Intense Automorphisms of Finite Groups

Mima Stanojkovski

Author address:

Mathematisch Instituut, Universiteit Leiden, The Netherlands.
Current address: Fakultät für Mathematik, Universität Bielefeld, Germany.
E-mail address: mstanojk@math.uni-bielefeld.de

Contents

Abstract

Let G be a group. An automorphism of G is called *intense* if it sends each subgroup of G to a conjugate; the collection of such automorphisms is denoted by $\mathrm{Int}(G)$. In the special case in which p is a prime number and G is a finite p-group, one can show that $\mathrm{Int}(G)$ is the semidirect product of a normal p-Sylow and a cyclic subgroup of order dividing $p-1$. In this paper we classify the finite p-groups whose groups of intense automorphisms are not themselves p-groups. It emerges from our investigation that the structure of such groups is almost completely determined by their nilpotency class: for $p > 3$, they share a quotient, growing with their class, with a uniquely determined infinite 2-generated pro-p group.

2010 *Mathematics Subject Classification.* Primary 20D15, 20D45, 20F28; Secondary 20E18, 20E36.

Key words and phrases. Classification, finite p-groups, intense automorphisms, intensity.

The results presented in this paper were achieved during the author's doctoral studies at Leiden University under the supervision of Prof. Hendrik Lenstra, whom the author is very thankful to. The author would also like to thank Prof. Andrea Lucchini and Dr. Jon Gonzàlez Sànchez for their help and suggestions: she thanks moreover the University of Padova and the University of the Basque Country for the hospitality and support received during her visits in 2014. In addition, the author wishes to thank Dr. Ellen Henke, for her accurate comments.

List of Symbols

General

p, a prime number
$\mathbb{Z}$, ring of integers
$\mathbb{Z}_{\geq x}$, set of integers that are at least x
$\mathbb{Z}_{>x}$, set of integers that are larger than x
$\mathbb{Z}_p$, ring of p-adic integers
$\mathbb{F}_q$, finite field of q elements
R^*, group of units of the ring R
$|X|$, the cardinality of the set X
$\langle X\rangle$, the subgroup generated by the set X and we write $\langle a, b, c, \ldots\rangle$ for $\langle\{a, b, c, \ldots\}\rangle$
id_X, the identity map on the set X
$\alpha_{|X}$, the map α restricted to the set X
$\mathrm{cl}(X)$, the closure of the set X
$\bigsqcup$, disjoint union
$\otimes = \otimes_{\mathbb{Z}}$
$\bigwedge = \bigwedge_{\mathbb{Z}}$
$\mathrm{GL}_n(k)$, the general linear group of degree n over k
$\mathrm{MC}(3)$, definition in Chapter 9
$\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$, definition in Section 13.4.1
$\mathrm{S}(\Delta_p)$, definition in Section 13.4.2

For any group G

$[x, y] = xyx^{-1}y^{-1}$, for any $x, y \in G$
$\mathrm{Z}(G)$, the centre of G
$\Phi(G)$, the Frattini subgroup of G
$(G_i)_{i\geq 1}$, the lower central series of G
$G^n = \langle x^n \ : \ x \in G\rangle$
$\mu_n(G) = \langle x \in G \ : \ x^n = 1\rangle$
$\mathrm{C}_G(X) = \bigcap_{x\in X} G_x$, where G_x is the stabilizer of x
$\mathrm{N}_G(H)$, the normalizer of H in G
$\mathrm{Aut}(G)$, the automorphism group of G
$\mathrm{Inn}(G)$, the inner automorphism group of G
$\mathrm{Int}(G)$, the intense automorphism group of G, see Chapter 3
$\mathrm{rk}(G)$, the rank of G, see Sections 8.2 and 13.1

For a finite p-group G

ρ, the map $x \mapsto x^p$
$\mathrm{dpt}_G(x)$, the depth of x in G, see Section 2.3
$\mathrm{wt}_H^G(j)$, the j-th width of H in G, see Section 2.3

$\mathrm{wt}_G(j) = \mathrm{wt}_G^G(j)$

χ_G, the intense character of G, see Section 3.2

$\mathrm{int}(G)$, the intensity of G, see Section 3.2

Exceptions

$(F_i)_{i\geq 1}$, the p-central series of the free group F, in Sections 5.3, 9.4, and 9.6

CHAPTER 1

Introduction

Let G be a group and let $\mathrm{Aut}(G)$ denote its group of automorphisms. An automorphism $\alpha \in \mathrm{Aut}(G)$ is *intense* if it sends each subgroup of G to a conjugate, i.e., for every subgroup H of G there exists $g \in G$ such that $\alpha(H) = gHg^{-1}$. The collection of intense automorphisms is a normal subgroup of $\mathrm{Aut}(G)$, which is denoted by $\mathrm{Int}(G)$.

Such automorphisms come to light in the field of Galois cohomology, as we will see at the end of this introductory section. Additionally, they give rise to a very rich theory. We study the case in which G is a finite p-group and show that, if $\mathrm{Int}(G)$ is not itself a p-group, then the structure of G is almost completely determined by its *class*.

If G is a finite abelian group, then the inversion map $x \mapsto x^{-1}$ is an intense automorphism of G and therefore, unless the exponent of G divides 2, the order of $\mathrm{Int}(G)$ is even. It follows, for example, that if G is non-trivial abelian of odd order, then G always has a non-trivial intense automorphism of order coprime to its order. In Chapter 3 we prove the following result for groups of prime power order.

Theorem A. *Let p be a prime number and let G be a finite p-group. Then $\mathrm{Int}(G)$ is isomorphic to a semidirect product $S_G C_G$, where S_G is a Sylow p-subgroup of $\mathrm{Int}(G)$ and C_G is a subgroup of the unit group $\mathbb{F}_p^*$ of the finite field $\mathbb{F}_p$. Moreover, if G is non-trivial abelian, then $C_G = \mathbb{F}_p^*$.*

Theorem A is the same as Theorem 3.1 and is proven in Section 3.3. If p is an odd prime number, then Theorem A guarantees the existence of infinitely many p-groups, up to isomorphism, whose group of intense automorphisms is not itself a p-group. Moreover, it is also clear from Theorem A that the order of the intense automorphism group of a 2-group can never have prime divisors other than 2. We define the *intensity* of a finite p-group G to be the order of C_G and we denote it by $\mathrm{int}(G)$. The main goal of this paper is to classify all pairs (p, G) such that p is a prime number and G is a finite p-group of intensity greater than 1. Theorem A classifies all such pairs (p, G) for which G is abelian... but what happens in general?

We proceed by separating into cases based on "how non-abelian" a group is. The *lower central series* $(G_i)_{i\geq 1}$ of a group G is defined by

$$G_1 = G \quad \text{and} \quad G_{i+1} = [G, G_i] = \langle xyx^{-1}y^{-1} \ : \ x \in G, y \in G_i \rangle$$

and the *(nilpotency) class* of G is

$$\mathrm{cl}(G) = \#\{k \in \mathbb{Z}_{\geq 1} : G_k \neq 1\}.$$

It is a classical result that, for any finite p-group, the lower central series stabilizes at $\{1\}$ and so the class is finite. In Chapter 4 we look at finite p-groups of class 2 – the first non-abelian case we treat – and prove the following result.

Theorem B. *Let p be a prime number and let G be a finite p-group of class* 2. *Then the following are equivalent.*

1. *One has* $\mathrm{int}(G) > 1$.
2. *One has* $\mathrm{int}(G) = p - 1$ *and p is odd.*
3. *The group G is extraspecial of exponent p.*

Theorem B is the same as Theorem 4.1 and is proven in Section 4.3. As we remark in Chapter 4, *extraspecial groups* of exponent p are exactly those of the form $(\mathbb{F}_p^{2n+1}, *)$, where $*$ is a twist of the usual $+$ by an inner product on $\mathbb{F}_p^n$. Thanks to their pleasant shape, it is not a surprise that they carry intense automorphisms of order coprime to p. Moreover, they provide, for each odd prime p, an infinite class of examples of p-groups of class 2 and intensity different from 1.

Passing to class at least 3, things drastically change: in Chapter 5, we prove the following very restrictive result.

Theorem C. *Let p be a prime number and let G be a finite p-group of class at least* 3. *Then the following hold.*

1. *One has* $\mathrm{int}(G) \leq 2$.
2. *If* $\mathrm{int}(G) = 2$*, then p is odd and* $|G : G_2| = p^2$.

Theorem C is a reformulation of Theorem 5.2, which is proven in Section 5.1. Moreover, Theorem C tells us that, for class greater than 2, a p-group G always has intensity 1 or 2; in the latter case, if p is odd, then the order of the abelianization of G is "small".

Starting from class 3, we want to understand the structure of the groups from Theorem C(2). To this end, let p be an odd prime number and let G be a finite p-group of class 3 with $|G : G_2| = p^2$. In Section 5.2, we prove that G/G_3 is extraspecial of exponent p and that the order of G is p^4 or p^5. Moreover, if we write $w_i = \log_p |G_i : G_{i+1}|$, then either $(w_1, w_2, w_3) = (2, 1, 1)$ or $(w_1, w_2, w_3) = (2, 1, 2)$. As a consequence, for the given prime number p, there are, up to isomorphism, only finitely many possibilities for G (for a sharp bound see for example [**Ben27**]) and so, contrarily to what happens for class 1 and 2, there are only finitely many isomorphism classes of finite p-groups of class 3 and intensity greater than 1. The fortunate outcome of our investigation in class 3 is the following.

Theorem D. *Let p be an odd prime number and let G be a finite p-group of class* 3. *Then the following are equivalent.*

1. *One has* $\mathrm{int}(G) = 2$.
2. *One has* $|G : G_2| = p^2$.

The last theorem is a simplification of Theorem 5.1, whose proof is given in Section 5.3. Thanks to Theorem D, we now know that the only condition, given an odd prime number p, for a finite p-group of class 3 to have intensity 2 is just that of having an abelianization of order p^2. The most urgent problem at this point is that of constructing examples of p-groups of class greater than 3 and intensity 2: those will serve as a model for further investigation.

Example 1.1. Let $p > 3$ be a prime number and let $\mathbb{Z}_p$ denote the ring of p-adic integers. Let t be a quadratic non-residue modulo p and denote by Δ_p the quaternion algebra $\Delta_p = \mathbb{Z}_p + \mathbb{Z}_p\mathrm{i} + \mathbb{Z}_p\mathrm{j} + \mathbb{Z}_p\mathrm{ij}$ with defining relations $\mathrm{i}^2 = t$, $\mathrm{j}^2 = p$, and $\mathrm{ji} = -\mathrm{ij}$. The algebra Δ_p is equipped with a *standard involution*, which is given by

$$x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{ij} \;\mapsto\; \overline{x} = a - b\mathrm{i} - c\mathrm{j} - d\mathrm{ij}$$

and which is an anti-ring-automorphism of Δ_p. Moreover, $\mathfrak{m} = \Delta_p\mathrm{j}$ is the unique (2-sided/left/right) maximal ideal of Δ_p and the residue field $\Delta_p/\mathfrak{m}$, as well as every quotient $\mathfrak{m}^k/\mathfrak{m}^{k+1}$, has cardinality p^2. Via the natural isomorphisms of groups $(1+\mathfrak{m}^k)/(1+\mathfrak{m}^{k+1}) \to \mathfrak{m}^k/\mathfrak{m}^{k+1}$, the multiplicative group $1+\mathfrak{m}$ is then seen to be a pro-p-subgroup of Δ_p^*. We define $\mathrm{S}(\Delta_p)$ to be the subgroup of $1+\mathfrak{m}$ consisting of those elements x satisfying $\overline{x} = x^{-1}$. Being closed in $1+\mathfrak{m}$, the group $\mathrm{S}(\Delta_p)$ is itself a pro-p-subgroup of Δ_p^* and, if $(\mathrm{S}(\Delta_p)_i)_{i\geq 1}$ denotes the lower central series of $\mathrm{S}(\Delta_p)$, then

$$(\log_p |\,\mathrm{S}(\Delta_p)_i : \mathrm{S}(\Delta_p)_{i+1}|)_{i\geq 1} = (2,1,2,1,2,1,\ldots).$$

We show in Section 13.4.2 that each non-trivial discrete quotient of $\mathrm{S}(\Delta_p)$ has intensity greater than 1.

Because of the last example, we know that, whenever p is a prime larger than 3 and c is a positive integer, then there always exists a finite p-group of class c and intensity greater than 1. We cannot however use the same strategy to build examples of high class 3-groups of intensity 2. As a matter of fact, even though the group $\mathrm{S}(\Delta_p)$ can be defined also for $p = 3$, the image of the 3-torsion of $\mathrm{S}(\Delta_3)$ in $\mathrm{S}(\Delta_3)/\mathrm{S}(\Delta_3)_2$ is non-trivial. The next result, which is obtained by combining Theorem 6.1 and Lemma 7.12(1), explains why this is a problem.

Theorem E. *Let p be an odd prime number and let G be a finite p-group. Let $(G_i)_{i\geq 1}$ denote the lower central series of G and write $w_i = \log_p |G_i : G_{i+1}|$. Assume that the class of G is at least 4 and that $\mathrm{int}(G) = 2$. Then the following conditions are satisfied.*

1. *One has $(w_1, w_2, w_3, w_4) = (2,1,2,1)$.*
2. *The map $x \mapsto x^p$ induces a bijection $\overline{\rho} : G/G_2 \to G_3/G_4$.*

Relying on *regularity*, one can prove that, whenever $p > 3$, the map $\overline{\rho}$ from Theorem E is a group isomorphism, while in the case of 3-groups it never is: because of this structural difference, we separate the two cases.

We define a *κ-group* to be a finite 3-group G such that $|G : G_2| = 9$ and such that cubing induces a bijection $\kappa : G/G_2 \to G_3/G_4$. In particular, κ coincides with $\overline{\rho}$ from Theorem E(2). In Chapter 9, we prove several structural results about κ-groups: we show, for example, that in class 3 there is, up to isomorphism, a unique κ-group and that the minimal extensions of that group to class 4 (which then have order 729) have an elementary abelian commutator subgroup. The just-mentioned results are presented in the form of Theorems 9.3 and 9.4. Our investigation of κ-groups leads to the construction of the following example.

Example 1.2. Let $R = \mathbb{F}_3[\epsilon]$ be of cardinality 9, with $\epsilon^2 = 0$. Denote by Δ the quaternion algebra $\Delta = R + R\mathrm{i} + R\mathrm{j} + R\mathrm{ij}$ with defining relations $\mathrm{i}^2 = \mathrm{j}^2 = \epsilon$ and $\mathrm{ji} = -\mathrm{ij}$. Let moreover the *standard involution* on Δ be the R-linear map that is given by $(\overline{1}, \overline{\mathrm{i}}, \overline{\mathrm{j}}, \overline{\mathrm{ij}}) = (1, -\mathrm{i}, -\mathrm{j}, -\mathrm{ij})$. Then, for each $x, y \in \Delta$, one has $\overline{xy} = \overline{y}\,\overline{x}$. We write $\mathfrak{m} = \Delta\mathrm{i} + \Delta\mathrm{j}$, which is a nilpotent maximal 2-sided ideal of Δ with $\Delta/\mathfrak{m}$ isomorphic to $\mathbb{F}_3$. We define additionally $\mathrm{MC}(3)$ to be the subgroup of the multiplicative group $1 + \mathfrak{m}$ consisting of those elements x satisfying $\overline{x} = x^{-1}$. The group $\mathrm{MC}(3)$ has order 729, class 4, and it is a κ-group. Moreover, $\mathrm{int}(\mathrm{MC}(3)) = 2$.

In Chapter 9 we prove the following result, which is a simplified version of Theorem 9.1.

Theorem F. *Let G be a finite 3-group of class at least 4. Then the following conditions are equivalent.*

1. *One has* $\mathrm{int}(G) = 2$.
2. *The group G is isomorphic to* $\mathrm{MC}(3)$.

Theorem F concludes the classification of finite 3-groups of intensity greater than 1. Except for the two infinite families of finite non-trivial abelian 3-groups and extraspecial 3-groups of exponent 3, there are, up to isomorphism, exactly 17 groups in class 3 (specifically 4 of order 81 and 13 of order 243), and 1, namely MC(3), in class 4. In class higher than 4, there are no 3-groups of intensity greater than 1.

To continue our investigation, we let $p > 3$ be a prime number. In Chapter 10, we define a *p-obelisk* to be a finite non-abelian p-group G such that $|G : G_3| = p^3$ and $G^p = G_3$. Among other things, we prove that p-obelisks of class at least 4 satisfy both (1) and (2) from Theorem E and it is in fact true that, for each p-obelisk G, one has

$$(\log_p |G_i : G_{i+1}|)_{i\geq 1} = (2, 1, 2, 1, \ldots, 2, 1, f, 0, 0, \ldots) \;\text{ with }\; f \in \{0, 1, 2\},$$

where the index $i \in \{\mathrm{cl}(G), \mathrm{cl}(G) + 1\}$ to which f corresponds is odd and larger than 2. We will see in Chapter 13 that, for every prime number $p > 3$, each non-abelian quotient of $\mathrm{S}(\Delta_p)$ is a special kind of p-obelisk that we call *framed*.

Let p be a prime number and let G be a finite p-group. The *Frattini subgroup* of G is $\Phi(G) = [G, G]G^p$; then $G/\Phi(G)$ is the largest possible quotient of G that is vector space over $\mathbb{F}_p$. If $p > 3$, then a p-obelisk G is *framed* if the Frattini subgroup of each maximal subgroup of G coincides with G_3, i.e. for each maximal subgroup M of G, one has $\Phi(M) = G_3$. Though it might not be evident at first sight, asking for a p-obelisk to be framed is equivalent to imposing strong limitations to the interaction of commutator maps and power maps in the group.

Using a wide range of techniques, we are able to prove the following characterization for p-groups of class at least 4, which coincides with the combination of Theorems 11.1, 12.2, and 12.1.

Theorem G. *Let $p > 3$ be a prime number and let G be a finite p-group of class at least 4. For each $i \in \mathbb{Z}_{\geq 1}$, write $w_i = \log_p |G_i : G_{i+1}|$. Then* $\mathrm{int}(G) = 2$ *if and only if there exists $\alpha \in \mathrm{Aut}(G)$ of order 2 such that α induces the inversion map $x \mapsto x^{-1}$ on G/G_2 and one of the following holds.*

1. *The group G is a p-obelisk of class 4.*
2. *The group G is a p-obelisk with $w_5 = 1$ and $\Phi(\mathrm{C}_G(G_4)) = G_3$.*
3. *The group G is a framed p-obelisk with $w_5 = 2$.*

Theorem G makes the role of p-obelisks in our theory clear and it can be used to prove that any p-group of class at least 6 and intensity greater than 1 is a framed p-obelisk. Class 5 is the highest class in which there still exist p-obelisks of intensity greater than 1 that are not framed . . . but "semi-framed". More precisely, if, as in Theorem G(2), the group G is a p-obelisk with $w_5 = 1$, then the class is 5, the order of G_5 is p, and $\mathrm{C}_G(G_4)$ is a maximal subgroup; it is the only maximal subgroup whose Frattini subgroup is required to coincide with G_3.

Theorem G completes the classification of prime power order groups of intensity greater than 1, modulo the existence of some special automorphism. Because of their relevance in the theory of intense automorphisms, we give a name to such an automorphism. If G is a group, we call an automorphism $\alpha \in \mathrm{Aut}(G)$ *concrete* if it has order 2 and the automorphism of G/G_2 that is induced by α coincides with the inversion map $x \mapsto x^{-1}$. To the present day, we know very little about concrete automorphisms and how to construct them in general: finding necessary and sufficient conditions for a p-obelisks to possess a concrete automorphism is an interesting problem that we have not yet addressed.

In the following table, we summarize the results we have formulated so far. We denote by p a prime number and by G a finite p-group of class c.

<table>
<tr><th colspan="4"><b>Intensity</b></th></tr>
<tr><th>c \ p</th><th>2</th><th>3</th><th>≥ 5</th></tr>
<tr><td>0</td><td rowspan="6">1</td><td colspan="2">1</td></tr>
<tr><td>1</td><td colspan="2">$p-1$</td></tr>
<tr><td>2</td><td colspan="2">$p-1$ if G extraspecial of exponent p;
1 otherwise</td></tr>
<tr><td>3</td><td colspan="2">2 if $|G : G_2| = p^2$;
1 otherwise</td></tr>
<tr><td>4</td><td>2 if $G \cong \mathrm{MC}(3)$;
1 otherwise</td><td>2 if G is a p-obelisk with a concrete automorphism;
1 otherwise</td></tr>
<tr><td>≥ 5</td><td>1</td><td>2 if G is a p-obelisk of class 5 with $|G_5| = p$, $\Phi(\mathrm{C}_G(G_4)) = G_3$, and G has a concrete automorphism;
2 if G is framed p-obelisk with $|G_5 : G_6| = p^2$ and G has a concrete automorphism;
1 in all other cases</td></tr>
</table>

We now have a clear picture of the intensity of groups of prime power order, according to their (finite) class. However, the theory of intense automorphisms can be extended to a larger family of groups with a striking result. In Chapter 13, we complete the picture by moving to infinite class and computing the *intensity* of infinite pro-p-groups.

We call an automorphism α of a profinite group G *topologically intense* if, for each closed subgroup H of G, there exists an element g in G such that $\alpha(H) = gHg^{-1}$. The group of topologically intense automorphisms of a profinite group G is denoted by $\mathrm{Int_c}(G)$ and it is itself profinite. As a consequence, several results concerning intense automorphisms of finite p-groups can be generalized to topologically intense automorphisms of pro-p-groups. For example, Theorem 13.15 asserts that, if p is a prime number and G is a pro-p-group, then $\mathrm{Int_c}(G)$ decomposes as

$$\mathrm{Int_c}(G) = S_G C_G,$$

where S_G is a Sylow pro-p-subgroup of $\mathrm{Int_c}(G)$ and C_G is isomorphic to a subgroup of $\mathbb{F}_p^*$. Similarly to the finite case, we define the intensity $\mathrm{int}(G)$ of a pro-p-group G to be the order of C_G and we ask which are the infinite pro-p-groups of intensity greater than 1. Surprisingly, this question can be answered much more exhaustively than in the finite case, as follows.

Theorem H. *Let p be a prime number and let G be an infinite pro-p-group. Then $\mathrm{int}(G) > 1$ if and only if exactly one of the following holds.*

1. *One has $p > 2$ and G is abelian.*
2. *One has $p > 3$ and G is topologically isomorphic to $\mathrm{S}(\Delta_p)$.*

Moreover, one has $\mathrm{int}(\mathrm{S}(\Delta_p)) = 2$ and, if G is abelian, then $\mathrm{int}(G) = p - 1$.

Theorem H tells us that, "in the limit", for a given prime number $p > 3$, there is a unique non-abelian pro-p-group, up to isomorphism, of intensity greater than 1. From the point of view of finite groups, this last statement translates into saying that, if $p > 3$ is a prime number, then each finite p-group G with $\mathrm{int}(G) > 1$ shares a "relatively big" quotient (growing in size with the class of G) with the infinite group $\mathrm{S}(\Delta_p)$. In a more definite way, we present this result in Section 13.6.3, under the name of Proposition 13.39.

We conclude our introductory section by giving a "cohomological context" to intense automorphism. As we already mentioned at the beginning of this paper, intense automorphisms arise naturally as solutions to certain problems coming from the field of Galois cohomology and we would like, with these last lines, to make this statement a little less vague. We start by looking at some examples.

Example 1.3. Let k be a field and let n be a positive integer. Moreover, let a be a non-zero element of k. Then the least degree of the irreducible factors of $x^n - a$ divides all other degrees.

Example 1.4. Let k be a field and let $\mathrm{Br}(k)$ denote the group of similarity classes of central simple algebras over k, endowed with the multiplication $\otimes_k$. If $[A] \in \mathrm{Br}(k)$, then an extension ℓ/k is said to *split* A if $[A \otimes_k \ell] = [\ell]$. In [**GT06**, Ch. 4.5], it is proven that the minimal degree of finite separable extensions of k that split a given central simple algebra A over k divides all other degrees.

Example 1.5. Let k be a field and let C be a smooth projective absolutely irreducible curve of genus 1 over k. As a consequence of the Riemann-Roch theorem, as explained for example in [**LT58**, §2], the least degree of the finite extensions of k for which C has a rational point divides all other degrees.

In a quite simplified manner, the last three examples suggest the following question: *When does it happen that "a problem", defined on a base field k, is solvable over a field extension ℓ/k whose degree divides the degrees of all extensions m/k over which the given problem can be solved?* The difficulty of translating this last question into rigorous mathematics is given by the fact that the known examples are quite diverse; however, we can try to unify them from the perspective of Galois cohomology. A first attempt of getting closer to the observed phenomena is Theorem I(1) from [**Sta13**].

