A. L. Gilotti et L. Serena. Strongly Closed Subgroups and Strong Fusion. *J, London Math. Soc.* 2^{nd} *series* **32** (1985), 103–106.

[HP] H.-W. Henn et S. Priddy. p-nilpotence, classifying space, indecomposability, and others properties of almost all finite groups, *Comment. Math. Helv.* **69** (1994), no. 3, 335–350.

[Hu] J. Huebschmann, The mod-p cohomology rings of metacyclic groups, *J. Pure Appl. Algebra* **60** (1989) 53–103

[Ma] U. Martin, Allmost all p-groups have automorphism group a p-group, *Bull. Amer. Math. Soc (N.S.)* **15** (1986), no. 1, 78–82.

[Mz] N. Mazza, Le groupe de Dade d'un p-groupe métacyclique, *J. Algebra*, à paraître.

[MP] J. Martino et S. Priddy. On the cohomology and homotopy of Swan groups, *Math. Z.* **225**(2) (1997) 277–288.

[Mi] G. Mislin, On group homomorphisms inducing mod $-\ p$ cohomology isomorphisms, *Coment. Math. Helvetici* **65** (1990) 454–461.

[Pu1] L. Puig, Structure locale dans les groupes finis, *Bul. Soc. Math. France*, Mémoire no. 47, thèse de doctorat, 1976.

[Pu2] L. Puig, Full Frobenius systems and their localizing categories, *preprint*, Juin 2001.

[Su] M. Suzuki, "Group Theory I," Spriger-Verlag, 1982

[Th] J. Thévenaz, "G-Algebras et Modular Representation Theory," Oxford Science Publications, 1995.

Index