Theorem I. *Let G be a finite group. Then the following are equivalent:*

1. *For every G-module M, integer q, and $c \in \widehat{\mathrm{H}}^q(G, M)$, the minimum of the set $\{\, |G : H| \,:\, H \leq G$ with $\mathrm{Res}^G_H(c) = 0 \,\}$ coincides with its greatest common divisor.*
2. *There exist nilpotent groups N and T of coprime orders and a homomorphism $\phi : T \to \mathrm{Int}(N)$ such that $G = N_\phi T$.*

A way to interpret (1) from Theorem I is the following. In some sense, the non-zero elements of a cohomology group are the obstructions to having solutions so, ideally, each subgroup H of G for which $\mathrm{Res}^G_H(c) = 0$ corresponds to a field extension "solving the problem". The merit of Theorem I is that of giving a splendid correspondence between a rather technical cohomological condition and a very concrete requirement regarding intense automorphisms. More about Theorem I and its proof can be found in [**Sta13**].

CHAPTER 2

Coprime Actions

The aim of this chapter is to create tools for later use, giving them however their own chance to shine. In Section 2.1, we define *actions through characters* and prove a fundamental result, Theorem 2.9, in the context of intense automorphisms of groups. In Section 2.2, we prove some elementary, yet quite entertaining, results concerning involutions of groups of odd order. The results from Section 2.2 will spark throughout the paper, starting with Chapter 5. The last section of this chapter, Section 2.3, is dedicated to the theory of *jumps*. In some sense, through jumps (and their width), we are able to recover structural information about subgroups of a given finite p-group. This theory will be heavily used when dealing with p-obelisks (from Chapter 10 onwards).

2.1. Actions through characters

Until the end of Section 2.1, let p be a prime number. Every finite abelian p-group G is naturally a $\mathbb{Z}_p$-module, with scalar multiplication $\mathbb{Z}_p \to \mathrm{End}(G)$ defined by

$$m \mapsto [x \mapsto (m \bmod |G|)\, x]\,.$$

It follows directly from this definition that every homomorphism between abelian p-groups is $\mathbb{Z}_p$-linear, a fact that we will make hidden use of in several proofs from Chapter 2. We remark that we have here adopted the additive notation for the abelian group G, but this will not be the case through the whole paper. We will indeed often deal, instead of abelian groups, with abelian quotients of non-abelian groups (for which the multiplicative notation will be used). The first time we adopt the multiplicative notation in this context is in the proof of Lemma 2.12.

Definition 2.1. Let A be a group acting on a set X. A subset Y of X is *A-stable* (or *stable under the action of A*) if the action of A on X restricts to an action of A on Y.

Definition 2.2. Let A be a group and let $\mathbb{Z}A$ denote its group ring over $\mathbb{Z}$. An *A-module* is a module over $\mathbb{Z}A$.

With respect to the last definition, any finite abelian p-group is naturally a $\mathbb{Z}_p^*$-module. We stress that, if A is a group, then each A-module is, in particular, an abelian group.

Definition 2.3. Let A be a group and let G be a finite p-group that is also an A-module. Let $\chi : A \to \mathbb{Z}_p^*$ be a homomorphism. Then *A acts on G through χ* if, for all $a \in A$ and $x \in G$, one has $ax = \chi(a)x$.

We want to emphasize the fact that $\mathrm{Hom}(A, \mathbb{Z}_p^*)$ is a group under multiplication (induced by that in $\mathbb{Z}_p^*$). We will refer to the elements of $\mathrm{Hom}(A, \mathbb{Z}_p^*)$ as *characters* of A.

Lemma 2.4. *Let X, Y, and Z be finite abelian p-groups. Let A be a group acting on X, Y, and Z and let $\phi : X \times Y \to Z$ be a bilinear map respecting the action of A. Let moreover, χ and ψ be group homomorphisms $A \to \mathbb{Z}_p^*$ such that A acts on X and Y respectively through χ and ψ. Then A acts on $\langle\phi(X \times Y)\rangle$ through $\chi\psi$.*

Proof. For each $(x, y) \in X \times Y$ and $a \in A$, one has $a\phi(x, y) = \phi(ax, ay) = \phi(\chi(a)x, \psi(a)y) = \chi(a)\psi(a)\phi(x, y) = (\chi\psi)(a)\phi(x, y)$. □

Lemma 2.5. *Let p be a prime number and let G be a finite p-group. Let moreover A be a finite group acting on G and let $\chi : A \to \mathbb{Z}_p^*$ be a homomorphism. Denote by $(G_i)_{i\geq 1}$ the lower central series of G and assume that the induced action of A on G/G_2 is through χ. Then, for all $i \in \mathbb{Z}_{\geq 1}$, the induced action of A on G_i/G_{i+1} is through χ^i.*

Proof. We work by induction on i. If $i = 1$, we are done by hypothesis. Suppose now that $i > 1$ and that the result holds for all indices smaller than i. The commutator map induces a bilinear map $G/G_2 \times G_{i-1}/G_i \to G_i/G_{i+1}$ whose image generates G_i/G_{i+1}. By the induction hypothesis, the induced action of A on G_{i-1}/G_i is through χ^{i-1} and so, thanks to Lemma 2.4, the group A acts on G_i/G_{i+1} through $\chi\chi^{i-1} = \chi^i$. □

Lemma 2.6. *Let A be a group and let G and H be finite p-groups that are also A-modules. Let moreover $\phi : G \to H$ and $\chi : A \to \mathbb{Z}_p^*$ be group homomorphisms. Assume that the action of A on G is through χ. If ϕ is surjective and ϕ respects the action of A, then A acts on H through χ.*

Proof. Let $a \in A$ and $g \in G$. Then one has $a\phi(g) = \phi(ag) = \phi(\chi(a)g) = \chi(a)\phi(g)$. □

It is a classical result, which can be found for example in [**Coh07**, §4.3], that the short exact sequence of abelian groups

$$1 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^* \longrightarrow \mathbb{F}_p^* \longrightarrow 1$$

has a unique section $\omega : \mathbb{F}_p^* \to \mathbb{Z}_p^*$, called the *Teichmüller character* at p. The image of ω is contained in the torsion subgroup of $\mathbb{Z}_p^*$ and, if p is odd, $\omega(\mathbb{F}_p^*)$ is in fact equal to the torsion subgroup of $\mathbb{Z}_p^*$ (see e.g. [**Coh07**, §4.3]). We note that, because of the definition of ω, the natural action of $\mathbb{F}_p^*$ on any vector space over $\mathbb{F}_p$ is through the Teichmüller character.

Lemma 2.7. *Let A be a finite group and let $\lambda, \mu : A \to \mathbb{Z}_p^*$ be distinct group homomorphisms. Assume that p is odd. Then there exists $a \in A$ such that the element $\lambda(a) - \mu(a)$ belongs to $\mathbb{Z}_p^*$.*

Proof. Let $\pi : \mathbb{Z}_p \to \mathbb{F}_p$ denote the canonical projection and let $\omega : \mathbb{F}_p^* \to \mathbb{Z}_p^*$ be the Teichmüller character. The group A being finite, the images of λ and μ live in the torsion of $\mathbb{Z}_p^*$, which is equal to $\omega(\mathbb{F}_p^*)$. Let now $a \in A$ be such that $\lambda(a) \neq \mu(a)$. Since each element of $\omega(\mathbb{F}_p^*)$ is uniquely determined by its image modulo p and, the characters being distinct, $\pi(\chi(a) - \psi(a)) \in \mathbb{F}_p^*$. It follows that $\chi(a) - \psi(a)$ is invertible in $\mathbb{Z}_p$. □

Lemma 2.8. *Let A be a finite group and let G be a finite p-group that is also an A-module. Let moreover $\lambda, \mu : A \to \mathbb{Z}_p^*$ be distinct group homomorphisms. Assume that p is odd and that A acts on G through both λ and μ. Then $G = \{0\}$.*

PROOF. Let $x \in G$ and let $a \in A$ be as in Lemma 2.7. Then $\lambda(a)x = ax = \mu(a)x$ and $(\lambda(a) - \mu(a))x = 0$. The element $\lambda(a) - \mu(a)$ being invertible in $\mathbb{Z}_p$, it follows that $x = 0$. □

THEOREM 2.9. *Assume that p is odd. Let A be a finite abelian group and let*

$$0 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} G/N \longrightarrow 0$$

be a short exact sequence of A-modules. Let moreover $\lambda, \mu : A \to \mathbb{Z}_p^*$ be two distinct group homomorphisms and assume that the following hold.

1. *The group G is a finite p-group.*
2. *The group A acts on N through λ.*
3. *The group A acts on G/N through μ.*

Then $\iota(N)$ has a unique A-stable complement in G.

We will devote the remaining part of Section 2.1 to the proof of Theorem 2.9. For this purpose, let $R = \mathbb{Z}_p A$ be the group algebra of A over $\mathbb{Z}_p$ and let σ_λ and σ_μ be the homomorphisms of $\mathbb{Z}_p$-algebras $R \to \mathbb{Z}_p$ that are respectively induced, via linear extension, by λ and μ. We define $I_\lambda = \ker \sigma_\lambda$ and $I_\mu = \ker \sigma_\mu$. Then, as a consequence of Lemma 2.7, there exists $a \in A$ such that the element $\lambda(a) - \mu(a) = -(a - \lambda(a)) + (a - \mu(a))$ is an invertible element of $I_\lambda + I_\mu$: it follows that $R = I_\lambda + I_\mu$. We now claim that $\iota(N)$ has an A-stable complement in G. To this end, let $(e, f) \in I_\lambda \times I_\mu$ be such that $e + f = 1$ in R. As a direct consequence of the definition of I_μ, the group G/N is annihilated by f and $f(G) \subseteq \iota(N)$. From the fact that $f \equiv 1 \bmod I_\lambda$, it follows that $f(G) = \iota(N)$. With a similar argument, one shows that $e(G)$ is isomorphic to $e(G/N) = G/N$. We now have that

$$G = (e + f)G = e(G) + f(G) = e(G) + \iota(N)$$

and so $G = e(G) \oplus \iota(N)$. The ring R being commutative, for all $a \in A$, one has that $ae(G) = ea(G)$ is contained in $e(G)$ and therefore $e(G)$ is an A-stable complement of $\iota(N)$. This proves the claim. We conclude the proof of Theorem 2.9 by proving uniqueness. Assume $\iota(N)$ has two A-stable complements in G. Then there exist maps $f, f' : G \to N$ respecting the action of A such that $f \circ \iota = f' \circ \iota = \mathrm{id}_N$. We fix such f, f' and write $r = f - f'$; we will show that $r = 0$. Since $f \circ \iota = f' \circ \iota$, the subgroup $\iota(N)$ is contained in the kernel of r. It follows that $r \in \mathrm{Hom}(G/\iota(N), N)$, and so, thanks to Lemma 2.6, the group A acts on the image of r through μ. On the other hand, the image of r is contained in N and hence the action of A on $r(G)$ is also through λ. It follows from Lemma 2.8 that $r = 0$, as claimed. In particular, $f = f'$, and so $\iota(N)$ has a unique A-stable complement in G. The proof of Theorem 2.9 is now complete.

2.2. Involutions

Let G be a finite group of odd order and let $A = \langle \alpha \rangle$ be a multiplicative group of order 2. It follows that the orders of G and A are coprime. Assume that A acts on G and define

$$G^+ = \{g \in G : \alpha(g) = g\} \quad \text{and} \quad G^- = \{g \in G : \alpha(g) = g^{-1}\}.$$

It is not difficult to show that $G^+ \cap G^- = \{1\}$ and that G^+ is a group acting by conjugation on the set G^-. We keep the notation we just introduced until the end of Section 2.2.

LEMMA 2.10. *The map $G/G^+ \to G^-$ that is defined by $xG^+ \mapsto x\alpha(x)^{-1}$ is a bijection. Moreover, $|G| = |G^+||G^-|$.*

PROOF. Denote by ϕ the map $G/G^+ \to G^-$ that is defined by $xG^+ \mapsto x\alpha(x)^{-1}$. To show that ϕ is injective is a straightforward exercise. To prove that it is surjective, we take $b \in G^-$ and we let $a \in G$ be such that $a^2 = b$. Since a belongs to $\langle b \rangle$, we have $\alpha(a) = a^{-1}$ and therefore $a\alpha(a)^{-1} = a^2 = b$. We have proven that ϕ is a bijection, from which it follows that $|G|/|G^+| = |G^-|$. □

LEMMA 2.11. *The map $G^+ \times G^- \to G$, defined by $(x, y) \mapsto xy$, is a bijection.*

PROOF. Let (x, y) and (z, t) be elements of $G^+ \times G^-$ satisfying $xy = zt$. Then $ty^{-1} = z^{-1}x$ is an element of G^+ and thus $ty^{-1} = \alpha(ty^{-1}) = t^{-1}y$. It follows that $t^2 = y^2$ so, the order of G being odd, $t = y$. Consequently, $(x, y) = (z, t)$ and the map is injective. Lemma 2.10 yields that the given multiplication is also surjective. □

Assume G is abelian. Then $G = G^+ \oplus G^-$.

LEMMA 2.12. *Let N be a normal A-stable subgroup of G such that the restriction of α to N equals the map $x \mapsto x^{-1}$. Assume moreover that the automorphism of G/N that is induced by α is equal to the inversion map $g \mapsto g^{-1}$. Then $G = G^-$ and G is abelian.*

PROOF. For each $x \in G$, the element $\alpha(x)x$ belongs to N and so, the order of G being odd, the subgroup G^+ is contained in N. It follows that G^+ is contained in G^- and so G^+ is trivial. As a consequence of Lemma 2.11, the group G is equal to G^-, which is a group if and only if any two of its elements commute. It follows that G is abelian. □

In a similar way, one can prove the following result.

LEMMA 2.13. *Let N be a normal A-stable subgroup of G. Assume that the action of A on N and the induced action of A on G/N are both trivial. Then $G = G^+$.*

LEMMA 2.14. *Let $1 \to N \xrightarrow{f} G \xrightarrow{g} \Gamma \to 1$ is a short exact sequence of A-groups. Denote by f' and g' the restrictions of f and g respectively to N^+ and G^+. Then $1 \to N^+ \xrightarrow{f'} G^+ \xrightarrow{g'} \Gamma^+ \to 1$ is a short exact sequence of A-groups.*

PROOF. We prove the surjectivity of g'. Let $\gamma \in \Gamma^+$. Then there exists $x \in G$ such that $g(x) = \gamma$ and, by Lemma 2.11, there exists $(a, b) \in G^+ \times G^-$ such that $x = ab$. Now, the pair $(g(a), g(b))$ belongs to $\Gamma^+ \times \Gamma^-$ and so $g(b) = g(a)^{-1}\gamma \in \Gamma^+ \cap \Gamma^- = \{1\}$. As a result, one has $\gamma = g(a)$. □

LEMMA 2.15. *Let H be an A-stable subgroup of G and let g be an element of G. Then the following are equivalent.*

1. *The subgroup gHg^{-1} is A-stable.*
2. *The element g belongs to $G^+ \mathrm{N}_G(H)$.*

PROOF. Let $I = \mathrm{N}_G(H)$; then I is A-stable, because H is. We first prove that (1) implies (2). It follows from the assumptions that $\alpha(gHg^{-1}) = gHg^{-1}$ and so $g^{-1}\alpha(g)$ belongs to I. As a consequence, $\alpha(gI) = \alpha(g)I = gI$ and so, the cardinality of I being odd, there is an element x in I such that $\alpha(gx) = gx$. For such an element x, we then have that $gx \in G^+$, so $g = gx \cdot x^{-1} \in G^+I$. Assume now (2) is satisfied. Since g belongs to G^+I, there exists $(\gamma, n) \in G^+ \times I$ such that $g = \gamma n$. For such pair (γ, n), we have that $gHg^{-1} = \gamma H \gamma^{-1}$, and therefore $\alpha(gHg^{-1}) = gHg^{-1}$. This proves (1). □

2.3. Jumps and width

Let p be a prime number and let G be a finite p-group. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. If x is a non-trivial element of G, then there exists a positive integer d such that $x \in G_d \setminus G_{d+1}$. The number d is called the *depth* of x (in G) and it is denoted by $\mathrm{dpt}_G(x)$. Let now H be a subgroup of G and let j be a positive integer. The *j-th width of H in G* is

$$\mathrm{wt}_H^G(j) = \log_p |H \cap G_j : H \cap G_{j+1}|.$$

We observe that, if $\pi_j : G_j \to G_j/G_{j+1}$ denotes the canonical projection, then $\pi_j(H \cap G_i)$ has cardinality $p^{\mathrm{wt}_H^G(j)}$. An index j is a *jump of H in G* if $\mathrm{wt}_H^G(j) \neq 0$ and, whenever it will be clear that j is a jump of H in G, we will refer to $\mathrm{wt}_H^G(j)$ as the *width of j in G*. If $G = H$, we denote the *j-th width of G* by $\mathrm{wt}_G(j)$ instead of $\mathrm{wt}_G^G(j)$ and, in several results, we will lighten the notation even further by writing $w_j = \mathrm{wt}_G(j)$. The *width of G* is defined as $\mathrm{wt}(G) = \max_{i\geq 1} \mathrm{wt}_G(i)$; for a generalization to general pro-p-groups, see [**KLGP97**].

In the following lemma, we collect some straightforward properties of jumps.

Lemma 2.16. *Let p be a prime number, let G be a finite p-group, and let H be a subgroup of G. Then the following are satisfied.*

1. *If $\alpha \in \mathrm{Aut}(G)$, then H and $\alpha(H)$ have the same jumps in G.*
2. *Let $j \in \mathbb{Z}_{>0}$. Then j is a jump of H in G if and only if H contains an element of depth j in G.*
3. *Let $\mathcal{J}$ be the collection of all jumps of H in G. Then $|H| = \prod_{j\in\mathcal{J}} p^{\mathrm{wt}_H^G(j)}$.*

Lemma 2.17. *Let p be an odd prime number and let G be a finite p-group. Let $A = \langle \alpha \rangle$ be a multiplicative group of order 2 acting on G. Let $\chi : A \to \{\pm 1\}$ be an isomorphism. Let $(G_i)_{i\geq 1}$ denote the lower central series of G and assume that the induced action of A on G/G_2 is through χ. Let H be an A-stable subgroup of G and let $\mathcal{O}$ and $\mathcal{E}$ be the collections of respectively all odd and all even jumps of H in G. Then the following hold.*

1. *One has $|H^+| = \prod_{j\in\mathcal{E}} p^{\mathrm{wt}_H^G(j)}$ and $\mathcal{E}$ is the set of jumps of H^+ in G.*
2. *One has $|H^-| = \prod_{j\in\mathcal{O}} p^{\mathrm{wt}_H^G(j)}$.*

Proof. For all $j \in \mathbb{Z}_{\geq 1}$, we define $V_j = (H \cap G_j)/(H \cap G_{j+1})$ and we consider the short exact sequence

$$1 \to H \cap G_{j+1} \to H \cap G_j \to V_j \to 1$$

of A-groups. If $j \in \mathbb{Z}_{\geq 1}$, we note that $(H \cap G_j)^+ = H^+ \cap G_j$, so Lemma 2.14 yields

$$|H^+ \cap G_j : H^+ \cap G_{j+1}| = |V_j^+|.$$

From Lemma 2.5 it follows that A acts on G_j/G_{j+1} by scalar multiplication by $(-1)^j$, and so, whenever j is an odd positive integer, the group $(G_j/G_{j+1})^+$ is trivial and thus so is V_j^+. On the other hand, if j is even, then V_j is equal to V_j^+. The cardinality of H^+ being equal to $\prod_{j\geq 1}|H^+ \cap G_j : H^+ \cap G_{j+1}|$, we get that

$$|H^+| = \prod_{j\geq 1}|V_j^+| = \prod_{j\in\mathcal{E}}|V_j^+| = \prod_{j\in\mathcal{E}}|V_j| = \prod_{j\in\mathcal{E}} p^{\mathrm{wt}_H^G(j)}.$$

Lemma 2.10 now yields $|H^-| = |H|/|H^+| = \prod_{j\in\mathcal{O}} p^{\mathrm{wt}_H^G(j)}$. □

CHAPTER 3

Intense Automorphisms

Let G be a group. An automorphism α of G is *intense* if for every subgroup H of G there exists $g \in G$ such that $\alpha(H) = gHg^{-1}$. We denote by $\mathrm{Int}(G)$ the collection of all intense automorphisms of G, which is easily seen to be a normal subgroup of $\mathrm{Aut}(G)$. A clear example of intense automorphisms is given by inner automorphisms, but, as we will see, one can builm more interesting ones.

In this chapter we will prove some basic properties of intense automorphisms and formulate the main research question of this paper. Among others, we will prove the following result.

Theorem 3.1. *Let p be a prime number and let G be a finite p-group. Then $\mathrm{Int}(G)$ is isomorphic to SC, where S is a Sylow p-subgroup of $\mathrm{Int}(G)$ and C is a subgroup of $\mathbb{F}_p^*$. Moreover, if G is non-trivial abelian, then $C = \mathbb{F}_p^*$.*

3.1. Basic properties

Section 3.1 is devoted to basic properties of intense automorphisms. The next lemma is a collection of the most straightforward ones.

Lemma 3.2. *Let G be a group and let N be a normal subgroup of G. Then the following hold.*

1. *The subgroup N is $\mathrm{Int}(G)$-stable.*
2. *The natural projection $G \to G/N$ induces a well-defined homomorphism $\mathrm{Int}(G) \to \mathrm{Int}(G/N)$, by means of $\alpha \mapsto (xN \mapsto \alpha(x)N)$.*

In the following lemma, $\omega : \mathbb{F}_p^* \to \mathbb{Z}_p^*$ is the Teichmüller character at p, as defined in Section 2.1.

Lemma 3.3. *Let p be a prime number and let V be a vector space over $\mathbb{F}_p$. Then there exists a unique injective homomorphism $\lambda : \mathrm{Int}(V) \to \mathbb{Z}_p^*$ such that the following hold.*

1. *The group $\mathrm{Int}(V)$ acts on V through λ.*
2. *If $V \neq 0$, then $\lambda(\mathrm{Int}(V)) = \omega(\mathbb{F}_p^*)$.*

Proof. If $V = 0$, define $\lambda : \mathrm{id}_V \mapsto 1$. Assume $V \neq 0$. Since V is abelian, every one-dimensional subspace of V is stable under the action of $\mathrm{Int}(V)$. It follows that, for all $v \in V \setminus \{0\}$ and $\alpha \in \mathrm{Int}(V)$, there exists (a unique) $\mu(\alpha, v) \in \mathbb{F}_p^*$ such that $\alpha(v) = \mu(\alpha, v)v$. Because of the linearity of α, the value of $\mu(\alpha, v)$ is independent of the choice of v: we fix thus $v \in V \setminus \{0\}$ and define $\mu : \mathrm{Int}(V) \to \mathbb{F}_p^*$ by $\alpha \mapsto \mu(\alpha, v)$. The map μ is an injective homomorphism of groups by construction. Moreover, μ is surjective, because scalar multiplication by any element of $\mathbb{F}_p^*$ is an intense automorphism of V. We define $\lambda = \omega \circ \mu$. Then $\mathrm{Int}(V)$ acts on V through λ and the image of λ is equal to $\omega(\mathbb{F}_p^*)$. The uniqueness of λ follows from Lemma 2.8. □

Lemma 3.4 (Glauberman's lemma). *Let G and A be finite groups of coprime orders. Assume that at least one of A and G is solvable. Assume A acts on G and that each of them acts on some set X, where the action of G is transitive. Finally, assume the three actions are compatible. Then there exists an A-stable element in X.*

Proof. See [**Isa08**, Lemma 3.24]. □

Lemma 3.5. *Let G be a finite group and let $\alpha \in \mathrm{Aut}(G)$ be of order coprime to the order of G. Let H and N be subgroups of G and assume that $\alpha(N) = N$. Then the following are equivalent.*

1. *There exists $a \in N$ such that $\alpha(H) = aHa^{-1}$.*
2. *There exists $b \in N$ such that bHb^{-1} is $\langle\alpha\rangle$-stable.*

Moreover, $\alpha \in \mathrm{Int}(G)$ if and only if each subgroup of G has an $\langle\alpha\rangle$-stable conjugate.

Proof. The implication (2) ⇒ (1) is easy so we prove the other one. Assume (1) holds and write $X = \{gHg^{-1} : g \in N\}$. Then N acts on X by conjugation and $\langle\alpha\rangle$ acts on X by assumption. The actions are compatible and the action of N is transitive. By Lemma 3.4, there exists an element of X that is fixed by α. This proves (2). To prove that $\alpha \in \mathrm{Int}(G)$ if and only if any subgroup of G has a $\langle\alpha\rangle$-stable conjugate, it now suffices to take $N = G$. □

Lemma 3.6. *Let G be a finite group and let $\alpha \in \mathrm{Int}(G)$ be of order coprime to the order of G. Let X be a collection of subgroups of G on which G acts by conjugation and let $X^+ = \{H \in X : \alpha(H) = H\}$. Then*

$$|X| \leq \sum_{H \in X^+} |G : \mathrm{N}_G(H)|.$$

Equality holds if and only if the elements of X^+ are pairwise non-conjugate in G.

Proof. Let $\mathcal{C}$ be the collection of orbits of X under G. By Lemma 3.5, there exists a subset $\mathcal{R}$ of X^+ whose elements are representatives for the elements of $\mathcal{C}$. It follows that

$$|X| = \sum_{C \in \mathcal{C}} |C| = \sum_{H \in \mathcal{R}} |G : \mathrm{N}_G(H)| \leq \sum_{H \in X^+} |G : \mathrm{N}_G(H)|.$$

Equality holds if and only if $\mathcal{R} = X^+$. □

3.2. The main question

In Section 3.2 we build the foundation for our theory and we give the dictionary that we will use throughout the whole paper. We will also prove the following result.

Proposition 3.7. *Let G be a finite 2-group. Then $\mathrm{Int}(G)$ is a finite 2-group.*

Definition 3.8. Let p be a prime number and let G be a finite p-group. The *intense character* of G is the homomorphism $\chi_G : \mathrm{Int}(G) \to \mathbb{Z}_p^*$ that is gotten from the composition of the following.

- ○ The homomorphism $\mathrm{Int}(G) \to \mathrm{Int}(G/\Phi(G))$ from Lemma 3.2(2).
- ○ The homomorphism $\lambda : \mathrm{Int}(G/\Phi(G)) \to \mathbb{Z}_p^*$ from Lemma 3.3.

Lemma 3.9. *Let p be a prime number and let G be a finite p-group. Let moreover $\chi_G : \mathrm{Int}(G) \to \mathbb{Z}_p^*$ be the intense character of G. Then the group $\ker \chi_G$ is the unique Sylow p-subgroup of $\mathrm{Int}(G)$.*

Proof. If G is the trivial group, then $\mathrm{Int}(G) = \ker \chi_G = \{1\}$. Assume now G is non-trivial and set $V = G/\Phi(G)$. Let moreover $\phi : \mathrm{Aut}(G) \to \mathrm{Aut}(V)$ be the natural homomorphism. By Lemma 3.3, the map $\lambda : V \to \mathrm{Int}(V)$ is injective and so $\ker \chi_G = \mathrm{Int}(G) \cap \ker \phi$. The kernel of ϕ being a normal p-subgroup of $\mathrm{Aut}(G)$, the kernel of χ_G is a normal Sylow p-subgroup of $\mathrm{Int}(G)$. □

Definition 3.10. Let p be a prime number and let G be a finite p-group. Let $\chi_G : \mathrm{Int}(G) \to \mathbb{Z}_p^*$ be the intense character of G. The *intensity* of G is $\mathrm{int}(G) = |\mathrm{Int}(G) : \ker \chi_G|$.

We remark that the intensity of a p-group G is equal to the size of the image of the intense character χ_G inside $\omega(\mathbb{F}_p^*)$. In particular, if G is a 2-group, then its intensity is always 1. The next lemma implies Proposition 3.7.

Lemma 3.11. *Let p be a prime number and let G be a finite p-group. Then $\mathrm{int}(G)$ divides $p-1$ and $\ker \chi_G$ has a cyclic complement in $\mathrm{Int}(G)$ of order $\mathrm{int}(G)$.*

Proof. The group $\chi_G(\mathrm{Int}(G))$ is contained in $\omega(\mathbb{F}_p^*)$. It follows that $\mathrm{int}(G)$ divides $p-1$ and, from Proposition 3.9 and the Schur-Zassenhaus theorem, that $\ker \chi_G$ has a cyclic complement in $\mathrm{Int}(G)$ of order $\mathrm{int}(G)$. □

The major goal of this paper if classifying all pairs (p, G) where p is a prime number and G is a finite p-group with $\mathrm{int}(G) > 1$. Because of Proposition 3.7, we will therefore often be working with odd primes. Explicit assumptions will be made at the beginning of each section.

3.3. The abelian case

In the present section we treat the case of abelian p-groups. In that respect, we prove the following proposition, which is the main result of Section 3.3.

Proposition 3.12. *Let p be a prime number and let G be a finite non-trivial abelian p-group. Then $\mathrm{int}(G) = p - 1$.*

Lemma 3.13. *Let p be a prime number, let G be a finite p-group, and let N be a normal subgroup of G. If $N \neq G$, then $\mathrm{int}(G)$ divides $\mathrm{int}(G/N)$.*

Proof. Assume $N \neq G$ and let $\phi : \mathrm{Int}(G) \to \mathrm{Int}(G/N)$ be as in Lemma 3.2(2). The subgroup $N\Phi(G)$ being different from G, one has $\chi_G = \chi_{G/N} \circ \phi$. It follows that the image of χ_G is contained in the image of $\chi_{G/N}$ and thus $\mathrm{int}(G)$ divides $\mathrm{int}(G/N)$. □

We recall that a group A acts through a character on a finite abelian p-group G if there exists a homomorphism $\chi : A \to \mathbb{Z}_p^*$ such that, for all $a \in A$ and $x \in G$, one has $ax = \chi(a)x$. For more details, see Section 2.1.

Lemma 3.14. *Let p be a prime number and let G be a finite abelian p-group. Let α be an intense automorphism of order dividing $\mathrm{int}(G)$ and write $\chi = \chi_{G|\langle\alpha\rangle}$. Then $\langle\alpha\rangle$ acts on G through χ and, if G is non-trivial, then $\mathrm{int}(G) = p - 1$.*

Proof. Write $A = \langle \alpha \rangle$. If G is the trivial group, then the only automorphism of G is the identity, which is intense. Assume now G is non-trivial. The group $\omega(\mathbb{F}_p^*)$ acts on G (as described at the beginning of Section 2.1) via intense automorphisms and it induces scalar multiplication by elements of $\mathbb{F}_p^*$ on $G/\Phi(G)$. The image of the intense character of G is thus $\omega(\mathbb{F}_p^*)$, and so, $\mathrm{int}(G) = p - 1$. Let now Ω denote the image of $\omega(\mathbb{F}_p^*) \to \mathrm{Int}(G)$ and write $\Omega = \langle \beta \rangle$. Then $\mathrm{Int}(G) = \ker \chi_G \Omega$, and, as a consequence of Schur-Zassenhaus, there exist $m \in \mathbb{Z}_{\geq 0}$ and $\gamma \in \ker \chi_G$ such that $\alpha = \gamma \beta^m \gamma^{-1}$. We get

$$\chi(\alpha) = \chi_G(\alpha) = \chi_G(\gamma \beta^m \gamma^{-1}) = \chi_G(\beta^m).$$

Since each homomorphism of abelian groups is $\mathbb{Z}_p$-linear and Ω acts on G through $\chi_{G|\Omega}$, the group A acts on G through χ. □

We remark that Proposition 3.12 is a special case of Lemma 3.14. Moreover, Theorem 3.1 is proven by combining Lemmas 3.9, 3.11, and Proposition 3.12.

Let p be a prime number and let G be a finite p-group. Let moreover α be an intense automorphism of G of order dividing $\mathrm{int}(G)$. Then $\langle \alpha \rangle$ acts on the centre of G through a character $\langle \alpha \rangle \to \mathbb{Z}_p^*$.

Proof. The group $\mathrm{Z}(G)$ being normal in G, Lemma 3.2(1) yields a map $\zeta : \mathrm{Int}(G) \to \mathrm{Aut}(\mathrm{Z}(G))$ whose image is easily seen to be contained in $\mathrm{Int}(\mathrm{Z}(G))$. Set now $A = \langle \alpha \rangle$ and define $\sigma = \chi_{\mathrm{Z}(G)|\zeta(A)} \circ \zeta_{|A}$. Then, as a consequence of Lemma 3.9, the group A acts on $\mathrm{Z}(G)$ through σ. □

Lemma 3.15. *Let p be a prime number and let G be a finite p-group. Let α be an intense automorphism of G of order dividing* $\mathrm{int}(G)$ *and write $A = \langle \alpha \rangle$ and $\chi = \chi_{G|A}$. Denote by $(G_i)_{i \geq 1}$ the lower central series of G. Then, for all $i \in \mathbb{Z}_{\geq 1}$, the induced action of A on G_i/G_{i+1} is through χ^i.*

Proof. As a consequence of Lemma 3.2(2), the action of A on G induces an action of A on G/G_2. By Lemma 3.14, the action of A on G/G_2 is through χ. We now apply Lemma 2.5. □

CHAPTER 4

Intensity of Groups of Class 2

The main goal of this paper, as stated in Section 3.2, is to classify all finite p-groups whose group of intense automorphisms is not itself a p-group. We will proceed to a classification by separating the cases according to the class of the p-groups. If the class is 0, the group is trivial and the intensity is 1. For the case in which the class is 1 (non-trivial abelian case) we refer to Chapter 3. In this chapter we study the case in which the class is equal to 2. We prove the following main result.

Theorem 4.1. *Let p be a prime number and let G be a finite p-group of class 2. Then the following are equivalent.*

1. *One has* $\mathrm{int}(G) \neq 1$.
2. *The group G is extraspecial of exponent p.*
3. *The prime p is odd and* $\mathrm{int}(G) = p - 1$.

4.1. Small commutator subgroup

Let p be a prime number. We recall that a group A acts on a finite abelian p-group G through a character if there exists a homomorphism $\chi : A \to \mathbb{Z}_p^*$ such that, for all $x \in G$, $a \in A$, one has $ax = \chi(a)x$. For more detail about actions through characters see Section 2.1.

Until the end of Section 4.1, the following assumptions will be valid. Let p be a prime number, let G be a finite p-group of nilpotency class 2, and let $(G_i)_{i\geq 1}$ denote the lower central series of G. Let moreover α be intense of order $\mathrm{int}(G)$. Write $A = \langle\alpha\rangle$ and $\chi = \chi_{G|A}$. Assume that the intensity of G is greater than 1. It follows that G is non-trivial, that p is odd (see Sections 3.2 and 3.3), and that $\chi \neq \chi^2$.

Lemma 4.2. *Assume G_2 has exponent p. Then $\mathrm{Z}(G) = \Phi(G) = G_2$ and A acts on $\mathrm{Z}(G)$ through χ^2.*

Proof. The group G_2 is a non-trivial subgroup of $\mathrm{Z}(G)$ and, by Lemma 3.15, the group A acts on G_2 through χ^2. By Corollary 3.3, the group A acts on $\mathrm{Z}(G)$ through a character and, as a consequence of Lemma 2.8, the action of A on the centre is through χ^2. On the other hand, by Lemma 3.15, the induced action of A on G/G_2 is through χ. The group A acts hence on $\mathrm{Z}(G)/G_2$ both through χ and χ^2. The characters χ and χ^2 being distinct, Lemma 2.8 yields $\mathrm{Z}(G) = G_2$. Since G_2 is elementary abelian, the subgroup $\Phi(G)$ is central, and thus $G_2 = \Phi(G) = \mathrm{Z}(G)$. □

Lemma 4.3. *Assume G_2 has order p. Then G is extraspecial of exponent p.*

Proof. Thanks to Lemma 4.2 we are only left with showing that G has exponent p. Assume by contradiction that there exists $g \in G$ of order p^2 and write

$H = \langle g \rangle$. Then H^p has order p and, as a consequence of Lemma 4.2, the subgroup H contains $\Phi(G)$. In particular, H is normal in G and thus A-stable. As a consequence of Lemma 3.15, the actions of A on H/G_2 and G_2 are respectively through χ and χ^2 and so, χ and χ^2 being distinct, it follows from Theorem 2.9 that H and $(H/G_2) \oplus G_2$ are isomorphic. Contradiction. □

Lemma 4.4. *Let Q be a finite p-group of both class and intensity greater than 1. Denote by $(Q_i)_{i\geq 1}$ the lower central series of Q. Then, for all $i \in \mathbb{Z}_{\geq 1}$, the exponent of Q_i/Q_{i+1} divides p.*

Proof. We work by induction on i. Let first $i = 1$ and let M be a normal subgroup of Q that is contained in Q_2 with index p. We write $\overline{Q} = Q/M$ and use the bar notation for the subgroups of $\overline{Q}$. Then $\overline{Q_2} = [\overline{Q}, \overline{Q}]$ has order p and $\overline{Q}$ has intensity greater than 1, by Lemma 3.13. From Lemma 4.3, it follows that $\overline{Q}/\overline{Q_2}$ is elementary abelian and therefore so is Q/Q_2. Assume now that i is greater than 1 and that the result holds for all indices smaller than i. The property of being annihilated by p is preserved by tensor products and surjective homomorphisms so, since the commutator map induces a surjective homomorphism $Q/Q_2 \otimes Q_{i-1}/Q_i \to Q_i/Q_{i+1}$, the exponent of Q_i/Q_{i+1} divides p. □

Let Q be a finite p-group of nilpotency class 2. If $\mathrm{int}(Q) > 1$, then $\mathrm{Z}(Q) = Q_2$.

Proof. This follows directly from Lemmas 4.4 and 4.2. □

4.2. More general setting

Throughout Section 4.2, let p be a prime number and let G be a finite p-group of class 2 and intensity greater than 1. Let α be intense of order $\mathrm{int}(G)$ and write $A = \langle \alpha \rangle$ and $\chi = \chi_{G|A}$. It follows from the work done in Sections 3.2 and 3.3 that G is not trivial, that p is odd, and that $\chi \neq \chi^2$. We denote by V and Z respectively G/G_2 and G_2 and by π the canonical projection $G \to V$. From Lemma 4.4 it follows that both V and Z are vector spaces over $\mathbb{F}_p$. By Corollary 4.1, the non-trivial subgroup Z is equal to $\mathrm{Z}(G)$ and so the map $\phi : V \times V \to Z$ that is induced by the commutator map is alternating.

Lemma 4.5. *Let H be a linear subspace of Z of codimension 1. Then the map $\phi_H : V \times V \to Z/H$, defined by $(x, y) \mapsto \phi(x, y) + H$, is non-degenerate. Moreover, $\dim V$ is even.*

Proof. The subgroup H is contained in the centre Z and is therefore a normal subgroup of G. It follows from Lemma 3.13 that $\mathrm{int}(G/H) > 1$. As a consequence of Lemma 4.3, the group G/H is extraspecial, and so the map $\phi_H : V \times V \to Z/H = [G/H, G/H]$ is non-degenerate. The dimension of Z/H being 1, it follows from linear algebra that $\dim V$ is even. □

In the proof of Theorem 4.1, an important role is played by *isotropic subspaces* of V associated to ϕ, i.e. linear subspaces T of V such that $\phi(T \times T) = 0$. It is not difficult to show that, because of the definition of ϕ, a linear subspace T of V is isotropic if and only if $\pi^{-1}(T)$ is abelian. The next lemma is a standard result and its proof is straightforward.

Lemma 4.6. *Let Γ be a group, let N be a central subgroup, and let H be a complement of N in Γ. Let moreover $\mathcal{C}_N$ be the collection of complements of N*

in Γ and, for all $f \in \mathrm{Hom}(H,N)$, call $\mathcal{G}_f = \{f(h)h : h \in H\}$. Then the map $\mathrm{Hom}(H,N) \to \mathcal{C}_N$, given by $f \mapsto \mathcal{G}_f$, is well-defined and bijective.

LEMMA 4.7. *Let T be an isotropic subspace of V. Then the map $\phi_T : V/T \to \mathrm{Hom}(T,Z)$, defined by $v + T \mapsto (t \mapsto \phi(v,t))$, is surjective.*

PROOF. Let T be an isotropic subspace of V. Then $\pi^{-1}(T)$ is abelian and it contains Z. It follows that $\pi^{-1}(T)$ is normal and so A-stable. By Lemma 3.15, the actions of A on $\pi^{-1}(T)/Z$ and on Z are respectively through χ and χ^2, which are distinct. By Theorem 2.9 the subgroup Z has hence a unique A-stable complement H in $\pi^{-1}(T)$, which is isomorphic to T via π. Let now $f \in \mathrm{Hom}(T,Z)$ and note that $\mathrm{Hom}(T,Z)$ and $\mathrm{Hom}(H,Z)$ are naturally isomorphic. We identify f with its image in $\mathrm{Hom}(H,Z)$. By Lemma 4.6, the set $L = \{f(t)t \mid t \in H\}$ is a complement of Z in $\pi^{-1}(T)$ and so, being H the unique A-stable complement of Z, Lemma 3.5 guarantees that there exists $g \in G$ such that $L = gHg^{-1}$. Fix such an element g. Then, for each $h \in H$, there exists $t \in H$ such that $[g,h]h = ghg^{-1} = f(t)t$. It follows that $ht^{-1} = [h,g]f(t)$ belongs to both H and Z, but H and Z intersect trivially, so $h = t$. We have proven that f is the map $t \mapsto [g,t]$ and thus, the choice of f being arbitrary, ϕ_T is surjective. □

A subspace of V is *maximal isotropic* with respect to ϕ if it is isotropic and if it is not properly contained in any other isotropic subspace of V. As a consequence of Lemma 4.7, a subspace T of V is maximal isotropic if and only if the map $\phi_T : V/T \to \mathrm{Hom}(T,Z)$ is a bijection.

LEMMA 4.8. *The dimension of Z is different from* 2.

PROOF. Assume by contradiction that Z has dimension 2. Let T be an isotropic subspace of V of maximal dimension t and let $d = \dim V$, which is positive. Since ϕ_T is a bijection, we have that $d = 3t$ and in particular that $t > 0$. Let L be a subspace of T of codimension 1, which is itself isotropic. Let moreover $\phi_L : V/L \to \mathrm{Hom}(L,Z)$ be defined by $v + L \mapsto (l \mapsto \phi(v,l))$. The linear map ϕ_L is surjective by Lemma 4.7. Let U be the kernel of ϕ_L and let $\phi_U : U \times U \to Z$ be induced by ϕ. Then $\dim U = d - 3(t-1) = 3$ and ϕ_U is alternating. By the universal property of wedge products, there exists a unique linear map $\psi : \bigwedge^2 U \to Z$ that, composed with the canonical map $U \times U \to \bigwedge^2 U$, gives ϕ_U. The dimension of $\bigwedge^2 U$ being 3, the map $U \times U \to \bigwedge^2 U$ is surjective and the dimension of $\ker\psi$ is positive.There are thus linearly independent elements $s, r \in U$ such that $\psi(s \wedge r) = 0$. Set $R = L \oplus \mathbb{F}_p s \oplus \mathbb{F}_p r$. By construction, R is an isotropic subspace of V of dimension $t+1$. Contradiction to the maximality of t. □

The group G is extraspecial of exponent p.

PROOF. If G_2 has order p, then G is extraspecial of exponent p, by Lemma 4.3. We claim that the order of G_2 is in fact p. Assume by contradiction that G_2 has order larger than p and let M be a normal subgroup of G that is contained in G_2 with index p^2. The group G/M has class 2 and, by Lemma 3.13, its intensity is greater than 1. This is a contradiction to Lemma 4.8, with G_2/M in the role of Z. □

We remark that Corollary 4.2 gives (1) ⇒ (2) in Theorem 4.1. We complete the proof in the next section.

4.3. The extraspecial case

In Section 4.3 we will see how the structure of extraspecial groups of exponent p is particularly suitable for explicit construction of intense automorphisms of order coprime to p. In this section, we conclude the proof of Theorem 4.1.

Lemma 4.9. *Let p be a prime number and let G be an extraspecial group of exponent p. Let moreover H be a subgroup of G that trivially intersects G_2. Then $|G : \mathrm{N}_G(H)| = |\operatorname{Hom}(H, G_2)|$.*

Proof. The subgroup $H \cap G_2$ is trivial and therefore $\mathrm{N}_G(H) = \mathrm{C}_G(H)$ and H is abelian. Moreover, the commutator map $G \times G \to G_2$ is bilinear and, since $H \cap \mathrm{Z}(G)$ is trivial, it induces a non-degenerate map $G/\mathrm{C}_G(H) \times H \to G_2$. Now, both $G/\mathrm{C}_G(H)$ and H are $\mathbb{F}_p$-vector spaces and G_2 has order p. It follows from linear algebra that $|G : \mathrm{N}_G(H)| = |G : \mathrm{C}_G(H)| = |H| = |\operatorname{Hom}(H, G_2)|$. □

Lemma 4.10. *Let p be a prime number and let G be an extraspecial group of exponent p. Let α be an automorphism of G such that $\langle\alpha\rangle$ acts on G/G_2 through a character. Then $\alpha \in \operatorname{Int}(G)$.*

Proof. Let H be a subgroup of G and write $A = \langle\alpha\rangle$. We want to show that H and $\alpha(H)$ are conjugate in G. Since G_2 has order p, either H contains G_2 or the intersection of H with G_2 is trivial. In the first case, H/G_2 is a linear subspace of G/G_2, and is therefore A-stable; in particular, H is A-stable. We now consider the case in which $H \cap G_2 = \{1\}$. In this case, H is abelian and the group $T = H \oplus G_2$ is A-stable. The group G_2 being A-stable, $\alpha(H)$ is a complement of G_2 in T. Also each G-conjugate of H is a complement of G_2 in T, because G_2 and T are both normal. By Lemma 4.6, the number of complements of G_2 in T equals the cardinality of $\operatorname{Hom}(H, G_2)$, which is equal to $|G : \mathrm{N}_G(H)|$ by Lemma 4.9. As all conjugates of H are themselves complements of G_2 in T, every complement of G_2 in T is conjugate to H in G. In particular, H and $\alpha(H)$ are conjugate in G. □

Lemma 4.11. *Let p be a prime number and let G be an extraspecial p-group of exponent p. Then p is odd and $\operatorname{int}(G) = p - 1$.*

Proof. The prime p is odd, because all groups of exponent 2 are abelian. We show that $\operatorname{int}(G) = p - 1$. Since G is extraspecial of exponent p, there exist finite-dimensional vector spaces X, Y, Z over $\mathbb{F}_p$, with $\dim_{\mathbb{F}_p} Z = 1$, and a non-degenerate bilinear map $\theta : X \times Y \to Z$ such that G is isomorphic to the group $G(Z, Y, X, \theta)$ whose underlying set is $Z \times Y \times X$ and whose multiplication is defined by

$$(z, y, x)(z', y', x') = (z + z' + \theta(x, y'), y + y', x + x').$$

Now, the group $\mathbb{F}_p^*$ acts on X, Y, and Z, as described in Section 2.1, and so each $m \in \mathbb{F}_p^*$ gives rise to an automorphism of each of the three vector spaces. Moreover, by the bilinearity of θ, for each $m \in \mathbb{F}_p^*$, the following diagram is commutative.

$$\begin{tikzcd}
X \times Y \arrow[r, "\theta"] \arrow[d, shift right, "m"'] \arrow[d, shift left, "m"] & Z \arrow[d, "m^2"'] \\
X \times Y \arrow[r, "\theta"] & Z
\end{tikzcd}$$

Thanks to the definition of $G(Z, Y, X, \theta)$, one can show that, for each $m \in \mathbb{F}_p^*$, there exists an automorphism a_m of G such that the maps induced by a_m respectively on

$X \times Y$ and Z are scalar multiplications by m and m^2. The set $A = \{a_m : m \in \mathbb{F}_p^*\}$ is a subgroup of $\mathrm{Aut}(G)$ that is isomorphic to $\mathbb{F}_p^*$. Thanks to Lemma 4.10, the subgroup A is contained in $\mathrm{Int}(G)$ and therefore $\mathrm{int}(G) = p - 1$. □

We remark that Lemma 4.11 is the same as (2) ⇒ (3) in Theorem 4.1. Since the implication (3) ⇒ (1) is clear and (1) ⇒ (2) is given by Corollary 4.2, Theorem 4.1 is finally proven.

PROPOSITION 4.12. *Let p be a prime number and let G be a finite p-group. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Assume that both the class and the intensity of G are greater than* 1. *Then, for all $i \in \mathbb{Z}_{\geq 1}$, the exponent of G_i/G_{i+2} divides p.*

PROOF. Let α be intense of order $\mathrm{int}(G)$ and write $\chi = \chi_{G|\langle\alpha\rangle}$. Let moreover i be a positive integer. The case in which $i = 1$ is given by the combination of Lemma 3.13 and Theorem 4.1. We now assume that $i > 1$: then G_i/G_{i+2} is abelian. By Lemma 3.15, the action of $\langle\alpha\rangle$ on G_i/G_{i+1} and G_{i+1}/G_{i+2} is respectively through χ^i and χ^{i+1}, which are distinct because $\mathrm{int}(G) \neq 1$. It follows from Theorem 2.9 that the groups G_i/G_{i+2} and $G_i/G_{i+1} \oplus G_{i+1}/G_{i+2}$ are isomorphic. The exponent of G_i/G_{i+2} divides p as a consequence of Lemma 4.4. □

CHAPTER 5

Intensity of Groups of Class 3

The purpose of this chapter is giving a complete overview of the case in which the class is 3. We will prove the following theorems.

THEOREM 5.1. *Let p be a prime number and let G be a finite p-group of class 3. Then the following are equivalent.*

1. *One has* $\mathrm{int}(G) > 1$.
2. *The prime p is odd and* $\mathrm{int}(G) = 2$.
3. *The prime p is odd and* $|G : G_2| = p^2$.

We remind the reader that, if G is a finite p-group and j is a positive integer, then the j-th width of G is $\mathrm{wt}_G(j) = \log_p |G_j : G_{j+1}|$. For more detail, see Section 2.3.

THEOREM 5.2. *Let p be a prime number and let G be a finite p-group of class at least* 3. *Assume that* $\mathrm{int}(G) > 1$. *For each positive integer j, set moreover $w_j = \mathrm{wt}_G(j)$. Then the following hold.*

1. *One has* $\mathrm{int}(G) = 2$.
2. *One has $(w_1, w_2, w_3) = (2, 1, f)$, where $f \in \{1, 2\}$.*

5.1. Low intensity

In Section 5.1 we derive some restrictions on the structure of finite p-groups of class at least 3 and intensity greater than 1. We will prove the following main result.

PROPOSITION 5.3. *Let p be a prime number and let G be a finite p-group of class at least* 3. *Assume that* $\mathrm{int}(G) > 1$. *Then the following hold.*

1. *The prime p is odd.*
2. *One has* $\mathrm{int}(G) = 2$.
3. *One has* $|G : G_2| = p^2$.

Our main goal for this section being the proof of Proposition 5.3, we will work under the following assumptions until the end of Section 5.1. Let p be a prime number and let G be a finite p-group of class at least 3. Assume that $\mathrm{int}(G) > 1$ and let α be intense of order $\mathrm{int}(G)$. Write $A = \langle \alpha \rangle$ and $\chi = \chi_{G|A}$, where χ_G denotes the intense character of G (see Section 3.2). For the rest of the notation we refer to the List of Symbols. We remark that, $\mathrm{int}(G)$ being greater than 1, the prime p is odd and G is non-trivial. For more detail see Chapter 3.

LEMMA 5.4. *Assume that G has class* 3. *Then the following hold.*

1. *One has* $G^p \subseteq G_3$.
2. *One has* $|G_2 : G_3| = p$.
3. *One has* $\mathrm{Z}(G) = G_3$.

Proof. By Lemma 3.13 the intensity of G/G_3 is greater than 1, and thus, by Theorem 4.1, the group G/G_3 is extraspecial of exponent p. It follows that G_2/G_3 has size p and that G^p is contained in G_3. Moreover, one has $\mathrm{Z}(G/G_3) = G_2/G_3$ and, since $\mathrm{Z}(G)/G_3$ is contained in $\mathrm{Z}(G/G_3)$, we get $G_3 \subseteq \mathrm{Z}(G) \subseteq G_2$. As the class of G is 3, we derive $\mathrm{Z}(G) = G_3$. □

Lemma 5.5. *Assume that G has class 3. Then the following hold.*

1. *The group G_2 is elementary abelian.*
2. *The group $\mathrm{C}_G(G_2)$ is abelian and A-stable.*

Proof. The group G_2 is abelian, since G_4 is trivial, and it has exponent p thanks to Proposition 4.12. Set now $C = \mathrm{C}_G(G_2)$. Then the commutator map induces a bilinear map $\phi : C/G_2 \times C/G_2 \to [C, C]$. The subgroups C and $[C, C]$ are characteristic in G and thus A-stable. Thanks to Lemma 3.15, the group A acts on C/G_2 through χ and, by Lemma 2.4, it acts on $[C, C]$ through χ^2. Again by Lemma 3.15, the action of A on G_3 is through χ^3. The character χ not being trivial, one has $\chi^2 \neq \chi^3$ and so Lemma 2.8 yields $[C, C] \cap G_3 = \{1\}$. By Lemma 5.4(3), the group G_3 is equal to $\mathrm{Z}(G)$ so the group $[C, C]$ is a normal subgroup of G that trivially intersects $\mathrm{Z}(G)$. It follows that $[C, C] = \{1\}$. □

Lemma 5.6. *Assume that G_3 has order p. Then the following hold.*

1. *One has $|G : \mathrm{C}_G(G_2)| = p$.*
2. *One has $|G : G_2| = p^2$.*
3. *One has $|\mathrm{C}_G(G_2)| = p^3$.*

Proof. Let $C = \mathrm{C}_G(G_2)$, $V = G/G_2$, $Z = G_2/G_3$, and $T = C/G_2$. The groups V, Z, and T are vector spaces over $\mathbb{F}_p$, as a consequence of Lemma 4.4. Let moreover $\psi : V \times Z \to G_3$ be the bilinear map that is induced by the commutator map and note that the left kernel of ψ is T. The centre of G is equal to G_3, by Lemma 5.4(3), and so the function $\psi_C : V/T \times Z \to G_3$ that is induced by ψ is non-degenerate. The dimension of G_3 being 1, Lemma 5.4(2) yields $\dim V/T = \dim Z = 1$. This proves (1). We prove (2) and (3) together. Let $\phi : V \times V \to Z$ be the bilinear map that is induced by the commutator map. By Lemma 5.5(2), the group C is abelian and therefore T is isotropic with respect to ϕ. As a consequence of (1), the space T has codimension 1 in V and T is thus maximal isotropic. It follows that the map ϕ_T from Lemma 4.7 is a bijection and hence $1 = \dim(V/T) = \dim \mathrm{Hom}(T, Z) = \dim T$. As a result, one gets $\dim V = 2$ and therefore $|G : G_2| = p^2$ and $|C| = p^3$. □

Lemma 5.7. *Assume that $\chi^2 \neq 1$ and that G has class 3. Then $\mathrm{C}_G(G_2)$ is elementary abelian.*

Proof. Let $C = \mathrm{C}_G(G_2)$. The group C is abelian and A-stable by Lemma 5.5(2). We will show that C has exponent p. By Lemma 5.5(1) the group G_2 is elementary abelian and $G_2 \subseteq C$. The group A acts on C/G_2 through χ, as a consequence of Lemma 3.15, and, by Lemma 2.6, it acts on C^p also through χ. It follows from Lemma 5.4(1) that $C^p \subseteq G_3$. The action of A on G_3 is through χ^3, by Lemma 5.5(2), and thus A acts on C^p both through χ and χ^3. Since $\chi^2 \neq 1$, the characters χ and χ^3 are distinct and, as a consequence of Lemma 2.8, the group C has exponent p. □

Lemma 5.8. *Assume that $\chi^2 \neq 1$ and that G_3 has order p. Then $\mathrm{C}_G(G_2)$ is a vector space over $\mathbb{F}_p$ with unique 1-dimensional A-stable subspaces C_1 and C_2 such that $\mathrm{C}_G(G_2) = C_1 \oplus C_2 \oplus G_3$.*

Proof. Set $C = \mathrm{C}_G(G_2)$. Then C is a vector space over $\mathbb{F}_p$ of dimension 3, as a consequence of Lemmas 5.6(3) and 5.7, and it is A-stable, by Lemma 5.5(2). By Lemma 3.15, the action of A on C/G_2, G_2/G_3, and G_3 is respectively through χ, χ^2, and χ^3, which are pairwise distinct. We first apply Theorem 2.9 to C/G_3, getting a unique A-stable complement D_1/G_3 of G_2/G_3. It follows that $D_1 \cap G_2 = G_3$. We now apply Theorem 2.9 to both D_1 and G_2 to get unique A-stable subspaces C_1 and C_2 of C satisfying $D_1 = C_1 \oplus G_3$ and $G_2 = C_2 \oplus G_3$. As a consequence of Lemma 5.4(2), the subspace G_2 has dimension 2, so both C_1 and C_2 have dimension 1. Moreover, the intersection of D_1 with G_2 being equal to G_3, it follows that $C = C_1 \oplus C_2 \oplus G_3$. □

Lemma 5.9. *Assume that G_3 has order p. Then $\mathrm{int}(G) = 2$.*

Proof. If $\chi^2 = 1$, then $1 < \mathrm{int}(G) \leq 2$ and we are done. We assume now that $\chi^2 \neq 1$ and we will derive a contradiction. Let C_1 and C_2 be as in Lemma 5.8 and denote by X be the collection of subspaces of dimension 1 of C. Since C is normal, the group G acts on X by conjugation. By Lemma 5.6(1), the index of C in G is equal to p and the size of each orbit of X under G is thus at most p. Moreover, the elements of X that are stable under the action of A are precisely C_1, C_2, and G_3. Lemma 3.6 yields

$$p^2 + p + 1 = |X| \leq |G : \mathrm{N}_G(C_1)| + |G : \mathrm{N}_G(C_2)| + |G : \mathrm{N}_G(G_3)| \leq 3p,$$

which is satisfied if and only if $(p-1)^2 \leq 0$. Contradiction. □

We can finally give the proof of Proposition 5.3. Since G has class at least 3, the group G_3 is non-trivial, so there exists a normal subgroup M of G that is contained in G_3 with index p. By Lemma 3.13, the group G/M has intensity greater than 1 and, as a consequence of Lemma 5.9, the intensity of G/M is equal to 2. From Lemma 3.13 it follows that $1 < \mathrm{int}(G) \leq \mathrm{int}(G/M) = 2$ and, from Lemma 5.6(2), that $|G : G_2| = p^2$. This concludes the proof of Proposition 5.3. We remark that Proposition 5.3 gives (1) ⇔ (2) and (1) ⇒ (3) in Theorem 5.1: we conclude the proof in Section 5.3. On the other hand, Theorem 5.2 follows directly from Proposition 5.3 and some basic commutator calculus.

Proposition 5.10. *The automorphism α has order 2 and, for all $i \geq 1$, it induces scalar multiplication by $(-1)^i$ on G_i/G_{i+1}.*

Proof. Let χ denote the restriction of χ_G to $\langle\alpha\rangle$. By Proposition 5.3, the intensity of G is 2 and p is odd. In particular, $\chi(\alpha)$ has order 2 in $\omega(\mathbb{F}_p^*)$, so $\chi(\alpha) = -1$. We conclude thanks to Lemma 3.15. □

5.2. Intensity given the automorphism

We recall that, for any group G, the lower central series of G is denoted $(G_i)_{i\geq 1}$ and it consists of characteristic subgroups of G. The main result of this section is the following.

Proposition 5.11. *Let p be an odd prime number and let G be a finite p-group of class 3 such that $|G : G_2| = p^2$. Let moreover α be an automorphism of G of* *order* 2 *that induces the inversion map* $x \mapsto x^{-1}$ *on* G/G_2. *Then* α *is intense and* $\mathrm{int}(G) = 2$.

The following assumptions will be valid until the end of Section 5.2. Let p be an odd prime number and let G be a finite p-group of class 3 such that $|G : G_2| = p^2$. As a consequence, the following are satisfied:

i. one has $\Phi(G) = G_2$;
ii. one has $|G_2 : G_3| = p$ and $|G_3| \in \{p, p^2\}$;
iii. the subgroup $\mathrm{C}_G(G_2)$ is abelian and $|G : \mathrm{C}_G(G_2)| = |G_3|$.

We will make some additional assumptions right before stating Lemma 5.14.

Lemma 5.12. *The group* G/G_3 *is extraspecial of exponent* p *and* $G_3 = \mathrm{Z}(G)$.

Proof. We write $\overline{G} = G/G_3$ and we use the bar notation for the subgroups of $\overline{G}$. The group $\overline{G}$ has class 2 and $\overline{G_2}$ is contained in $\mathrm{Z}(\overline{G})$. Moreover, the order of $\overline{G_2}$ is equal to p and, since $\overline{G}$ is not abelian, the groups $\overline{G_2}$ and $\mathrm{Z}(\overline{G})$ coincide. In particular, $\overline{G}$ is extraspecial. We now show that $\overline{G}$ has exponent p. Define $C = \mathrm{C}_G(G_2)$ and $D = \{x \in G \ : \ x^p \in G_3\}$. Then $C \neq G$ and D is a group, as a consequence of the Hall-Petrescu formula. Let now $x \in G \setminus C$: then x^p belongs to G_2. The commutator map induces an isomorphism $G/C \otimes G_2/G_3 \to G_3$, so, since x is not in the centralizer of G_2, the element x^p belongs to G_3. It follows that $x \in D$ and, in particular, we have proven that $G = C \cup D$. The group C is different from G, thus the groups D and G are the same. In particular, $\overline{G} = \overline{D}$ and so $\overline{G}$ has exponent p. To conclude, the groups G_3 and $\mathrm{Z}(G)$ are the same because $G_3 \subseteq \mathrm{Z}(G)G_2$ and $|G_2 : G_3| = p$. □

Lemma 5.13. *The subgroup* G_2 *is elementary abelian.*

Proof. The group G_2 is abelian, because G_4 is trivial; we prove that it has exponent p. Let M be a maximal subgroup of G_3. Then M has index p in G_3 and it is normal in G. We write $\overline{G} = G/M$ and use the bar notation for the subgroups of $\overline{G}$. The subgroup $\overline{G_3}$ has order p and $|\overline{G} : \overline{G_2}| = |G : G_2| = p^2$. It follows that $\mathrm{C}_{\overline{G}}(\overline{G_2})$ is abelian and that it contains $\overline{G_2}$ with index p. Write $\overline{C} = \mathrm{C}_{\overline{G}}(\overline{G_2})$. As a consequence of Lemma 5.12, the subgroup $\overline{C}^p$ is contained in $\overline{G_3}$, so $\mu_p(\overline{C})$ is a normal subgroup of $\overline{G}$ of order at least p^2. Moreover, $\overline{G_3}$ is contained in $\mu_p(\overline{C})$, so $\mu_p(\overline{C})/\overline{G_3}$ is a non-trivial normal subgroup of G/G_3. The quotient G/G_3 is extraspecial, by Lemma 5.12, so G_2/G_3 is equal to $\mathrm{Z}(G/G_3)$. The quotient G_2/G_3 having order p, we get that $\overline{G_2} \subseteq \mu_p(\overline{C})$. In particular, one has $G_2^p \subseteq M$. If $M = \{1\}$ we are done, otherwise let N be another maximal subgroup of G_3. In this case, G_3 is elementary abelian of order p^2 and G_2^p is contained in $N \cap M = \{1\}$. In each case, the exponent of G_2 is thus p. □

Let α be an automorphism of G of order 2 and write $A = \langle \alpha \rangle$. Let moreover $\chi : A \to \{\pm 1\}$ be an isomorphism of groups and assume that the induced action of A on G/G_2 is through χ. These assumptions will hold until the end of Section 5.2. We will prove that α is intense.

Lemma 5.14. *Every subgroup of* G *that contains* G_3 *has an* A*-stable conjugate in* G.

Proof. Let H be a subgroup of G that contains G_3. By Lemma 5.12, the group G/G_3 is extraspecial of exponent p and by assumption A acts on G/G_2 through

χ. As a consequence of Lemmas 4.10 and Lemma 3.5, there exists $g \in G$ such that $\alpha(gHg^{-1})/G_3 = (gHg^{-1})/G_3$ and so, G_3 being A-stable, $\alpha(gHg^{-1}) = gHg^{-1}$. □

We remind the reader that, if H is a subgroup of G, then a positive integer j is a jump of H in G if $H \cap G_j \neq H \cap G_{j+1}$. The j-th width of H in G is $\mathrm{wt}_H^G(j) = \log_p |H \cap G_j : H \cap G_{j+1}|$. For more information about jumps and width see Section 2.3.

Lemma 5.15. *Let H be a subgroup of G that trivially intersects G_3. Then the following hold.*

1. *If 1 is a jump of H in G, then $\mathrm{wt}_H^G(1) = 1$.*
2. *If 2 is a jump of H in G, then $H \subseteq \mathrm{C}_G(G_2)$.*

Proof. Assume first that 1 is a jump of H in G. Since H does not contain G_3, one has $H \neq G$. It follows that $H\Phi(G) \neq G$ and thus $H\Phi(G)/\Phi(G) = HG_2/G_2$ has order p. In particular, the 1-st width of H in G is 1. Assume now that 2 is a jump of H in G. Then by Lemma 2.16(2) there exists an element $x \in (H \cap G_2) \setminus G_3$. Fix x. Then $G_2 = \langle x \rangle G_3$ and so, G_3 being central, it follows that $[H, G_2] = [H, \langle x \rangle]$. The subgroup $[H, \langle x \rangle]$ is contained in $H \cap [G, G_2] = H \cap G_3$, which is trivial by assumption, and hence H centralizes G_2. □

Lemma 5.16. *Let H be a subgroup of G that trivially intersects G_2. Then H has an A-stable conjugate in G.*

Proof. The group H is abelian, because $[H, H] \subseteq H \cap [G, G] = \{1\}$. By Lemma 5.12, the groups G_3 and $\mathrm{Z}(G)$ are equal, so the group $T = H \oplus G_3$ is abelian. By Lemma 5.14, there exists $g \in G$ such that gTg^{-1} is A-stable and, the group G_3 being characteristic, $gTg^{-1} = gHg^{-1} \oplus G_3$. We fix such element g and note that $gTg^{-1} \cap G_2 = G_3$. It follows from Lemma 2.6 that the induced action of A on gTg^{-1}/G_3 is through χ. Moreover, by Lemma 2.5, the group A acts on G_3 through $\chi^3 = \chi$. From Lemma 2.12, it follows that α sends each element of gTg^{-1} to its inverse, so each subgroup of gTg^{-1} is A-stable. In particular, gHg^{-1} is A-stable. □

Lemma 5.17. *Let H be a subgroup of G with $G_2 = H \oplus G_3$. Then H has an A-stable conjugate in G.*

Proof. By Lemma 2.5, the induced action of A on G_2/G_3 and G_3 is respectively through χ^2 and $\chi^3 = \chi$. Moreover, since G_4 is trivial, G_2 is abelian and so, by Theorem 2.9, there exists a unique A-stable complement K of G_3 in G_2. We want to show that H and K are conjugate in G. The groups G_3 and $\mathrm{Z}(G)$ coincide, by Lemma 5.12, thus $\mathrm{C}_G(H) = \mathrm{C}_G(G_2)$ and moreover, since $H \cap [H, G] \subseteq H \cap G_3 = \{1\}$, we have that $\mathrm{C}_G(H) = \mathrm{N}_G(H)$. Let now X be the collection of complements of G_3 in G_2. Since H has order p, Lemma 4.6 yields that the cardinality of X is equal to the cardinality of $\mathrm{Hom}(H, G_3)$, which coincides with $|G_3| = |G : \mathrm{C}_G(G_2)|$. It follows that $|X| = |G : \mathrm{N}_G(H)|$ and so, every conjugate of H being in X, every complement of G_3 in G_2 is G-conjugate to H. In particular, K and H are conjugate in G. □

Lemma 5.18. *Let H be a subgroup of G that is not contained in $\mathrm{C}_G(G_2)$ and that has trivial intersection with G_3. Then H has a conjugate that is A-stable.*

Proof. As a consequence of Lemma 5.15(2), the subgroup H has trivial intersection with G_2. We now apply Lemma 5.16. □

Lemma 5.19. *Let H be a subgroup of $\mathrm{C}_G(G_2)$ of order p that has trivial intersection with G_3. Then H has a conjugate that is A-stable.*

Proof. Set $T = H \oplus G_3$. If $T = G_2$, then H has an A-stable conjugate by Lemma 5.17. Assume now that $T \cap G_2 = G_3$. Then $H \cap G_2 = H \cap T \cap G_2 = H \cap G_3 = \{1\}$, so we are done by Lemma 5.16. □

We write $G^+ = \{x \in G : \alpha(x) = x\}$ and $G^- = \{x \in G : \alpha(x) = x^{-1}\}$, in concordance with the notation from Section 2.2. We adopt this notation in Lemmas 5.20 and 5.21.

Lemma 5.20. *Let H be a subgroup of $\mathrm{C}_G(G_2)$ such that $H \cap G_3 = \{1\}$. Then the following hold.*

1. *The subgroup H is elementary abelian.*
2. *One has $G^+\,\mathrm{N}_G(H) = \mathrm{N}_G(H)$.*

Proof. The subgroup $\mathrm{C}_G(G_2)$ is abelian and therefore so is H. Moreover, as a consequence of Lemma 5.12, the subgroup H^p is contained in $H \cap G_3 = \{1\}$, so H is elementary abelian. Now, G^+ is contained in G_2, thanks to Lemma 2.17, and G_2 centralizes C. It follows that $G^+\,\mathrm{N}_G(H) \subseteq G_2\,\mathrm{N}_G(H) = \mathrm{N}_G(H)$. □

Lemma 5.21. *Let H be a subgroup of G such that $\mathrm{C}_G(G_2) = H \oplus G_3$. Then H has a conjugate in G that is A-stable.*

Proof. Write $C = \mathrm{C}_G(G_2)$. If $C = G_2$, then we are done by Lemma 5.17. Assume now that $C \neq G_2$. Then C contains G_2 with index p and G_3 has order p. We define X to be the collection of subgroups K of G such that $C = K \oplus G_3$ and denote $X^+ = \{K \in X \mid \alpha(K) = K\}$. The centre of G is equal to G_3, by Lemma 5.12, and so all elements of X are non-normal subgroups of G. In particular, for any $K \in X$, one has $|G : \mathrm{N}_G(K)| \geq p$. Now, by Lemma 5.20(1), the subgroup H is elementary abelian, and, G_3 being central of order p, it follows that C is an $\mathbb{F}_p$-vector space of dimension 3. Write $C^+ = C \cap G^+$ and $C^- = C \cap G^-$. Then $C = C^+ \oplus C^-$, thanks to Corollary 2.2 and, as a consequence of Lemma 2.17, the linear subspaces C^+ and C^- of C have respectively dimension 1 and 2. One shows that

$$X^+ = \{C^+ \oplus \ell : \ell \subseteq G^-,\ \ell \cap G_3 = \{1\},\ \dim(\ell) = 1\}.$$

It follows that X^+ has cardinality p, while the cardinality of X is p^2. Moreover, the combination of Lemmas 2.15 and 5.20(2) ensures that no two elements of X^+ are conjugate in G. Lemma 3.6 yields

$$p^2 = |X| \geq \sum_{K \in X^+} |G : \mathrm{N}_G(K)| \geq \sum_{K \in X^+} p = |X^+|p = p^2,$$

and therefore every element of X is conjugate in G to an element of X^+. In particular, H has an A-stable conjugate. □

Lemma 5.22. *Every subgroup of G that trivially intersects G_3 has an A-stable conjugate in G.*

PROOF. Let H be a subgroup of G such that $H \cap G_3 = \{1\}$. If H is contained in $\mathrm{C}_G(G_2)$ and has order p, then we are done by Lemma 5.19. Assume now that H is contained in $\mathrm{C}_G(G_2)$ and that H has order p^2. The group $\mathrm{C}_G(G_2)$ being abelian, one has $\mathrm{C}_G(G_2) = H \oplus G_3$ and hence H has an A-stable conjugate by Lemma 5.21. We conclude by Lemma 5.18, in case H is not contained in $\mathrm{C}_G(G_2)$. □

LEMMA 5.23. *Let H be a subgroup of G such that $H \cap G_3 \neq \{1\}$. Then H has a conjugate that is A-stable.*

PROOF. Lemma 5.14 covers the case in which H contains G_3. Assume now that the group $H \cap G_3$ is different from both $\{1\}$ and G_3. Then G_3 has order p^2 and $H \cap G_3$ has order p. The subgroup $H \cap G_3$ is normal, thanks to Lemma 5.12, and so we write $\overline{G} = G/(H \cap G_3)$ and use the bar notation for the subgroups of $\overline{G}$. The group $\overline{G}$ has class 3 and $|\overline{G} : \overline{G_2}| = p^2$. Moreover, $\overline{H} \cap \overline{G_3} = \{1\}$. Thanks to Lemma 5.22, the subgroup $\overline{H}$ has an A-stable conjugate, and therefore so does H. □

LEMMA 5.24. *The automorphism α is intense and* $\mathrm{int}(G) = 2$.

PROOF. We will show that $\alpha \in \mathrm{Int}(G)$. Thanks to Lemma 3.5, it suffices to show that every subgroup of G has an A-stable conjugate. Let H be a subgroup of G. If $H \cap G_3 = \{1\}$, we are done by Lemma 5.22, otherwise apply Lemma 5.23. The automorphism α being intense, $\mathrm{int}(G) = 2$. □

Thanks to Lemma 5.24, Proposition 5.11 is proven.

5.3. Constructing intense automorphisms

The aim of Section 5.3 is giving the proof of Theorem 5.1. We will prove the following essential result.

PROPOSITION 5.25. *Let p be an odd prime number and let G be a finite p-group of class 3 such that $|G : G_2| = p^2$. Then there exists an automorphism α of G of order 2 that induces the inversion map $x \mapsto x^{-1}$ on G/G_2.*

In order to prove Proposition 5.25, let p be an odd prime number and let G be a finite p-group of class 3. Let moreover $(G_i)_{i\geq 1}$ denote the lower central series of G and assume that $|G : G_2| = p^2$. We will keep these assumptions and notation until the end of Section 5.3. We will work to construct an automorphism α of G and an isomorphism $\chi : \langle \alpha \rangle \to \{\pm 1\}$ in order to apply the results achieved in the previous section.

Let F be the free group on the set $S = \{a, b\}$ and let $\iota : S \to G$ be a map such that $G = \langle \iota(S) \rangle$. By the universal property of free groups, there exists a unique homomorphism $\theta : F \to G$ such that $\theta(a) = \iota(a)$ and $\theta(b) = \iota(b)$. In particular, the map θ is surjective. We denote by $(F_i)_{i\geq 1}$ the p-central series of F, which is recursively defined as

$$F_1 = F \quad \text{and} \quad F_{i+1} = [F, F_i]F_i^p.$$

We want to stress the fact that the notation we use here for the p-central series of F clashes with the notation we have adopted so far (see the section "Exceptions" from the List of Symbols). Define additionally

$$L = F_3 F^p \ \text{ and } \ E = [F, L]F_2^p.$$

The notation we just introduced will be valid until the end of Section 5.3. We will introduce some extra notation between Lemma 5.28 and Lemma 5.29. We refer to the diagram given at the end of the present section for a visualization of the proof of Proposition 5.25.

Lemma 5.26. *One has $\theta^{-1}(G_2) = F_2$.*

Proof. This follows directly from the fact that $\Phi(G) = G_2$. □

Lemma 5.27. *The commutator map induces an alternating map $F/F_2 \times F/F_2 \to F_2/L$ whose image generates F_2/L. Furthermore, one has $\theta^{-1}(G_3) = L$ and $|F_2 : L| = p$.*

Proof. We first claim that $|F_2 : L| \leq p$. To this end, we write $\overline{F} = F/L$ and we will use the bar notation for the subgroups of $\overline{F}$. The subgroup $\overline{F}$ being annihilated by p, the subgroup $\overline{F_2}$ coincides with $[\overline{F}, \overline{F}]$ and so the commutator map induces an alternating bilinear map $\phi : \overline{F}/\overline{F_2} \times \overline{F}/\overline{F_2} \to \overline{F_2}$ whose image generates $\overline{F_2} = [\overline{F}, \overline{F}]$. By the universal property of the exterior square, ϕ factors as a surjective homomorphism $\bigwedge^2(\overline{F}/\overline{F_2}) \to \overline{F_2}$ and therefore, $\bigwedge^2(\overline{F}/\overline{F_2})$ having dimension 1, it follows that $\overline{F_2}$ has order at most p. This proves the claim. Note now that, a consequence of Lemma 5.12, the group G_3 contains G^p and hence $\theta(L) = G_3$. As a consequence of Lemma 5.26, the subgroup $\theta^{-1}(G_3)$ is contained in F_2 and, since G_2 and G_3 are distinct, $\theta^{-1}(G_3) \neq F_2$. It follows that F_2 is different from L and so, as a consequence, $|F_2 : L| = p$ and $\theta^{-1}(G_3) = L$. □

Lemma 5.28. *One has $E \subseteq \ker\theta \cap F_3$.*

Proof. The group E is clearly contained in F_3. Moreover, as a consequence of Lemmas 5.27 and 5.13, one has $\theta(E) = \theta([F, L]F_2^p) = [G, G_3]G_2^p = \{1\}$ and so $E \subseteq \ker\theta$. □

Let β be the endomorphism of F sending a to a^{-1} and b to b^{-1}, and note that β exists by the universal property of free pro-p-groups. Then β^2 is equal to id_F, and thus β is an automorphism of F. Write $B = \langle\beta\rangle$ and define the homomorphism $\sigma : B \to \{\pm 1\}$ by $\beta \mapsto -1$. We will respect this notation until the end of Section 5.3.

Lemma 5.29. *The induced action of B on F/F_2 and F_2/L is respectively through σ and σ^2.*

Proof. By definition of β, the action of B on F/F_2 is through σ and, by Lemma 5.27, the commutator map induces a bilinear map $\phi : F/F_2 \times F/F_2 \to F_2/L$ whose image generates F_2/L. The group B acts on F/F_2 through σ and so, by Lemma 2.4, the action of B on F_2/L is through σ^2. □

Lemma 5.30. *The induced action of B on L/F_3 is through σ.*

Proof. We write $\overline{F} = F/F_3$ and we use the bar notation for its subgroups. Then $\overline{L}$ is equal to $\overline{F}^p$ and $\overline{F}$ has class at most 2. Moreover, $[\overline{F}, \overline{F}]$ is annihilated by p. By the Hall-Petrescu formula, the p-power map is an endomorphism of $\overline{F}$, and therefore $\overline{L}$ is an epimorphic image of $\overline{F}/\overline{F_2}$. By Lemma 2.6, the induced action of B on $\overline{L}$ is through σ. □

Lemma 5.31. *The induced action of B on F_3/E is through σ.*

Proof. The group F_2/L is cyclic, thanks to Lemma 5.27, so $[F_2, F_2] = [F_2, L]$ is contained in E. Moreover, since $[F, F_3]$ is also contained in E, the commutator map induces a bilinear map $\phi : F/F_2 \times F_2/L \to F_3/E$. By Lemma 5.29, the induced actions of B on F/F_2 and F_2/L are respectively through σ and σ^2 and thus, by Lemma 2.4, the action of B on F_3/E is through $\sigma^3 = \sigma$. □

Lemma 5.32. *The induced action of B on L/E is through σ. Moreover, the kernel of θ is B-stable.*

Proof. As a consequence of Lemmas 5.30 and 5.31, the induced actions of B on L/F_3 and F_3/E are both through σ. It follows from Lemma 2.12 that the action of B on L/E is through σ. As a consequence of Lemmas 5.27 and 5.28, one has $E \subseteq \ker\theta \subseteq L$, and, in particular, the action of B on L/E restricts to an action of B on $\ker\theta/E$. It follows that $\ker\theta$ is B-stable and the proof is complete. □

$$\begin{tikzcd}
& F \arrow[rr, dashed] \arrow[d, dash, "p^2"', "-"] & & G \arrow[d, dash, "-"'] \\
& F_2 \arrow[rr, dashed] \arrow[d, dash, "p"', "+"] & & G_2 \arrow[d, dash, "+"'] \\
& L = F_3F^p \arrow[rr, dashed] \arrow[dl, dash, "-"', "p^2"] \arrow[dr, dash, "-", "p^2"'] & & G_3 \arrow[d, dash, "-"'] \\
F_3 \arrow[dr, dash, "p^2", "-"'] & & \ker\theta \arrow[r, dashed] \arrow[dl, dash, "p^2"', "-"] & 1 \\
& E = [F, L]F_2^p & &
\end{tikzcd}$$

Lemma 5.33. *Given any two generators x and y of G, there exists an intense automorphism of G such that $\alpha(x) = x^{-1}$ and $\alpha(y) = y^{-1}$.*

Proof. Let x and y be generators of G. Without loss of generality, we assume that $\iota(a) = x$ and $\iota(b) = y$. Let moreover $\bar{\theta} : F/\ker\theta \to G$ be the isomorphism that is induced from θ. By Lemma 5.32, the subgroup $\ker\theta$ of F is B-stable, and therefore β induces an automorphism $\bar{\beta}$ of $F/\ker\theta$. Define $\alpha : G \to G$ by $\alpha = \bar{\theta}\circ\bar{\beta}\circ\bar{\theta}^{-1}$. Then α is an automorphism G of order 2 that inverts the generators x and y. Proposition 5.11 yields that α is intense. □

We remark that Proposition 5.25 follows directly from Lemma 5.33. Moreover, we are also finally ready to give the proof of Theorem 5.1. Proposition 5.3 gives (1) $\Leftrightarrow$ (2) and (1) $\Rightarrow$ (3). On the other hand, the implication (3) $\Rightarrow$ (2) is given by the combination of Lemma 5.33 and Proposition 5.11. The proof of Theorem 5.1 is complete.

CHAPTER 6

Some Structural Restrictions

In this chapter we will see how the structure of finite p-groups whose intensity is greater than 1 starts becoming more and more rigid, as soon as the class is at least 4. We recall that, if $(G_i)_{i\geq 1}$ denotes the lower central series of G, then, for each positive integer i, the i-th width of G is $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$ (see Section 2.3). The main results from Chapter 6 are the following.

Theorem 6.1. *Let p be a prime number and let G be a finite p-group of class at least* 4. *For all $i \in \{1,2,3,4\}$, write $w_i = \mathrm{wt}_G(i)$. If* $\mathrm{int}(G) > 1$, *then* $(w_1, w_2, w_3, w_4) = (2,1,2,1)$.

Theorem 6.2. *Let p be a prime number and let G be a finite p-group of class at least* 3. *For all $i \in \mathbb{Z}_{\geq 1}$, write $w_i = \mathrm{wt}_G(i)$. Assume that* $\mathrm{int}(G) > 1$. *Then, for all $i \in \mathbb{Z}_{\geq 1}$, one has $w_i w_{i+1} \leq 2$.*

6.1. Normal subgroups

We devote Section 6.1 to understanding the normal subgroup structure of a finite p-group of intensity greater than 1. We prove the following result.

Proposition 6.3. *Let p be a prime number and let G be a finite p-group with* $\mathrm{int}(G) > 1$. *Let N be a subgroup of G. Then N is normal if and only if there exists $i \in \mathbb{Z}_{\geq 1}$ such that $G_{i+1} \subseteq N \subseteq G_i$.*

The following assumptions will be satisfied until the end of Section 6.1. Let p be a prime number and let G be a finite p-group of intensity greater than 1. It follows that p is odd and that G is non-trivial (see Section 3.2). Denote by $(G_i)_{i\geq 1}$ the lower central series of G and, for each positive integer i, write $w_i = \mathrm{wt}_G(i)$ for the i-th width of G. Let α be intense of order 2 and write $A = \langle \alpha \rangle$. Denote $\chi = \chi_{G|A}$, the restriction of the intense character of G to A (once again, we refer to Section 3.2). In concordance with the notation from Section 2.2, let $G^+ = \{x \in G \mid \alpha(x) = x\}$ and $G^- = \{x \in G \mid \alpha(x) = x^{-1}\}$. For a subgroup H of G we will write $H^+ = H \cap G^+$ and $H^- = H \cap G^-$. Thanks to Corollary 2.2 from Section 2.2 once can show, for each subgroup H of G, that if H is A-stable and cyclic, then $H \subseteq G^+$ or $H \subseteq G^-$. To conclude, we recall that, as defined in Section 2.3, if x is a non-trivial element of G, then the depth $\mathrm{dpt}_G(x)$ of x is the unique positive integer d for which $x \in G_d \setminus G_{d+1}$.

Lemma 6.4. *Let $x \in G \setminus \{1\}$. Then the following hold.*

1. *The depth of x is even if and only if there exists $g \in G$ such that gxg^{-1} belongs to G^+.*
2. *The depth of x is odd if and only if there exists $g \in G$ such that gxg^{-1} belongs to G^-.*

Proof. The automorphism α being intense, it follows from Lemma 3.5 that there exists $g \in G$ such that $\langle gxg^{-1}\rangle$ is A-stable. Write $d = \mathrm{dpt}_G(x) = \mathrm{dpt}_G(gxg^{-1})$ and $H = \langle gxg^{-1}\rangle$. Then the A-stable subgroup H is contained in G^+ or in G^-. By Lemma 3.15, the action of A on $(HG_{d+1})/G_{d+1}$ is through χ^d and the choice between G^+ and G^- only depends from the parity of d. □

We recall that, if H is a subgroup of G, then a jump of H in G is a positive integer j such that $H \cap G_j \neq H \cap G_{j+1}$. A direct conseuqence of Lemma 6.4 is the following result.

Lemma 6.5. *All jumps of a cyclic subgroup of G have the same parity.*

Lemma 6.6. *Let $c \in \mathbb{Z}_{\geq 1}$ denote the class of G. Then the following hold.*

1. *The induced action of A on $\mathrm{Z}(G)$ is through χ^c.*
2. *If c is even, then $\mathrm{Z}(G) \subseteq G^+$.*
3. *If c is odd, then $\mathrm{Z}(G) \subseteq G^-$.*

Proof. The subgroup G_c is contained in $\mathrm{Z}(G)$ and, by Lemma 3.15, the group A acts on G_c through χ^c. From the combination of Corollary 3.3 with Lemma 2.8, it follows that A acts on $\mathrm{Z}(G)$ through χ^c. If c is even, then $\chi^c = 1$ and $\mathrm{Z}(G)$ is contained in G^+. Otherwise, $\chi^c = \chi$ and $\mathrm{Z}(G) \subseteq G^-$. □

Lemma 6.7. *Let $c \in \mathbb{Z}_{\geq 1}$ be the class of G. Then, for all $i \in \{1, \ldots, c\}$, if H is a quotient of G of class i, then $\mathrm{Z}(H) = H_i$.*

Proof. If $i = 1$ the result is clear; we assume that i is at least 2 and that the result holds for $i - 1$. Let H be a quotient of G of class i, which has, thanks to Lemma 3.13, intensity greater than 1. Let β be intense of order 2 and let $B = \langle\beta\rangle$ and $\psi = \chi_{H|B}$. The subgroup H_i is central in H, so $\mathrm{Z}(H)/H_i$ is isomorphic to a subgroup of $\mathrm{Z}(H/H_i)$. By the induction hypothesis $\mathrm{Z}(H/H_i) = H_{i-1}/H_i$ and it follows that $H_i \subseteq \mathrm{Z}(H) \subseteq H_{i-1}$. By Lemma 3.15, the group B acts on H_{i-1}/H_i and H_i, respectively through ψ^{i-1} and ψ^i, which are distinct characters since $\psi \neq 1$. Moreover, the induced action of B on $\mathrm{Z}(H)$ is through ψ^i, by Lemma 6.6(1). Lemma 2.8 yields $\mathrm{Z}(H) = H_i$. □

We remark that Proposition 6.3 follows now directly from Lemma 6.7 and the following elementary lemma.

Lemma 6.8. *Let q be a prime number and let Q be a finite q-group of class c. Let moreover N be a subgroup of Q. Assume that, for all $i \in \{1, \ldots, c\}$, if H is a quotient of Q of class i, then $\mathrm{Z}(H) = H_i$. Then N is normal if and only if there exists $i \in \mathbb{Z}_{>0}$ such that $Q_{i+1} \subseteq N \subseteq Q_i$.*

6.2. About the third width

Let p be a prime number and let G be a finite p-group. If i is a positive integer, we recall that the i-th width of G is defined to be $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$, where $(G_i)_{i\geq 1}$ denotes the lower central series of G. Thanks to Theorem 5.2(2), we know that, if G has class at least 3 and $\mathrm{int}(G) > 1$, then $(\mathrm{wt}_G(1), \mathrm{wt}_G(2)) = (2, 1)$ and $\mathrm{wt}_G(3)$ is either 1 or 2. In the case in which the class of G equals 3, then both situations $\mathrm{wt}_G(3) = 1$ and $\mathrm{wt}_G(3) = 2$ occur. What about higher nilpotency classes? We prove the following.

Proposition 6.9. *Let p be a prime number and let G be a finite p-group of class at least 4. For each positive integer i, denote $w_i = \mathrm{wt}_G(i)$. Assume that $\mathrm{int}(G) > 1$. Then $(w_1, w_2, w_3) = (2, 1, 2)$.*

Until the end of Section 6.2, the following assumptions will hold. Let p be a prime number and let G be a finite p-group. Let $(G_i)_{i \geq 1}$ denote the lower central series of G and, for each positive integer i, denote $w_i = \mathrm{wt}_G(i)$. We assume that G has class 4 and that $(w_1, w_2, w_3, w_4) = (2, 1, 1, 1)$. We will show that $\mathrm{int}(G) = 1$.

Lemma 6.10. *Assume that p is odd. Then $\mathrm{Z}(G) = G_4$.*

Proof. The group $\mathrm{Z}(G)/G_4$ is contained in $\mathrm{Z}(G/G_4)$ and, thanks to Lemma 5.12, the centre of G/G_4 is equal to G_3/G_4. It follows that $G_4 \subseteq \mathrm{Z}(G)G_3$ and so $G_4 = \mathrm{Z}(G)$. □

Lemma 6.11. *The subgroup G_2 is abelian.*

Proof. The group G_2/G_3 is cyclic so $[G_2, G_2] = [G_2, G_3]$. It follows that $[G_2, G_2] \subseteq G_5 = \{1\}$, and thus G_2 is abelian. □

In the case in which p is odd, Lemmas6.10 and 6.11, together with some basic commutator calculus, yield the following:

i. the subgroup $[\mathrm{C}_G(G_3), G_2]$ is contained in G_4; and
ii. one has $|\,\mathrm{C}_G(G_3) : G_2| = p$.

This last observation will turn out useful in the proofs of the following lemmas.

Lemma 6.12. *If $\mathrm{int}(G) > 1$, then $\mathrm{C}_G(G_3)$ is abelian.*

Proof. Assume that $\mathrm{int}(G) > 1$, so that p is odd. Let α be an intense automorphism of G of order 2 and write $A = \langle \alpha \rangle$ and $\chi = \chi_{G|A}$. Write moreover $C = \mathrm{C}_G(G_3)$. The index $|C : G_2|$ being p, one has $[C, C] = [C, G_2]$; moreover, $[C, G_2]$ is contained in G_4 and $G_4 = \mathrm{Z}(G)$, by Lemma 6.10. It follows that the commutator map $C \times G_2 \to G_4$ is bilinear and, as a consequence of Lemma 6.11, it factors as $\phi : C/G_2 \times G_2/G_3 \to G_4$. By Lemma 3.15, the group A acts on C/G_2 and G_2/G_3 respectively through χ and χ^2, so, as a consequence of Lemma 2.4, the group A acts on $[C, G_2]$ through $\chi^3 = \chi$. By Lemma 3.15, the group A acts on G_4 through $\chi^4 = 1$. Since $\chi \neq 1$, it follows from Lemma 2.8 that $[C, C]$ is trivial, and therefore C is abelian. □

We recall here that, if $A = \langle \alpha \rangle$ is a multiplicative group of order 2 acting on a finite group B of odd order, then one defines $B^+ = \{x \in B : \alpha(x) = x\}$ and $B^- = \{x \in B : \alpha(x) = x^{-1}\}$. (See Section 2.2.)

Lemma 6.13. *Assume that $\mathrm{int}(G) > 1$ and let α be an intense automorphism of G of order 2. Write $C = \mathrm{C}_G(G_3)$. Then $C = C^+ \oplus C^-$ and $|C^+| = |C^-| = p^2$.*

Proof. The group C is A-stable and it is abelian by Lemma 6.12. Corollary 2.2 yields $C = C^+ \oplus C^-$, while the cardinalities of C^+ and C^- are both equal to p^2, thanks to Lemma 2.17. □

Lemma 6.14. *Assume that $\mathrm{int}(G) > 1$ and let α be an intense automorphism of G of order 2. Write $C = \mathrm{C}_G(G_3)$. Then C^+ is cyclic if and only if C^- is cyclic.*

Proof. The subgroup C^p is characteristic in G, so C^p is A-stable. Moreover, as a consequence of Lemma 6.6(2), the subgroup $\mathrm{Z}(G)$ is contained in G^+. Assume first that C^- is cyclic. Then C^p is a non-trivial subgroup of the p-group G and thus has non-trivial intersection with $\mathrm{Z}(G)$. In particular, $C^p \cap G^+ \neq \{1\}$ and so C^+ is cyclic. Assume now that C^+ is cyclic. As a consequence of Lemma 2.17, the group C^+ is contained in G_2. We claim that there exists an element $x \in C \setminus G_2$ of order p^2: if not, then C is equal to the union of two proper subgroups, namely $C \cap G_2$ with $\mu_p(C)$, which is impossible. Fix thus $x \in C$ of order p^2 with $\mathrm{dpt}_G(x) = 1$. By Lemma 6.4, there exists $g \in G$ such that gxg^{-1} belongs to G^-. Since both C^- and $\langle x \rangle$ have order p^2, the group C^- is cyclic. □

Lemma 6.15. *Let H be a subgroup of $\mathrm{C}_G(G_3)$. If $\mathrm{int}(G) > 1$, then H has at most p conjugates in G.*

Proof. Assume that $\mathrm{int}(G) > 1$. The group $\mathrm{C}_G(G_3)$ is abelian, by Lemma 6.12, and therefore $\mathrm{C}_G(G_3)$ normalizes H. It follows that $|G : \mathrm{N}_G(H)| \leq |G : \mathrm{C}_G(G_3)| = p$ and thus H has at most p conjugates. □

Lemma 6.16. *Assume that $\mathrm{int}(G) > 1$ and let α be an intense automorphism of G of order 2. Write $C = \mathrm{C}_G(G_3)$. Then C^+ is cyclic.*

Proof. Assume the contrary. Then, as a consequence of Lemma 6.14, both C^+ and C^- are elementary abelian. From Lemma 6.13 it follows that C is an $\mathbb{F}_p$-vector space of dimension 4. Let X be the collection of 1-dimensional subspaces of C; then we have $|X| = p^3 + p^2 + p + 1$. Let moreover $X^+ = \{H \in X \ : \ \alpha(H) = H\}$. Then X^+ consists of the 1-dimensional subspaces of C that are contained in $C^+ \cup C^-$ and so $|X^+| = 2(p+1)$. By Lemma 6.15, each element of X^+ has at most p conjugates in G, so it follows from Lemma 3.6 that

$$2p(p+1) = p|X^+| \geq \sum_{H \in X^+} |G : \mathrm{N}_G(H)| \geq |X| = p^3 + p^2 + p + 1.$$

Contradiction. □

Lemma 6.17. *The intensity of G is equal to 1.*

Proof. Assume by contradiction that $\mathrm{int}(G) > 1$ and let α be an intense automorphism of G of order 2. Write $C = \mathrm{C}_G(G_3)$. The group C is abelian, by Lemma 6.12, and $C = C^+ \oplus C^-$, by Lemma 6.13. Moreover, C^+ and C^- have both cardinality p^2. By Lemma 6.16, the subgroup C^+ is cyclic so, by Lemma 6.14, the subgroup C^- is also cyclic. Let X be the collection of cyclic subgroups of C of order p^2 and let X^+ be the subset of X consisting of the A-stable ones. Then $X^+ = \{C^+, C^-\}$ and the cardinality of X^+ is 2. On the other hand, the cardinality of X is equal to $p(p+1)$. By Lemma 6.15, each element of X^+ has at most p conjugates, so it follows from Lemma 3.6 that

$$2p \geq p|X^+| \geq |X| = p^2 + p.$$

Contradiction. □

We conclude Section 6.2 by giving the proof of Proposition 6.9. Let Q be a finite p-group of class at least 4 with $\mathrm{int}(Q) > 1$. Let moreover M be a normal subgroup of Q that is contained in Q_4 with index p and denote $\overline{Q} = Q/M$. Thanks to Lemma 3.13, the intensity of $\overline{Q}$ is greater than 1, so it follows from Theorem 5.2(2) that $(\mathrm{wt}_{\overline{Q}}(1), \mathrm{wt}_{\overline{Q}}(2), \mathrm{wt}_{\overline{Q}}(3), \mathrm{wt}_{\overline{Q}}(4)) = (2, 1, f, 1)$, where $f \in \{1, 2\}$. Lemma 6.17 yields $f = 2$ and the proof of Proposition 6.9 is complete.

6.3. A bound on the width

From Section 2.3, we recall that, given a finite p-group G and a positive integer i, the i-th width of G is defined to be $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$. The unique purpose of Section 6.3 is to prove the following result.

Proposition 6.18. *Let p be a prime number and let G be a finite p-group. Let c denote the class of G. Assume $c \geq 3$ and $\mathrm{int}(G) > 1$. Then, for each i in $\{1, 2, \ldots, c-1\}$, one has $\mathrm{wt}_G(i)\,\mathrm{wt}_G(i+1) \leq 2$.*

We devote the remaining part of this section to the proof of the last proposition. Until the end of Section 6.3 we will work thus under the assumptions of Proposition 6.18, which imply that p is odd. We define

$$\phi : G/G_2 \to \mathrm{Hom}(G_{c-1}/G_c, G_c)$$

to be the homomorphism of groups that is induced by the commutator map and remark that, using elementary commutator calculus, one can show that G_{c-1} is abelian. We first claim that ϕ is surjective. In order to prove so, we let α be an intense automorphism of G of order $\mathrm{int}(G)$ and write $A = \langle\alpha\rangle$. Now, the group G_{c-1} is abelian and, thanks to the combination of Lemma 3.15 with Theorem 2.9, there exists a unique A-stable complement M of G_c in G_{c-1}. The group A acts in a natural way on the set of complements of G_c in G_{c-1} and, the automorphism α being intense, it follows from Lemma 3.5 that all complements of G_c in G_{c-1} are conjugate to M in G. On the other hand, by Lemma 4.6, the set of complements of G_c in G_{c-1} consists of the elements $\{mf(m) : m \in M\}$ as f varies in $\mathrm{Hom}(M, G_c)$. It follows that, for each $f \in \mathrm{Hom}(M, G_c)$, there exists $x \in G$, such that $\{mf(m) : m \in M\} = xMx^{-1}$. Fix the pair (f, x). Then, for all $m \in M$, there exists $n \in M$ such that $mf(m) = xnx^{-1} = [x, n]n$. It follows that $n^{-1}m = [x, n]f(m)^{-1}$ belongs to $M \cap G_c = \{1\}$, so $m = n$. We have proven that $f(m) = [x, m]$. Now, the groups $\mathrm{Hom}(G_{c-1}/G_c, G_c)$ and $\mathrm{Hom}(M, G_c)$ are isomorphic and, the choice of f being arbitrary, each homomorphism $f : G_{c-1}/G_c \to G_c$ is of the form $mG_c \mapsto [x, m]$, for some $x \in G$. This proves the claim. Now, the groups G_{c-1}/G_c and G_c are vector spaces over $\mathbb{F}_p$, thanks to Lemma 4.4, and so the dimension of $\mathrm{Hom}(G_{c-1}/G_c, G_c)$ is equal to $\mathrm{wt}_G(c-1)\,\mathrm{wt}_G(c)$. It follows then from the last claim and Theorem 5.2(2) that

$$\mathrm{wt}_G(c-1)\,\mathrm{wt}_G(c) = \dim \mathrm{Hom}(G_{c-1}/G_c, G_c) \leq \mathrm{wt}_G(1) = 2.$$

Without loss of generality, we can assume that $c = i + 1$ and so the proof of Proposition 6.18 is complete.

We remark that Theorem 6.2 is the same as Proposition 6.18. Moreover, Theorem 6.1 is given by the combination of Propositions 6.9 and 6.18.

CHAPTER 7

Higher Nilpotency Classes

The aim of this chapter is to gain better control of the p-power map on finite p-groups of intensity greater than 1. We remind the reader that, if n is a positive integer and G is a group, then G^n is equal to the subgroup of G that is generated by the n-th powers of the elements of G, i.e. $G^n = \langle x^n : x \in G \rangle$. One of the most important results we achieve in Chapter 7 is the following.

Theorem 7.1. *Let p be a prime number and let G be a finite p-group. Assume that the class of G is at least 4 and that $\mathrm{int}(G) > 1$. Then $G^p = G_3$.*

We remark that, whenever p is larger than 3, Theorem 7.1 cannot be extended to groups of class 3. There are indeed examples, for $p > 3$, of finite p-groups of class 3, intensity greater than 1, and exponent p. We deal extensively with the case of 3-groups in Chapter 9.

7.1. Class 4 and intensity

The main purpose of Section 7.1 is to give the proof of the following proposition.

Proposition 7.2. *Let p be a prime number and let G be a finite p-group of class at least 4. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. If $\mathrm{int}(G) > 1$, then $G^p = G_3$.*

The following assumptions will be valid until the end of Section 7.1. Let p be a prime number. Let moreover G be a finite p-group of class 4 and denote by $(G_i)_{i\geq 1}$ the lower central series of G. For $i \in \{1, 2, 3, 4\}$, we define w_i to be $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$ (see Section 2.3). The following is an elementary result whose proof we leave to the reader. The importance of Lemma 7.3 will be clear once we will state Lemma 7.4.

Lemma 7.3. *Assume that $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$ and that $\mathrm{Z}(G) = G_4$. Then the commutator map induces a non-degenerate map $G/G_2 \times G_3/G_4 \to G_4$.*

We add here some extra assumptions and notation that will hold until the end of Section 7.1. Let $\rho : G \to G$ be defined by $x \mapsto x^p$. Assume that $\mathrm{int}(G) > 1$. It follows that p is odd and the group G is non-trivial (see Section 3.2). Let moreover α denote an intense automorphism of G of order 2 and write $A = \langle \alpha \rangle$. In concordance with Section 2.2, set

$$G^+ = \{g \in G \ : \ \alpha(g) = g\} \quad \text{and} \quad G^- = \{g \in G \ : \ \alpha(g) = g^{-1}\}.$$

We will introduce some additional notation right before stating Lemma 7.8.

Lemma 7.4. *One has $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$ and G has order p^6. Moreover, $\mathrm{Z}(G) = G_4$.*

Proof. The quadruple (w_1, w_2, w_3, w_4) is equal to $(2, 1, 2, 1)$ by Theorem 6.1 and the order of G is equal to p^6, as a consequence of Lemma 2.16. The centre of G is equal to G_4 thanks to Lemma 6.7. □

Lemma 7.5. *Let $\mathcal{M}$ be the collection of maximal subgroups of G and let $\mathcal{N}$ be the collection of normal subgroups of G that contain G_4 with index p. Let $f : \mathcal{M} \to \mathcal{N}$ be defined by $M \mapsto \mathrm{Z}(M)$. Then f is a bijection with inverse $f^{-1} : N \mapsto \mathrm{C}_G(N)$.*

Proof. We first show that f is well-defined. To this end, let M be a maximal subgroup of G. As a consequence of Lemmas 7.4 and 7.3, the subgroup $G_3 \cap \mathrm{Z}(C)$ has index p in G_3. The subgroup $\mathrm{Z}(C)$ being normal in G, Proposition 6.3 yields $\mathrm{Z}(C) \subseteq G_3$ and $|G_3 : \mathrm{Z}(C)| = |\,\mathrm{Z}(C) : G_4| = p$. We next show that $g : \mathcal{N} \to \mathcal{M}$, sending N to $\mathrm{C}_G(N)$, is well-defined. Let indeed N be a normal subgroup of G that contains G_4 with index p. As a consequence of Proposition 6.3, the subgroup M is contained in G_3. The commutator map from Lemma 7.3 being non-degenerate, it follows that $\mathrm{C}_G(M)$ is maximal in G. It is now easy to conclude, showing that f and g are inverses to each other. □

Lemma 7.6. *The map ρ induces a map $\overline{\rho} : G/G_2 \to G_3/G_4$.*

Proof. For each index $i \in \mathbb{Z}_{\geq 1}$, the subset $\rho(G_i)$ is contained in G_{i+2}, as a consequence of Proposition 4.12. In particular, $\rho(G_2)$ is contained in G_4. Let x be an element of G and define $C = \langle x, G_2 \rangle$; denote by $(C_i)_{i \geq 1}$ the lower central series of C. The quotient C/G_2 is cyclic, so $C_2 = [C, G_2]$. It follows that C_3 is contained in G_4, and, the prime p being odd, we get that $C_2^p C_p$ is contained in G_4. Let now $y \in G_2$. By the Hall-Petrescu formula, we have that $\rho(xy) \equiv \rho(x)\rho(y) \bmod C_2^p C_p$, and therefore $\rho(xy) \equiv \rho(x)\rho(y) \bmod G_4$. Since $\rho(y)$ belongs to G_4, the map $\overline{\rho}$ is well-defined. □

Lemma 7.7. *Let C be a maximal subgroup of G and assume that $\rho(C \setminus G_2) \cap G_4$ is not empty. Then $\rho(C \setminus G_2) = \{1\}$.*

Proof. Let H be a cyclic subgroup of C, not contained in G_2, and such that $\rho(H) \subseteq G_4$. Without loss of generality we assume that H is A-stable (otherwise we can take a conjugate of H that is A-stable, thanks to Lemma 3.5). As a consequence of Proposition 5.10, the automorphism α induces scalar multiplication by -1 on $H/(H \cap G_2)$, so, thanks to Lemma 2.6, the restriction of α to H^p coincides with scalar multiplication by -1. However, the subgroup H^p being contained in G_4, it follows from Proposition 5.10 that α coincides with the identity map on H^p. Lemma 2.8 yields $H^p = \{1\}$, and, the choiche of H being arbitrary, we get $\rho(C \setminus G_2) = \{1\}$. □

For each maximal subgroup C of G, define Y_C to be the collection of abelian subgroups of G that can be written as $\langle x \rangle \oplus \langle y \rangle$, with $x \in C \setminus G_2$ and $y \in \mathrm{Z}(C) \setminus G_4$. We will call Y_C^+ the set consisting of the A-stable elements of Y_C.

Lemma 7.8. *Let C be a maximal subgroup of G and assume that $\rho(C \setminus G_2) \cap G_4$ is not empty. Let H be an element of Y_C. Then H has exponent p and $H \cap G_4 = \{1\}$.*

Proof. Let $H = \langle x \rangle \oplus \langle y \rangle$ be an element of Y_C, where $x \in C \setminus G_2$ and $y \in \mathrm{Z}(C) \setminus G_4$. The subgroup $\mathrm{Z}(C)$ is normal in G and, as a consequence of Lemma 7.5, contained in G_3. From Proposition 4.12, it follows that $\mathrm{Z}(C)$ has exponent p, and thus $y^p = 1$. The element x^p is 1, by Lemma 7.7, and so $H^p = \{1\}$. To conclude, assume that $x^ay^b \in H \cap G_4$. Then $x^a = (x^ay^b)y^{-b}$ belongs to $H \cap G_3$, so $a \equiv 0 \bmod p$. Since $\langle y\rangle \cap G_4 = \{1\}$, we conclude that $H \cap G_4 = \{1\}$. □

Lemma 7.9. *Let C be a maximal subgroup of G and assume that $\rho(C \setminus G_2) \cap G_4$ is not empty. Then the cardinality of Y_C^+ is equal to p.*

Proof. We first claim that each element of Y_C^+ is contained in G^-. To this end, let $H = \langle x\rangle \oplus \langle y\rangle \in Y_C^+$, where $x \in C \setminus G_2$ and $y \in \mathrm{Z}(C) \setminus G_4$. By Lemma 7.8, the group H has exponent p and so the order of H is p^2. Since $\mathrm{dpt}_G(x) = 1$ and $\mathrm{dpt}_G(y) = 3$, Lemma 2.17 yields

$$|H| \geq |H \cap G^-| = p^{\mathrm{wt}_H^G(1)} p^{\mathrm{wt}_H^G(3)} \geq p^2 = |H|.$$

It follows that $H \cap G^- = H$ and the claim is proven. Write $C^- = C \cap G^-$ and $\mathrm{Z}(C)^- = \mathrm{Z}(C) \cap G^-$. Fix moreover a basis (x, y) for a subgroup H of G, where $x \in C^- \setminus G_2$ and $y \in \mathrm{Z}(C)^- \setminus G_4$. Thanks to Lemma 7.8, the set of equivalent bases for H is $B = \{(x^ay^b, y^c) : a, c \in \mathbb{F}_p^*,\ b \in \mathbb{F}_p\}$, and thus $|B| = p(p-1)^2$. Thanks to Lemmas 2.11 and 2.17, we compute

$$|Y_C^+| = \frac{|C^- \setminus G_2|\,|\mathrm{Z}(C^-) \setminus G_4|}{|B|} = \frac{(p^3 - p^2)(p-1)}{p(p-1)^2} = p.$$

□

Lemma 7.10. *Let C be a maximal subgroup of G and assume that $\rho(C \setminus G_2) \cap G_4$ is not empty. Then the cardinality of Y_C is equal to p^4.*

Proof. Fix (x, y) a basis for an element $H \in Y_C$, such that $x \in C \setminus G_2$ and $y \in \mathrm{Z}(C) \setminus G_4$. As a consequence of Lemma 7.8, the set of equivalent bases for H is $B = \{(x^ay^b, y^c) : a, c \in \mathbb{F}_p^*,\ b \in \mathbb{F}_p\}$, and so B has cardinality $p(p-1)^2$. It follows from Lemma 7.5 that

$$|Y_C| = \frac{|C \setminus G_2|\,|\mathrm{Z}(C) \setminus G_4|}{|B|} = \frac{(p^5 - p^4)(p^2 - p)}{p(p-1)^2} = p^4.$$

□

Lemma 7.11. *One has $\rho^{-1}(G_4) \subseteq G_2$.*

Proof. Assume by contradiction that there exists a maximal subgroup C of G such that $\rho(C \setminus G_2) \cap G_4$ is not empty. We claim that the normalizer of each element H of Y_C^+ is equal to HG_4. Assume by contradiction that there exists $K \in Y_C^+$ such that $\mathrm{N}_G(K) \neq KG_4$. Then $|G : \mathrm{N}_G(K)| < p^3$, and thus Lemma 3.6 yields

$$|Y_C| \leq \sum_{H \in Y_C^+} |G : \mathrm{N}_G(H)| < |Y_C^+|\,p^3.$$

By Lemma 7.9, the cardinality of Y_C^+ is equal to p, so we get a contradiction to Lemma 7.10. This proves the claim. In particular, given any $H \in Y_C^+$, the A-stable subgroup $\mathrm{N}_G(H)$ does not contain G_2. As a consequence of Lemma 2.17, the subgroup G^+ is not contained in $\mathrm{N}_G(H)$. From the combination of Lemmas 2.15 and 3.6, we get that

$$|Y_C| < \sum_{H \in Y_C^+} |G : \mathrm{N}_G(H)| = \sum_{H \in Y_C^+} |G : HG_4| \leq |Y_C^+| p^3.$$

Contradiction to Lemmas 7.9 and 7.10. □

Lemma 7.12. *Let $\overline{\rho}$ be as in Lemma* 7.6*. Let moreover C be a maximal subgroup of G. Then the following hold.*

1. *The map $\overline{\rho}$ is a bijection.*
2. *One has $\mathrm{Z}(C) = C^p$.*

Proof. The restriction of $\overline{\rho}$ to any cyclic subgroup of G/G_2 is a homomorphism, in particular the restriction to C/G_2. As a consequence of Lemma 7.11, the subgroup $\overline{\rho}(C/G_2)$ has size p, and so C^p is not contained in G_4. The subgroup C^p is characteristic in the normal subgroup C, and therefore C^p is normal in G. It follows from Proposition 6.3 that C^p contains G_4, and so, if $x \in C \setminus G_2$, then $C^p = \langle x^p, G_4\rangle$. By Lemma 7.3, the commutator map induces a non-degenerate map $\gamma : G/G_2 \times G_3/G_4 \to G_4$ and, if $x \in C$, then $\gamma(xG_2, x^pG_4) = 1$. It follows that $\gamma(C/G_2, \overline{\rho}(C/G_2)) = 1$ and so $C^p \subseteq \mathrm{Z}(C)$. Since γ is non-degenerate, we get $C^p = \mathrm{Z}(C)$, and thus (2) is proven. We now prove (1). Denote by $\mathcal{M}$ the collection of maximal subgroups of G. As a consequence of Lemma 7.5, the quotient G_3/G_4 is equal to $\bigcup_{M\in\mathcal{M}} \mathrm{Z}(M)/G_4 = \bigcup_{M\in\mathcal{M}} \overline{\rho}(M/G_2)$ and so $\overline{\rho}$ is surjective. By Lemma 7.4, the indices $|G_1 : G_2|$ and $|G_3 : G_4|$ are equal, so the map $\overline{\rho}$ is a bijection. □

We remark that Theorem 7.1 is the same as Proposition 7.2, which we now prove. Let Q be a finite p-group of class at least 4. Assume that $\mathrm{int}(Q) > 1$. As a consequence of Lemma 3.13, the group Q/Q_5 has intensity greater than 1, so Lemma 7.12 yields $Q_3 = Q^pQ_5$. The subgroup Q^p being normal in Q, it follows from Proposition 6.3 that $Q^p = Q_3$. The proof of Proposition 7.2 is now complete.

7.2. Class 5 and intensity

We recall that, if G is a finite group, we denote by $(G_i)_{i\geq 1}$ the lower central series of G. In this section, we prove the following result.

Proposition 7.13. *Let p be a prime number and let G be a finite p-group of class at least* 5*. If* $\mathrm{int}(G) > 1$*, then $G_2^p = G_4$.*

We will keep the following assumptions until the end of Section 7.2. Let p be a prime number and let G be a finite p-group. For any positive integer i, write $w_i = \mathrm{wt}_G(i)$ and assume that $|G_5| = p$. Then the class of G is 5. Assume moreover that $\mathrm{int}(G) > 1$, so that, thanks to Proposition 3.7, the prime p is odd. As a consequence of Lemmas 3.13 and 7.4, we have moreover that $(w_1, w_2, w_3, w_4, w_5) = (2, 1, 2, 1, 1)$ and that the order of G_5 is p^7. The centre of G is equal to G_5 by Lemma 6.7. Let α be an intense automorphism of G of order 2 and write $A = \langle\alpha\rangle$. In concordance with the notation from Section 2.2, write $G^+ = \{x \in G : \alpha(x) = x\}$. In conclusion, define X to be the collection of all subgroups of G whose jumps in G (see Section 2.3) are exactly 2 and 4 and denote $X^+ = \{H \in X : \alpha(H) = H\}$. Lemma 2.16 ensures that the elements of X have order p^2.

Lemma 7.14. *Assume that G_2 has exponent p. Let H be a subgroup of G. Then $H \in X$ if and only if there exist $x \in G_2 \setminus G_3$ and $y \in G_4 \setminus G_5$ such that $H = \langle x\rangle \oplus \langle y\rangle$.*

Proof. If $H = \langle x\rangle \oplus \langle y\rangle$, with $x \in G_2 \setminus G_3$ and $y \in G_4 \setminus G_5$, then H belongs to X, thanks to Lemma 2.16. We prove the converse. The subgroup H has order p^2 and H cannot be cyclic, because G_2 has exponent p. The jumps of H in G being 2 and 4, it follows from Lemma 2.16 that there exist elements x and y in H of depths respectively 2 and 4 in G. Since $[G_2, G_4] = \{1\}$, we have $H = \langle x\rangle \oplus \langle y\rangle$. □

Lemma 7.15. *Assume that G_2 has exponent p. Then $|X| = p^4$.*

Proof. Thanks to Lemma 7.14, all elements H of X are of the form $H = \langle x\rangle \oplus \langle y\rangle$, with $x \in G_2 \setminus G_3$ and $y \in G_4 \setminus G_5$. Let $(x, y) \in (G_2 \setminus G_3) \times (G_4 \setminus G_5)$ and let H be the $\mathbb{F}_p$-vector space that is spanned by x and y. The collection of equivalent bases for H is $B = \{(x^a y^b, y^c) : a, c \in \mathbb{F}_p^*, b \in \mathbb{F}_p\}$ and so B has cardinality $p(p-1)^2$. We then have

$$|X| = \frac{|G_2 \setminus G_3|\,|G_4 \setminus G_5|}{|B|} = \frac{(p^5 - p^4)(p^2 - p)}{p(p-1)^2} = p^4.$$

□

Lemma 7.16. *The exponent of G_2 is different from p.*

Proof. We work by contradiction, assuming that the exponent of G_2 is p. Write $C = \mathrm{C}_{G_3}(G_2)$ and $N = CG^+$. The group G^+ is contained in G_2, thanks to Lemma 2.17, so N is a subgroup of $\mathrm{N}_G(G^+)$. Using basic commutator calculus, it is not difficult to show that C is contained in G_3 with index at most p. It follows from Lemma 2.16 that the order of N is at least p^4 and so $|G : N| \le p^3$. Now, as a consequence of Lemma 2.17, the set X^+ has only one element, namely G^+, so Lemma 3.6 yields

$$|X| \le |G : \mathrm{N}_G(G^+)| \le |G : N| \le p^3.$$

Contradiction to Lemma 7.15. □

Lemma 7.17. *One has $\rho(G_2) = G_4$.*

Proof. We first claim that the restriction of ρ to G_2 is an endomorphism of G_2. Indeed, since G_2/G_3 is cyclic, one has $[G_2, G_2] = [G_2, G_3] \subseteq G_5$ and so the class of G_2 is at most 2. The prime p being odd, the Hall-Petrescu formula yields the claim. In particular, $\rho(G_2)$ is a characteristic subgroup of G and, by Lemma 7.16, it is non-trivial. Now, the centre of G is equal to G_5 so $G_5 \cap \rho(G_2)$ is non-trivial and therefore $\rho(G_2)$ contains G_5. Thanks to Proposition 4.12, the quotient G_2/G_4 is elementary abelian and so $G_5 \subseteq \rho(G_2) \subseteq G_4$. There are now only two possibilities: either $\rho(G_2) = G_4$ or $\rho(G_2) = G_5$. In the first case we are done, so assume by contradiction the second. Then, by Lemma 6.5, each element of $G_2 \setminus G_3$ has order p. It follows that G_2 is equal to the union of two proper subgroups, namely $\ker \rho_{|G_2}$ and G_3. Contradiction. □

We are finally ready to prove Proposition 7.13. To this end, let Q be a finite p-group of class at least 5 with $\mathrm{int}(Q) > 1$. Let moreover M be a normal subgroup of Q that is contained in Q_5 with index p. Then the group Q/M has class 5 and, as a consequence of Lemma 3.13, the intensity of Q/M is greater than 1. By Lemma 7.17, the subgroups $(Q_2/M)^p$ and Q_4/M are equal, and so $Q_2^p M = Q_4$. The subgroup Q_2^p being normal in Q, it follows from Proposition 6.3 that $Q_2^p = Q_4$. This concludes the proof of Proposition 7.13.

We remark that Proposition 7.13 can be easily derived, when p is greater than 3, from Theorem 7.1. We will show a way of doing so in Section 8.1.

CHAPTER 8

A Disparity between the Primes

The main result of Chapter 8 is Theorem 8.1. We recall that, if G is a finite p-group and i is a positive integer, then $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$, where $(G_i)_{i\geq 1}$ denotes the lower central series of G.

Theorem 8.1. *Let $p > 3$ be a prime number and let G be a finite p-group with $\mathrm{int}(G) > 1$. Let c denote the class of G and assume that $c \geq 3$. If i is a positive integer such that $\mathrm{wt}_G(i)\,\mathrm{wt}_G(i+1) = 1$, then $i = c - 1$.*

An equivalent way of formulating Theorem 8.1 is that of saying that, if G satisfies the assumptions of Theorem 8.1 and we write $w_i = \mathrm{wt}_G(i)$, then

$$(w_i)_{i\geq 1} = (2, 1, 2, 1, \ldots, 2, 1, f, 0, 0, \ldots) \text{ where } f \in \{0, 1, 2\}.$$

The restriction to primes greater than 3 in Theorem 8.1 is superfluous; it is however not worth the effort proving the result in general, since, as we will see in the next chapter, 3-groups of intensity greater than 1 have class at most 4 and we know from Theorems 5.2(2) and 6.1 that Theorem 8.1 is valid when c is 3 or 4.

8.1. Regularity

In Section 8.1 we make a distinction, for the first time, among the odd primes: namely we separate the cases $p = 3$ and $p > 3$. The main result of this section is Proposition 8.2, which determines which p-groups of intensity greater than 1 are *regular*, i.e. such that, for any two of their elements x and y, there always exists $\gamma \in [\langle x, y\rangle, \langle x, y\rangle]^p$ such that $(xy)^p = x^p y^p \gamma$. For an overview of regular p-groups, we refer to [**Hup67**, Ch. III.10].

Proposition 8.2. *Let p be a prime number and let G be a finite p-group. Assume that $\mathrm{int}(G) > 1$. Then the following are equivalent.*

1. *The group G is not regular.*
2. *The class of G is larger than 2 and $p = 3$.*

We will give the proof of Proposition 8.2 at the end of Section 8.1. We will rely on the fact that, if p is a prime number and G is a finite p-group such that

i. the class of G is at most $p - 1$, or
ii. one has $|G : G^p| < p^p$

then the group G is regular (see Sätze 10.2(a) and 10.13 in [**Hup67**, Ch. III]).

Lemma 8.3. *Let p be a prime number and let G be a finite p-group. Assume that G is regular. Then for all $k \in \mathbb{Z}_{\geq 0}$, the following hold.*

1. *One has $G^{p^k} = \rho^k(G)$.*
2. *One has $\mu_{p^k}(G) = \{x \in G \ :\ \rho^k(x) = 1\}$.*
3. *One has $|\mu_{p^k}(G)| = |G : G^{p^k}|$.*

Proof. The lemma is a combination of Sätze 10.5 and 10.7(a) from [**Hup67**], Chapter 3. □

Lemma 8.4. *Let $p > 3$ be a prime number and let G be a finite p-group. Assume that* $\mathrm{int}(G) > 1$. *Then the following hold.*

1. *The group G is regular.*
2. *If the class of G is at least 4, then $G_3 = \rho(G)$.*

Proof. If the class of G is at most 4, then G is regular (class $\leq p-1$). We assume that G has class at least 4. It follows from Lemma 3.13 that $\mathrm{int}(G/G_5)$ is larger than 1, and so, thanks to Lemma 7.4, the index $|G : G_3|$ is equal to p^3. From Theorem 7.1, we get that $G^p = G_3$, and therefore $|G : G^p| < p^p$. Then G is regular and so, by Lemma 8.3, the set $\rho(G)$ coincides with the subgroup G^p. □

We would like to stress that, for $p > 3$, Proposition 8.4(2) is a stronger version of Theorem 7.1. In fact, not only $G_3 = G^p = \langle \rho(G) \rangle$ but G_3 coincides with the set of p-th powers of elements of G.

Lemma 8.5. *LetG be a finite 3-group that can be generated by 2 elements. If G is regular, then G_2 is cyclic.*

Proof. See Satz 10.3(b) from [**Hup67**], Chapter III. □

Lemma 8.6. *Let G be a finite 3-group with* $\mathrm{int}(G) > 1$. *Then G is regular if and only if G has class at most 2.*

Proof. If G has class at most 2, then G is regular (class $\leq p-1$). Assume by contradiction that G is regular of class at least 3. As a consequence of Theorem 5.2(2), the group G is 2-generated, and so, by Lemma 8.5, the subgroup G_2 is cyclic. Proposition 4.12 yields that $G_3 = \{1\}$. Contradiction. □

We now give the proof of Proposition 8.2. To this end, let p be a prime number and let G be a finite p-group with $\mathrm{int}(G) > 1$. The intensity of G being greater than 1, it follows from Proposition 3.7 that p is odd. The implication (2) ⇒ (1) is given by Lemma 8.6. We prove (1) ⇒ (2). Assume that G is not regular. Then Lemma 8.4 yields $p = 3$ and so the class of G is larger than $p - 1 = 2$. The proof of Proposition 8.2 is complete.

8.2. Rank

The *rank* of a finite group G is the smallest integer r with the property that each subgroup of G can be generated by r elements. We denote the rank of G by $\mathrm{rk}(G)$. We will prove the following.

Proposition 8.7. *Let $p > 3$ be a prime number and let G be a finite p-group of class at least 4. If* $\mathrm{int}(G) > 1$, *then* $\mathrm{rk}(G) = 3$.

If G is a group and n is a positive integer, we set $\mu_n(G) = \langle x \in G : x^n = 1 \rangle$.

Lemma 8.8. *Let p be an odd prime number and let G be a non-trivial finite p-group. Then one has* $\mathrm{rk}(G) \leq \log_p |\mu_p(G)|$.

Proof. This is is Corollary 2 from [**Laf73**]. □

We give here the proof of Proposition 8.7. In order to do this, let $p > 3$ be a prime number and let G be a finite p-group of class at least 4, with $\mathrm{int}(G) > 1$. We first claim that $\mathrm{rk}(G) \leq 3$. Indeed, by Theorem 7.1, the subgroup G^p is equal to G_3 so the order of $\mu_p(G)$ is equal to $|G : G^p| = |G : G_3|$ (see [**Hup67**, Ch. III, Satz 10.7]). As a consequence of Theorem 6.1, the index $|G : G_3|$ is equal to p^3, and thus Lemma 8.8 yields $\mathrm{rk}(G) \leq \log_p |G : G_3| = 3$. This proves the claim. To conclude the proof of Proposition 8.7, it now suffices to present a subgroup of G whose minimum number of generators is at least 3. The group G/G_5 has class 4 and, thanks to Lemma 3.13, it has intensity greater than 1. As a consequence of Theorem 6.1, the index $|G_2 : G_4|$ is equal to p^3 and, thanks to Proposition 4.12, the quotient G_2/G_4 is elementary abelian. It follows that $\Phi(G_2) \subseteq G_4$ and the minimum number of generators for G_2 is at least $\log_p |G_2 : G_4| = 3$. Proposition 8.7 is now proven.

We would like to remark that, if $p = 3$, then Proposition 8.7 is not valid. We will see indeed in the next chapter that finite 3-groups of class 4 and intensity larger than 1 have a commutator subgroup that is elementary abelian of order p^4, so the rank of such groups is at least 4.

8.3. A sharper bound on the width

The aim of Section 8.3 is to give the proof of Proposition 8.9, which is the same as Theorem 8.1.

Proposition 8.9. *Let $p > 3$ be a prime and let G be a finite p-group with $\mathrm{int}(G) > 1$. Let c denote the class of G and assume that that $c \geq 3$. If i is a positive integer such that $\mathrm{wt}_G(i)\,\mathrm{wt}_G(i+1) = 1$, then $i = c - 1$.*

We list here a number of assumptions that will hold until the end of Section 8.3. Let $p > 3$ be a prime number and let G be a finite p-group with lower central series $(G_i)_{i\geq 1}$. Let c denote the class of G and, for each positive integer i, write $w_i = \mathrm{wt}_G(i)$. Assume that $\mathrm{int}(G) > 1$. Then, as a consequence of Proposition 3.7, the prime p is odd and G is non-trivial. Let α be an intense automorphism of G of order 2 and write $A = \langle\alpha\rangle$. It follows from the work done in the previous chapters that, under these assumptions, the following are satisfied:

i. if $i \in \mathbb{Z}_{\geq 1}$ is such that $w_i w_{i+1} = 1$, then $i > 1$;
ii. if $w_2 w_3 = 1$, then $c = 3$;
iii. if $c > 3$ and $i \in \mathbb{Z}_{\geq 1}$ is such that $w_i w_{i+1} = 1$, then $i \geq 4$.

Lemma 8.10. *Let $i \in \mathbb{Z}_{\geq 1}$ be minimal such that $w_i w_{i+1} = 1$. If $c > 3$, then i is even and $w_{i-1} = 2$.*

Proof. Assume $c > 3$. Then $i - 1 > 1$ and the width w_{i-1} is at most 2, as a consequence of Theorem 6.2. The index i being minimal with the property that $w_i w_{i+1} = 1$, it follows that $w_{i-1} = 2$. Another consequence of the minimality of i is that i is even. Indeed, thanks to Theorem 6.2 and the minimality of i, whenever $j < i$, the product $w_j w_{j+1}$ is equal to 2. Moreover, by Theorem 5.2(2), we have that $w_1 = 2$, so i is even. □

Lemma 8.11. *Let $i \in \mathbb{Z}_{\geq 1}$ be minimal such that $w_i w_{i+1} = 1$. Assume that $c > 3$ and that $w_{i+2} = 1$. Then G_{i-1}/G_{i+3} has exponent p.*

Proof. We write $\overline{G} = G/G_{i+3}$ and we will use the bar notation for the subgroups of $\overline{G}$. The intensity of $\overline{G}$ is larger than 1 thanks to Lemma 3.13. The group $[G_{i-1}, G_{i-1}]$ is contained in G_{2i-2} and the index i is larger than 3. It follows that $[G_{i-1}, G_{i-1}] \subseteq G_{2i-2} \subseteq G_{i+2}$, and therefore $\overline{G}_{i-1}$ has class at most 2 and $[\overline{G}_{i-1}, \overline{G}_{i-1}]^p = \{1\}$. Thanks to the Hall-Petrescu formula, the p-power map is an endomorphism of $\overline{G}_{i-1}$. By Proposition 4.12, the subgroup $\overline{G}_{i-1}^p$ is contained in $\overline{G}_{i+1}$ and, from Lemmas 8.3(3) and 8.10, it follows that

$$|\mu_p(\overline{G}_{i-1})| = |\overline{G}_{i-1} : \overline{G}_{i-1}^p| \geq |\overline{G}_{i-1} : \overline{G}_{i+1}| = p^3.$$

Also the order of $\overline{G}_i$ is equal to p^3 and, as a consequence of Proposition 6.3, the subgroup $\overline{G}_i$ is contained in $\mu_p(\overline{G}_{i-1})$. The p-power map factors thus as a homomorphism $\overline{G}_{i-1}/\overline{G}_i \to \overline{G}_{i+1}$. By Lemma 8.10, the index i is even, and so, by Proposition 5.10, the automorphism of $\overline{G}_{i-1}/\overline{G}_i$ that is induced by α is equal to the inversion map. It follows from Lemma 2.6 that α restricts to the inversion map on $\overline{G}_{i-1}^p$. Moreover, again by Proposition 5.10, the action of A on $\overline{G}_{i+2}$ is trivial. It follows from Lemma 2.8 that $\overline{G}_{i-1}^p \cap \overline{G}_{i+2} = \{1\}$. The subgroup $\overline{G}_{i-1}^p$ is clearly characteristic in $\overline{G}$, while the subgroup $\overline{G}_{i+2}$ is equal to the centre of $\overline{G}$, by Lemma 6.7. It follows that $\overline{G}_{i-1}^p = \{1\}$. □

We conclude Section 8.3 with the proof of Proposition 8.9. The integer i is larger than 1 and, if $i = 2$, then $c = 3 = i + 1$. We assume that i is greater than 2, so $c > 3$, and, without loss of generality, that i is minimal with the property that $w_i w_{i+1} = 1$. In particular, the subgroup G_{i+1} is non-trivial. If $G_{i+2} = \{1\}$, then the class of G is equal to $i + 1$, and so $i = c - 1$. Assume now by contradiction that G_{i+2} is non-trivial and let N be a normal subgroup of G that is contained in G_{i+2} with index p. Write $\overline{G} = G/N$ so that Lemma 3.13 yields $\mathrm{int}(\overline{G}) > 1$. By Lemma 8.10, the width $\mathrm{wt}_{\overline{G}}(i-1) = w_{i-1}$ is equal to 2 so, by Lemma 2.16, the order of $\overline{G}_{i-1}$ is equal to p^5. The index i being at least 4, the subgroup $[\overline{G}_{i-1}, \overline{G}_i]$ is contained in $\overline{G}_{i+3} = \{1\}$. It follows that $\overline{G}_{i-1}$ and $\overline{G}_i$ centralize each other. Let now M be a maximal subgroup of $\overline{G}_{i-1}$ that contains $\overline{G}_i$. The index $|M : \overline{G}_i|$ is equal to p, because $w_{i-1} = 2$, and so $[M, M] = [M, \overline{G}_i] = \{1\}$. Moreover, the order of M is equal to p^4 and M has exponent p, because of Lemma 8.11. In particular, M is a 4-dimensional vector space over $\mathbb{F}_p$. Contradiction to proposition 8.7.

CHAPTER 9

The Special Case of 3-groups

Let $R = \mathbb{F}_3[\epsilon]$ be of cardinality 9, with $\epsilon^2 = 0$. Denote by $\mathbb{A}$ the quaternion algebra

$$\mathbb{A} = R + R\mathrm{i} + R\mathrm{j} + R\mathrm{k}$$

with defining relations $\mathrm{i}^2 = \mathrm{j}^2 = \epsilon$ and $\mathrm{k} = \mathrm{ji} = -\mathrm{ij}$. Let the *bar map* on $\mathbb{A}$ be defined by

$$x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \ \mapsto\ \overline{x} = a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k}.$$

We write $\mathfrak{m} = \mathbb{A}\mathrm{i} + \mathbb{A}\mathrm{j}$, which is a 2-sided nilpotent ideal of $\mathbb{A}$, and we define $\mathrm{MC}(3)$ to be the subgroup of $1 + \mathfrak{m}$ consisting of those elements x satisfying $\overline{x} = x^{-1}$. The main result of this chapter is the following.

Theorem 9.1. *Let G be a finite 3-group. Then the following are equivalent.*

1. *The group G has class at least 4 and $\mathrm{int}(G) > 1$.*
2. *The group G has class 4, order 729, and $\mathrm{int}(G) = 2$.*
3. *The group G is isomorphic to $\mathrm{MC}(3)$.*

A considerable part of the present chapter is devoted to the proof of Theorem 9.1, which is given in Section 9.7. An essential contribution to it is given by the theory of "κ-groups" we develop.

Definition 9.2. A κ-group is a finite 3-group G such that $|G : G_2| = 9$ and with the property that the cubing map on G induces a bijective map $\kappa : G/G_2 \to G_3/G_4$.

Our interest in κ-groups arises from Lemma 7.12(1), which asserts that, if p is an odd prime number and G is a finite p-group of class at least 4 with $\mathrm{int}(G) > 1$, then the map $x \mapsto x^p$ induces a bijection $\overline{\rho} : G/G_2 \to G_3/G_4$. As a consequence of Theorem 5.2, each finite 3-group of class at least 4 and intensity greater than 1 is a κ-group, where κ coincides with $\overline{\rho}$. The reason why, in this chapter, we work exclusively with 3-groups is that they are more "difficult to deal with": several techniques that apply to the case in which p is a prime larger than 3 do not apply to the case of 3-groups of higher class, as the results from Chapter 8 suggest. For example, it is not difficult to show, using properties of regular groups, that, whenever $p > 3$ and G is a finite p-group, the map $\overline{\rho} : G/G_2 \to G_3/G_4$ from Lemma 7.12 is an isomorphism of groups, while, if G is a κ-group, then, given any two elements $x, y \in G/G_2$, one has

$$\kappa(xy) \equiv \kappa(x)\kappa(y)[xy^{-1}, [x, y]] \bmod G_4,$$

as we show in Lemma 9.7. What plays in our favour is that a finite 3-group G is a κ-group if and only if G/G_4 is a κ-group: to detect κ-groups it is thus sufficient to be able to detect κ-groups among the finite 3-groups of class 3. We will prove the following result.

THEOREM 9.3. *Let G be a finite 3-group of class 3. Then G is a κ-group if and only if G is isomorphic to* $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$.

In Section 9.4, we prove Theorem 9.3 by building κ-groups as quotients of a free group: we give a sketch of the proof here. Let F be the free group on 2 generators and let $(F_i)_{i\geq 1}$ be defined recursively by $F_1 = F$ and $F_{i+1} = [F, F_i]F_i^3$. Then $V = F/F_2$ is a vector space over $\mathbb{F}_3$ of dimension 2. Let moreover $L = F_3F^3$ and set $\overline{F} = F/([F, L]F_2^3)$; we use the bar notation for the subgroups of $\overline{F}$. We will show that the cubing map on F induces a map $V \to \overline{L}$, which we denote by c, and we will construct, in Sections 9.3 and 9.4, isomorphisms of the following $\mathrm{Aut}(F)$-sets, all having cardinality 3.

$$\mathcal{I}_V = \{k \subseteq \mathrm{End}(V) \text{ subfield} : |k| = 9\}$$

$$\downarrow$$

$$\mathcal{K}_V = \{\kappa : V \to V \otimes \textstyle\bigwedge^2(V) \text{ bijective} : \text{for all } x, y \in V, \text{ one has}$$
$$\kappa(x + y) = \kappa(x) + \kappa(y) + (x - y) \otimes (x \wedge y)\}$$

$$\downarrow$$

$$\mathcal{P} = \{\pi \in \mathrm{Hom}(\overline{L}, \overline{F_3}) : \pi \circ c \text{ is bijective}, \pi_{|\bar{F}_3} = \mathrm{id}_{\bar{F}_3}\}$$

$$\downarrow$$

$$\mathcal{N}_3 = \{N \subseteq F \text{ normal subgroup} : F/N \text{ is a } \kappa\text{-group of class } 3\}.$$

We will then prove that the natural action of $\mathrm{Aut}(F)$ on $\mathcal{I}_V$ is transitive and so it will follow that $\mathrm{Aut}(F)$ acts transitively on $\mathcal{N}_3$, leading to the fact that all κ-groups of class 3 are isomorphic to the κ-group $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$. To extend the investigation of κ-groups to class 4, we consider the "smallest possible case" and look at extensions of $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$ by a group of order 3. In Section 9.5, we prove the following result.

THEOREM 9.4. *Let G be a κ-group such that G_4 has order 3. Then G_2 is elementary abelian.*

It would be interesting to explore the world of κ-groups more extensively, however Theorems 9.3 and 9.4 provide us with sufficient information on the structure of κ-groups to be able to go into the proof of Theorem 9.1. Let G be a finite 3-group of class at least 4. We have seen that a necessary condition for $\mathrm{int}(G)$ to be greater than 1 is that of being a κ-group, however we can only hope to construct an intense automorphism of G of order 2 if

$(*)$ there exists an automorphism of G of order 2 that inverts all elements of G modulo G_2.

We proved in Section 5.3 that such an automorphism can always be constructed for G/G_4, so we want to understand which conditions we need to impose on the structure of G to be able to lift such an automorphism from G/G_4 to G. For this purpose, we define

$$\mathcal{N}_4 = \{N \subseteq F \text{ normal subgroup} : F/N \text{ is a } \kappa\text{-group of class 4 with}$$
$$\mathrm{wt}_{F/N}(4) = 1 \text{ and satisfying } (*)\}.$$

Via building a bijection $\mathcal{N}_4 \to \mathcal{N}_3$, we will be able to prove that the natural action of $\mathrm{Aut}(F)$ on $\mathcal{N}_4$ is transitive and so that, given M and N in $\mathcal{N}_4$, the quotients F/M and F/N are isomorphic. The group $\mathrm{MC}(3)$ being a κ-group of class 4 with

$\mathrm{wt}_{\mathrm{MC}(3)}(4) = 1$ and $(*)$, it follows that each quotient F/N, with $N \in \mathcal{N}_4$, is isomorphic to MC(3). Since MC(3) has an elementary abelian commutator subgroup, Proposition 7.13 yields that each finite 3-group of intensity greater than 1 has class at most 4.

9.1. The cubing map

In this section we prove some structural properties about κ-groups of class 4. We remind the reader that, if G is a finite 3-group and i is a positive integer, then the i-th width of G is defined to be $\mathrm{wt}_G(i) = \log_3 |G_i : G_{i+1}|$ (see Section 2.3). We warn the reader that we will make a set of assumptions, which will hold until the end of Section 9.1, right after Lemma 9.9.

Lemma 9.5. *Let G be a group of order* 81 *and class* 3. *Then the exponent of G is different from* 3.

Proof. It follows from the assuptions that $\mathrm{wt}_G(1) = 2$ and that $\mathrm{wt}_G(2) = \mathrm{wt}_G(3) = 1$. Let now $C = \mathrm{C}_G(G_2)$. By Lemma 5.12, the centre of G is equal to G_3 and C contains G_2 with index 3. Let $(a, b) \in G \times C$ be such that $\{a, b\}$ generates G and define $c = [a, b]$, which is an element of $G_2 \setminus G_3$. Let moreover d be a generator for G_3. Assume by contradiction that the exponent of G is 3. Then C is elementary abelian and, in particular, $G_2 = \langle c\rangle \oplus \langle d\rangle$. Since G_2 is central modulo G_3 and d generates G_3, there exists an integer k such that $aca^{-1} = cd^k$ and $d^k \neq 1$. Keeping in mind that C is abelian, we compute

$$1 = (ba)^3 = bababa = b(cba)(cba)a = b^2cacba^2 =$$
$$b^2c^2d^kaba^2 = b^2c^2d^kcba^3 = b^3c^3d^k = d^k.$$

Contradiction. □

We recall here that, if G is a group and n is a positive integer, then G^n is defined to be $G^n = \langle x^n : x \in G\rangle$.

Lemma 9.6. *Let G be a finite* 3*-group of class* 3 *such that* $|G : G_2| = 9$. *Then* $G_3 = G^3$.

Proof. Assume by contradiction that $G_3 \neq G^3$ and let M be a normal subgroup of G such that $G^3 \subseteq M \subseteq G_3$ and $|G_3 : M| = 3$. Then the exponent of G/M is 3. Contradiction to Lemma 9.5. □

Lemma 9.7. *Let G be a group of class at most* 3 *and assume that G_2 has exponent dividing* 3. *Then, for all $x, y \in G$, one has* $(xy)^3 = x^3y^3[xy^{-1}, [x, y]]$.

Proof. Use the fact that G_2 has exponent 1 or 3, the fact that G_3 is central and the bilinearity of the map $G/G_2 \times G_2/G_3 \to G_3$ that is induced by the commutator map. □

Lemma 9.8. *Let G be a finite* 3*-group of class at least* 3 *and assume that* $|G : G_2| = 9$. *Then the cubing map induces a map* $\kappa : G/G_2 \to G_3/G_4$.

Proof. We assume without loss of generality that $G_4 = \{1\}$. As a consequence of Lemma 9.6, the image of the cubing map is contained in G_3 and, by Lemma 5.13, the commutator subgroup of G has exponent 3. We now prove that the map $\kappa : G/G_2 \to G_3$, given by $\kappa(xG_2) = x^3$, is well-defined. To this end, let

$(x, y) \in G \times G_2$. Then $y^3 = 1$ and $[y, x]$ belongs to G_3, a central subgroup. From Lemma 9.7, we get

$$(xy)^3 = x^3y^3[[y, x], xy^{-1}] = x^3y^3 = x^3$$

so every element of xG_2 has the same cube x^3 in G, as claimed. □

We remark that, in concordance with Definition 9.2, the real requirement for a 3-group G satisfying $|G : G_2| = 9$ to be a κ-group is that the map from Lemma 9.8 is a bijection. The reason why we are interested in κ-groups is given by the following lemma.

Lemma 9.9. *Let G be a finite 3-group of class 4 with $\text{int}(G) > 1$. Then G is a κ-group.*

Proof. Take $p = 3$ in Lemma 7.12(1). □

In the remaining part of this section, we will prove some structural results about κ-groups. Until the end of Section 9.1, let thus G be a finite 3-group of class 4. Let $(G_i)_{i\geq1}$ denote the lower central series of G and, for each $i \in \mathbb{Z}_{\geq1}$, denote $w_i = \text{wt}_G(i)$. Assume that $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$ and, to conclude, let $\kappa : G/G_2 \to G_3/G_4$ be the map from Lemma 9.8. It follows from these assuptions that $\Phi(G) = G_2$, that G_2 is abelian, and that the commutator map $G\times G_2 \to G_3$ induces an isomorphism $G/G_2\otimes G_2/G_3 \to G_3/G_4$. We recall that, if C is a group and n is a positive integer, then C^n and $\mu_n(C)$ are respectively defined as $C^n = \langle x^n : x \in C\rangle$ and $\mu_n(C) = \langle x \in C : x^n = 1\rangle$.

Lemma 9.10. *Let C be a maximal subgroup of G. Then $G_4C^3 \subseteq \text{Z}(C)$.*

Proof. The subgroup G_4 is central in G, so G_4 is contained in $\text{Z}(C)$. The commutator map induces a homomorphism $\gamma : G/G_2 \otimes G_3/G_4 \to G_4$ and, C/G_2 being cyclic, the subgroup $\gamma(C/G_2 \otimes \kappa(C/G_2))$ is trivial. The quotient G_4C^3/G_4 being equal to $\kappa(C/G_2)$, it follows that $G_4C^3 \subseteq \text{Z}(C)$. □

Lemma 9.11. *Assume that G is a κ-group. Then $\text{Z}(G) = G_4$.*

Proof. We first claim that $G_4 \subseteq \text{Z}(G)G_3$. The subgroup G_4 is contained in $\text{Z}(G)$ and, as a consequence of Lemma 5.12, one has $\text{Z}(G)/G_4 \subseteq \text{Z}(G/G_4) = G_3/G_4$. Since the class of G is 4, the claim is proven. Now, G_2 is equal to $\Phi(G)$ and so, the dimension w_1 being equal to 2, the group G has precisely 4 maximal subgroups. We claim that there exists at most one maximal subgroup C of G such that $G_3 \subseteq \text{Z}(C)$. Let indeed C and D be maximal subgroups of G such that G_3 is contained in $\text{Z}(C) \cap \text{Z}(D)$. Then CD centralizes G_3 and, the class of G being equal to 4, the subgroup CD is different from G. It follows that $C = D$ and thus the claim is proven. As a consequence of it, there exist two distinct maximal subgroups C and D of G such that neither $\text{Z}(C)$ nor $\text{Z}(D)$ contains G_3. Fix such C and D. Since κ is a bijection and $w_3 = 2$, Lemma 9.10 yields $\text{Z}(C) \cap G_3 = C^3G_4$ and $\text{Z}(D) \cap G_3 = D^3G_4$. Now, the subgroup $\text{Z}(G)$ contains G_4 and is contained in $\text{Z}(C) \cap \text{Z}(D) \cap G_3 = C^3G_4 \cap D^3G_4$. The map κ being a bijection, the subgroup $C^3G_4 \cap D^3G_4$ is equal to G_4 and therefore $\text{Z}(G) = G_4$. □

Lemma 9.12. *Let C be a maximal subgroup of G. Assume moreover that G is a κ-group and that G_2 has exponent 3. Then $[C, C] \cap \text{Z}(C) = G_4$.*

Proof. The quotient C/G_2 is cyclic of order 3 so $[C,C]=[C,G_2]$. It follows that $[C,C]$ is contained in G_3 and that the index of $([C,C]G_4)/G_4$ in G_3/G_4 is equal to $|G:C|=3$. In particular, $[C,C]$ is non-trivial. Now, $[C,C]$ is normal in G and thus $[C,C]\cap \mathrm{Z}(G)\neq 1$. Moreover, by Lemma 9.11, the centre of G is equal to G_4 and so $[C,C]$ contains G_4. As a result, $[C,C]$ is equal to $[C,C]G_4$ and it has thus cardinality 9. In an analogous way, since G is a κ-group, the normal subgroup C^3 is non-trivial and it contains G_4. However, C^3 is different from G_4 because G is a κ-group. We have proven that G_4 is contained in $[C,C]\cap \mathrm{Z}(C)$. We assume now by contradiction that $[C,C]\cap \mathrm{Z}(C)$ is different from G_4. It follows that $[C,C]\cap \mathrm{Z}(C)$ has cardinality at least 9, which is the same as the cardinality of $[C,C]$. Then $[C,C]$ is contained in $\mathrm{Z}(C)$ and so it follows from the Hall-Petrescu formula that the cubing map is an endomorphism of C. By assumption, the exponent of G_2 is 3, and so $|C^3|=|C:\mu_3(C)|\leq |C:G_2|=3$. Since C^3 contains G_4, we get that $C^3=G_4$. Contradiction. □

Lemma 9.13. *Assume that G is a κ-group. Then G_3 has exponent* 3.

Proof. The subgroup G_2 is abelian and G_2^3 is contained in G_4, as a consequence of Lemma 9.8. It follows that $\mu_3(G_2)$ has cardinality at least $|G_2:G_4|=27$. Set $N=\mu_3(G_2)\cap G_3$. We denote $\overline{G}=G/N$ and use the bar notation for the subgroups of $\overline{G}$. If $\overline{G_3}=\{1\}$, then G_3 is contained in $\mu_3(G_2)$ and we are done. Assume by contradiction that $\overline{G_3}$ is non-trivial. Then $\overline{G_3}$ has cardinality at least 3 so, $\mu_3(G_2)$ consisting of at least 27 elements, it follows that $\overline{\mu_3(G_2)}$ is non-trivial. However, $\overline{\mu_3(G_2)}$ has trivial intersection with $\overline{G_3}$, which is equal to $\mathrm{Z}(\overline{G})$, thanks to Lemma 5.12. Contradiction. □

9.2. A specific example

This section is entirely devoted to understanding the structure of the group MC(3), which is defined at the beginning of the present chapter. The name MC(3) refers to the fact that MC(3) turns out to be an example of maximal class among the finite 3-groups of intensity greater than 1. Moreover, as stated in Theorem 9.1, given any finite 3-group G of class at least 4, either $\mathrm{int}(G)=1$ or G is isomorphic to MC(3). We recall the definition of MC(3).

Let $R=\mathbb{F}_3[\epsilon]$ be of cardinality 9, with $\epsilon^2=0$, and let $\mathbb{A}$ denote the quaternion algebra $\left(\frac{\epsilon,\epsilon}{R}\right)$. In other words, $\mathbb{A}$ is given by

$$\mathbb{A}=R+R\mathrm{i}+R\mathrm{j}+R\mathrm{k}$$

with defining relations $\mathrm{i}^2=\mathrm{j}^2=\epsilon$ and $\mathrm{k}=\mathrm{ji}=-\mathrm{ij}$. The ring $\mathbb{A}$ has a unique (left/right/2-sided) maximal ideal $\mathfrak{m}=\mathbb{A}\mathrm{i}+\mathbb{A}\mathrm{j}$ and the residue field $k=\mathbb{A}/\mathfrak{m}$ is equal to $\mathbb{F}_3$. The algebra $\mathbb{A}$ is also equipped with a natural anti-automorphism of order 2, which is defined by

$$x=s+t\mathrm{i}+u\mathrm{j}+v\mathrm{k}\ \mapsto\ \overline{x}=s-t\mathrm{i}-u\mathrm{j}-v\mathrm{k}.$$

We define MC(3) to be the subgroup of $1+\mathfrak{m}$ consisting of those elements x satisfying $\overline{x}=x^{-1}$. We denote by $(\mathrm{MC}(3)_i)_{i\geq 1}$ the lower central series of MC(3) and, for each $i\in\mathbb{Z}_{\geq 1}$, we define moreover $M_i=(1+\mathfrak{m}^i)\cap G$. One easily shows that $(M_i)_{i\geq 1}$ is central and that, for each $i\geq 1$, the commutator map induces a map

$M_1/M_2 \times M_i/M_{i+1} \to M_{i+1}/M_{i+2}$ whose image generates M_{i+1}/M_{i+2}. For each $i \geq 1$, it follows that $M_{i+1} = [M_1, M_i]$ and, since $M_1 = G$, we have that

$$\mathrm{MC}(3)_i = \mathrm{MC}(3) \cap (1 + \mathfrak{m}^i).$$

The rest of the present section is devoted to the proof of some technical Lemmas that we will use in the proof of Theorem 9.1.

Lemma 9.14. *The group* MC(3) *has class* 4 *and order* 729.

Proof. We start by proving that MC(3) has order 729. The cardinality of R is equal to 9 and therefore the cardinality of $\mathbb{A}$ is 9^4. Since $\mathbb{A}/\mathfrak{m}$ is isomorphic to $\mathbb{F}_3$, the cardinality of $\mathfrak{m}$ is equal to $(9^4/3) = 3^7$ and therefore also $1+\mathfrak{m}$ has cardinality 3^7. Now, asking for an element $x \in 1+\mathfrak{m}$ to satisfy $x\overline{x} = 1$ lowers our freedom in the choice of coordinates of x by 1 and therefore G has cardinality $3^6 = 729$. To conclude the proof, we note that $\mathrm{MC}(3)_5$ is trivial, because $\mathfrak{m}^5 = \{0\}$, while $1 + \epsilon\mathrm{k}$ is a non-trivial element of $\mathrm{MC}(3)_4$. It follows that MC(3) has class 4. □

Lemma 9.15. *Set* $G = \mathrm{MC}(3)$ *and, for each* $i \in \mathbb{Z}_{\geq 1}$, *denote* $w_i = \mathrm{wt}_G(i)$. *Then the following hold.*

1. *One has* $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$.
2. *There exist generators* a *and* b *of* G *such that* $a^3 \equiv [b,[a,b]]^{-1} \bmod G_4$ *and* $b^3 \equiv [a,[a,b]] \bmod G_4$.

Proof. (1) Let $i \in \{1,2,3,4\}$. Then the function $G \to \mathfrak{m}$ that is defined by $x \mapsto x - 1$ induces an injective homomorphism $d_i : G_i/G_{i+1} \to \mathfrak{m}^i/\mathfrak{m}^{i+1}$, which commutes with the bar map of $\mathbb{A}$. Now, for each element $x \in G_i$, one has that $\overline{x-1} + (x-1)$ belongs to $\mathfrak{m}^{i+1}$ and therefore the image of d_i is contained in $D_i = \{y + \mathfrak{m}^{i+1} : y \in \mathfrak{m}^i, \overline{y} + y \in \mathfrak{m}^{i+1}\}$. With an easy computation, one shows that D_i coincides with the image of d_i and, consequently, that $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. To prove (2), define

$$a = 1 - \epsilon + \mathrm{i} \quad \text{and} \quad b = 1 - \epsilon + \mathrm{j}$$

and note that a and b belong to G. Since $w_1 = 2$ and a and b are linearly independent modulo $G_2 = G \cap (1 + \mathfrak{m}^2)$, the group G is generated by a and b. Using the defining properties of $\mathbb{A}$, we compute $a^3 = 1 + \epsilon\mathrm{i}$ and $b^3 = 1 + \epsilon\mathrm{j}$. Define $c = [a, b]$, $d = [a, c]$, and $e = [b, c]$. Then, working modulo G_3, we get

$$c = ab\overline{a}\overline{b} \equiv 1 - \mathrm{k} \bmod G_3.$$

Moreover, one has $d \equiv [a, 1 + \mathrm{k}] \bmod G_4$ and $e \equiv [b, 1 + \mathrm{k}] \bmod G_4$ and it is now easy to compute $d \equiv 1 + \epsilon\mathrm{j} \bmod G_4$ and $e \equiv 1 - \epsilon\mathrm{i} \bmod G_4$. It follows that both ea^3 and $d^{-1}b^3$ belong to G_4 and so the proof is complete. □

We remind the reader that, in concordance with Definition 9.2, a κ-group is a finite 3-group G such that $|G : G_2| = 9$ and such that the cubing map on G induces a bijection $G/G_2 \to G_3/G_4$.

Lemma 9.16. *The group* MC(3) *is a* κ*-group.*

Proof. Write $G = \mathrm{MC}(3)$ and, for each $i \in \mathbb{Z}_{\geq 1}$, denote $w_i = \mathrm{wt}_G(i)$. By Lemma 9.14, the group G has class 4 and, by Lemma 9.15(1), one has $w_1 = w_3 = 2$ and $w_2 = w_4 = 1$. Let $\kappa : G/G_2 \to G_3/G_4$ be as in Lemma 9.8; we want to show that κ is a bijection. Let a and b be as in Lemma 9.15(2) and define $d = [a,[a,b]]$ and $e = [b,[a,b]]$. Then $\kappa(a) \equiv e^{-1} \bmod G_4$ and $\kappa(b) \equiv d \bmod G_4$. Moreover, since

$w_2 = 1$, the elements d and e generate G_3 modulo G_4. We claim that κ is surjective. Let r, s be integers and let $y = d^s e^r$. If $r = 0$ or $s = 0$, then $\kappa(b^s) \equiv y \bmod G_4$ or $\kappa(a^{-r}) \equiv e^r \bmod G_4$. The quotient G_3/G_4 being elementary abelian, we may now assume that r and s are both non-zero modulo 3 and they satisfy therefore $r^2 \equiv s^2 \equiv 1 \bmod 3$. Define $x = a^r b^{-s}$. Working modulo G_4, we get from Lemma 9.7 that

$$\kappa(x) \equiv a^{3r}b^{-3s}[a^rb^s,[a^r,b^{-s}]] \equiv e^{-r}d^{-s}[a,[a,b]]^{-r^2s}[b,[a,b]]^{-rs^2} \equiv e^{-r-rs^2}d^{-s-r^2s}$$
$$\equiv e^{-2r}d^{-2s} \equiv y \bmod G_4.$$

The widths w_1 and w_3 being the same, it follows that κ is a bijection. □

Lemma 9.17. *Define* $\alpha : \mathrm{MC}(3) \to \mathrm{MC}(3)$ *by*

$$x = s + t\mathrm{i} + u\mathrm{j} + v\mathrm{k} \ \mapsto\ \alpha(x) = s - t\mathrm{i} - u\mathrm{j} + v\mathrm{k}.$$

Then α *is an automorphism of order* 2 *of* $\mathrm{MC}(3)$ *that induces the inversion map on* $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_2$.

Proof. Set $G = \mathrm{MC}(3)$. It is easy to check that α is an automorphism of order 2 of G, so we prove that α induces the inversion map on G/G_2. The subgroup G_2 is equal to $G \cap (1+\mathfrak{m}^2)$ and, thanks to Lemma 9.15(1), the group G/G_2 is elementary abelian of order 9. We define $a = 1 - \epsilon + \mathrm{i}$ and $b = 1 - \epsilon + \mathrm{j}$. Then a and b span G modulo G_2 and $\alpha(a) = \bar{a} = a^{-1}$ and $\alpha(b) = \bar{b} = b^{-1}$. The quotient G/G_2 being commutative, the map $G/G_2 \to G/G_2$ that is induced by α is $x \mapsto x^{-1}$. □

We conclude Section 9.2 by remarking that another characterization of MC(3) has been provided by Derek Holt and Frieder Ladisch; this characterization was found using computer algebra systems. The group MC(3) turns out to be isomorphic to a Sylow 3-subgroup of the Schur cover 3.J$_3$ of the simple Janko-3 group J$_3$. If S is a Sylow 3-subgroup of 3.J$_3$ and N denotes the normalizer of S in 3.J$_3$, then conjugation under any element of order 2 of N restricts to an automorphism of order 2 of S that induces the inversion map on the abelianization. The isomorphism class of MC(3) is denoted by $[729, 57]$ in the GAP system.

9.3. Structures on vector spaces

Until the end of Section 9.3, the following notation will be adopted. Let V be a 2-dimensional vector space over $\mathbb{F}_3$. A *κ-structure* on V is a bijective map $\kappa : V \to V \otimes \bigwedge^2 V$ such that, for each $x, y \in V$, one has

$$\text{(A1)} \qquad \kappa(x+y) = \kappa(x) + \kappa(y) + (x-y) \otimes (x \wedge y).$$

We denote by $\mathcal{K}_V$ the collection of κ-structures of V and by $\mathcal{I}_V$ the collection of subfields of $\mathrm{End}(V)$ of cardinality 9. We remark that, for each element k of $\mathcal{I}_V$, there exists $i \in \mathrm{End}(V)$ such that $i^2 = -1$ and $k = \mathbb{F}_3[i]$. Moreover, V is naturally a vector space of dimension 1 over each of the elements of $\mathcal{I}_V$. The rest of Section 9.3 will be devoted to the proof of the following result. Until the end of Section 9.3, all tensor and wedge products will be defined over $\mathbb{F}_3$.

Proposition 9.18. *Let* V *be a* 2*-dimensional vector space over* $\mathbb{F}_3$ *and let the map* $s_V : \mathcal{I}_V \longrightarrow \mathcal{K}_V$ *be defined by*

$$k = \mathbb{F}_3[i] \ \mapsto\ (x \mapsto ix \otimes (ix \wedge x)).$$

Then s_V *is a bijection. Moreover, the cardinality of* $\mathcal{K}_V$ *is equal to* 3.

As the goal of this section is to prove Proposition 9.18, we will respect the notation of the very same proposition until the end of Section 9.3.

We put a field structure on V, via an $\mathbb{F}_3$-linear isomorphism with $\mathbb{F}_9$. We define then Λ to be the collection of bijective maps $\lambda : V \to V$ such that, for all $x, y \in V$, one has

$$\lambda(x+y) = \lambda(x) + \lambda(y) + (x-y)(xy^3 - x^3y). \tag{A2}$$

We let moreover $\sigma_V : \mathcal{I}_V \to \Lambda_V$ be defined by

$$k = \mathbb{F}_3[i] \;\mapsto\; (x \mapsto ix((ix)x^3 - (ix)^3x)).$$

Lemma 9.19. *The map $V \to V$, defined by $x \mapsto x^5$, is an element of Λ.*

Proof. The group of units of V has order 8 and, since 8 and 5 are coprime, the map $x \mapsto x^5$ is a bijection $V^* \to V^*$ which extends to a bijection $V \to V$. Let now x and y be elements of V. Keeping in mind that V has characteristic 3, one computes

$$(x+y)^5 = \sum_{k=0}^{5} \binom{5}{k} x^k y^{5-k} = x^5 + y^5 + (x-y)(xy^3 - x^3y)$$

and therefore $x \mapsto x^5$ satisfies (A2). □

Lemma 9.20. *The map σ_V is well-defined.*

Proof. Let $k = \mathbb{F}_3[i]$ be an element of $\mathcal{I}_V$. The group k^* is cyclic of order 8 and there are therefore exactly two square roots of -1 in k, namely i and $-i$. Now, for each element x of V, we have

$$ix((ix)x^3 - (ix)^3x)) = -ix((-ix)x^3 - (-ix)^3x))$$

and thus k gives a map $V \to V$. Let now $k \to V$ denote an isomorphism of fields and identify i with its image in V. Then, for each $x \in V$, we have

$$ix((ix)x^3 - (ix)^3x) = x(ix)^2(x^2 - (ix)^2) = -x^3(x^2 + x^2) = x^5$$

and so, as a consequence of Lemma 9.19, the map σ_V is well-defined. □

Lemma 9.21. *Let $\mathbb{P}V$ denote the collection of 1-dimensional subspaces of V. Then the natural homomorphism $\mathrm{Aut}(V) \to \mathrm{Sym}(\mathbb{P}V)$ induces an isomorphism $\mathrm{Aut}(V)/\mathbb{F}_3^* \to \mathrm{Sym}(\mathbb{P}V)$.*

Proof. The natural map $\mathrm{Aut}(V) \to \mathrm{Sym}(\mathbb{P}V)$ factors as an injective homomorphism $\mathrm{Aut}(V)/\mathbb{F}_3^* \to \mathrm{Sym}(\mathbb{P}V)$, which is in fact also surjective, because $|\,\mathrm{Aut}(V) : \mathbb{F}_3^*| = 24 = |\,\mathrm{S}_4\,| = |\,\mathrm{Sym}(\mathbb{P}V)|$. □

Lemma 9.22. *The set $\mathcal{I}_V$ has cardinality 3. Moreover, the action by conjugation of $\mathrm{Aut}(V)$ on $\mathcal{I}_V$ is transitive.*

Proof. Let $f : \mathcal{I}_V \to \mathrm{Aut}(V)/\mathbb{F}_3^*$ be defined by $k = \mathbb{F}_3[i] \mapsto i\mathbb{F}_3^*$ and observe that, since $\mathbb{F}_3[i] = \mathbb{F}_3[-i]$, the map f is well-defined. Moreover, since each element of $\mathcal{I}_V$ is uniquely determined, modulo $\mathbb{F}_3^*$, by a square root of -1, the map f is injective. Let $\mathbb{P}V$ denote the collection of 1-dimensional subspaces of V and let $\epsilon : \mathrm{Aut}(V)/\mathbb{F}_3^* \to \mathrm{S}_4$ be the composition of the isomorphism $\mathrm{Aut}(V)/\mathbb{F}_3^* \to \mathrm{Sym}(\mathbb{P}V)$ from Lemma 9.21 with a given isomorphism $\mathrm{Sym}(\mathbb{P}V) \to \mathrm{S}_4$. Then $(\epsilon \circ f)(\mathcal{I}_V)$ consists of elements of order 2. Now, each element k of $\mathcal{I}_V$ can be written as

$k = \mathbb{F}_3[i]$, with $i^2 = -1$, and this suffices to show that $(\epsilon \circ f)(\mathcal{I}_V)$ is in fact contained in the Klein subgroup V_4 of S_4. The set $V_4 \setminus \{1\}$ forms a unique conjugacy class in S_4 and thus the elements of $\mathcal{I}_V$ form a unique orbit under the action by conjugation of $\mathrm{Aut}(V)$. Since the set $V_4 \setminus \{1\}$ has cardinality 3, the cardinality of $\mathcal{I}_V$ is also equal to 3. □

Lemma 9.23. *Write $V = \mathbb{F}_3[i]$, with $i^2 = -1$. Then the map $\bigwedge^2 V \to \mathbb{F}_3 i$ defined by $x \wedge y \mapsto xy^3 - x^3y$ is an isomorphism of vector spaces.*

Proof. Let $\phi : V \times V \to V$ be defined by $(x, y) \mapsto xy^3 - x^3y$. It is easy to show that ϕ is alternating and that $\phi(V \times V)$ is contained in $\mathbb{F}_3 i$, the eigenspace of the Frobenius homomorphism that is associated to -1. Moreover, the map ϕ is non-zero. It follows that ϕ induces a linear homomorphism $\phi' : \bigwedge^2 V \to \mathbb{F}_3 i$ that is non-trivial. Since both $\bigwedge^2 V$ and $\mathbb{F}_3 i$ have dimension 1 over $\mathbb{F}_3$, the map ϕ' is an isomorphism. □

Write $V = \mathbb{F}_3[i]$ with $i^2 = -1$. Define $\theta : V \otimes \bigwedge^2 V \to V \otimes \mathbb{F}_3 i$ by

$$\theta(a \otimes (x \wedge y)) = a \otimes (xy^3 - x^3y)$$

and note that θ is an isomorphism of vector spaces, as a consequence of Lemma 9.23. Let moreover $\mu : V \otimes \mathbb{F}_3 i \to V$ be the isomorphism of vector spaces that is defined by $x \otimes y \mapsto xy$. We keep this notation until the end of Section 9.3.

Lemma 9.24. *The map $l_V : \mathcal{K}_V \to \Lambda$ that is defined by $\kappa \mapsto \mu \circ \theta \circ \kappa$ is bijective.*

Proof. Let κ be an element of $\mathcal{K}_V$. Then $l_V(\kappa)$ is bijective, because it is the composition of bijective maps, and, for each $x, y \in V$, one has

$$l_V(\kappa)(x + y) = \mu \circ \theta \circ \kappa(x + y) = l_V(\kappa)(x) + l_V(\kappa)(y) + (x - y)(xy^3 - x^3y).$$

We have proven that $l_V(\kappa)$ belongs to Λ and so l_V is well-defined. Moreover, l_V is bijective, because μ and θ are bijective. □

Lemma 9.25. *Let l_V be as in Lemma 9.24. Then $\sigma_V = l_V \circ s_V$ and s_V is well-defined.*

Proof. Let $k = \mathbb{F}_3[i]$ be an element of $\mathcal{I}_V$. Let moreover κ and λ respectively denote $s_V(k)$ and $\sigma_V(k)$. Then one has $l_V(\kappa)(x) = \mu \circ \theta(ix \otimes ix \wedge x) = \lambda(x)$ and so, the choices of k and x being arbitrary, $\sigma_V = l_V \circ s_V$. As a consequence, the map s_V is well-defined. □

Lemma 9.26. *The map s_V is injective.*

Proof. Let k and k' be elements of $\mathcal{I}_V$ and let $i, j \in \mathrm{End}(V)$ be such that $k = \mathbb{F}_3[i]$, $k' = \mathbb{F}_3[j]$, and $i^2 = j^2 = -1$. Assume moreover that $s_V(k) = s_V(k')$. For each $x \in V$, we have $\mathbb{F}_3 x + \mathbb{F}_3 ix = V = \mathbb{F}_3 x + \mathbb{F}_3 jx$ and therefore there exists $\omega_x \in \{\pm 1\}$ such that $ix \equiv \omega_x jx \bmod \mathbb{F}_3 x$. For each $x \in V$, it then follows that

$$jx \otimes (jx \wedge x) = ix \otimes (ix \wedge x) = ix \otimes ((\omega_x jx) \wedge x) = \omega_x ix \otimes (jx \wedge x)$$

and, $\mu \circ \theta$ being bijective, jx and $\omega_x ix$ are the same. The choice of x being arbitrary, we get

$$V = \{x \in V : ix = jx\} \cup \{x \in V : ix = -jx\}$$

and so, V being equal to the union of two subgroups, either $i = j$ or $i = -j$. In either case, i and j are linearly dependent over $\mathbb{F}_3$ and so $k = k'$. □

Lemma 9.27. *Let ϕ be an $\mathbb{F}_3$-linear endomorphism of V. Then there exist unique $a, b \in V$ such that, for each $x \in V$, one has $\phi(x) = ax^3 + bx$.*

Proof. The characteristic of V being 3, for each pair (a, b) in V^2, the map $x \mapsto ax^3 + bx$ is an $\mathbb{F}_3$-linear endomorphism of V. The order of $\operatorname{End}(V)$ being equal to the order of V^2, it follows that each element ψ of $\operatorname{End}(V)$ is of the form $x \mapsto ax^3 + bx$, where $a, b \in V$ are uniquely determined by ψ. In particular, this holds for ϕ. □

Lemma 9.28. *Let $\lambda \in \Lambda$. Then there exist $a, b \in V$ such that, for each $x \in V$, one has $\lambda(x) = x^5 + ax^3 + bx$.*

Proof. Because of (A2), the difference of any two elements of Λ belongs to $\operatorname{End}(V)$, so, thanks to Lemma 9.19, we have $\lambda \in (x \mapsto x^5) + \operatorname{End}(V)$. It now follows from Lemma 9.27 that there exist $a, b \in V$ such that, for each $x \in V$, we have $\lambda(x) = x^5 + ax^3 + bx$. □

Lemma 9.29. *Let m be a positive integer and let q be a prime power. Then*

$$\sum_{x \in \mathbb{F}_q} x^m = \begin{cases} -1 & \textit{when } \ (q-1)|m \\ 0 & \textit{otherwise} \end{cases}$$

Proof. This is Lemma 2.5.1 from [**Coh07**]. □

Lemma 9.30. *Let $\lambda \in \Lambda$. Then there exists $b \in V$ such that, for each $x \in V$, one has $\lambda(x) = x^5 + bx$.*

Proof. Let $a, b \in V$ be as in Lemma 9.28. By definition of Λ, the map λ is bijective so each element of V belongs to the image of λ. With x replaced by $\lambda(x)$, Lemma 9.29 yields

$$0 = \sum_{x \in V} \lambda(x)^2 = \sum_{x \in V} (x^5 + ax^3 + bx)^2 = \sum_{x \in V} 2ax^8 = -2a.$$

It follows that $a = 0$ and therefore, for each $x \in V$, one has $\lambda(x) = x^5 + bx$. □

Lemma 9.31. *The cardinality of Λ is at most 3.*

Proof. Let $\lambda \in \Lambda$ and let $b \in V$ be as in Lemma 9.30. The map λ is bijective and so, with x replaced by $\lambda(x)$, Lemma 9.29 gives

$$0 = \sum_{x \in V} \lambda(x)^4 = \sum_{x \in V} (x^5 + bx)^4 = \sum_{x \in V} (bx^{16} + b^3x^8) = -b(1 + b^2).$$

It follows that there are at most 3 choices for b in V and thus Λ has cardinality at most 3. □

We conclude Section 9.3 by giving the proof of Proposition 9.18. The function $s_V : \mathcal{I}_V \to \mathcal{K}_V$ is injective by Lemma 9.26 and, by Lemma 9.22, the cardinality of $\mathcal{I}_V$ is equal to 3. It follows that $\mathcal{K}_V$ has at least 3 elements. Now, as a consequence of Lemma 9.24, the set Λ has the same cardinality as $\mathcal{K}_V$ and thus, as a consequence of Lemma 9.31, the cardinality of $\mathcal{K}_V$ is equal to 3. From its injectivity, it now follows that s_V is bijective. The proof of Proposition 9.18 is complete.

9.4. Structures and free groups

We recall that a κ-group is a finite 3-group G such that $|G : G_2| = 9$ and such that the cubing map on G induces a bijection $G/G_2 \to G_3/G_4$. In particular, each κ-group is 2-generated. In the present section, we consider κ-groups of class 3 and we prove the following main result.

Proposition 9.32. *Let G be a finite 3-group of class 3. Then G is a κ-group if and only if G is isomorphic to* $\mathrm{MC}(3) \,/\, \mathrm{MC}(3)_4$.

Our strategy, for proving Proposition 9.32, will be that of constructing all κ-groups of class 3 as quotients of a free group. To this end, the following assumptions will be valid until the end of Section 9.4. Let F be the free group on two generators and let $(F_i)_{i\geq 1}$ denote the lower 3-series of F, which we recall from Section 5.3 to be defined by

$$F_1 = F \quad \text{and} \quad F_{i+1} = [F, F_i]F_i^3.$$

We remark that the notation we use for the lower 3-series is not concordant with our usual notation (see Exceptions in List of Symbols). We denote

$$V = F/F_2, \; L = F_3F^3, \quad \text{and} \quad E = [F, L]F_2^3.$$

The group V is a vector space of dimension 2 over $\mathbb{F}_3$, so we let $\mathcal{K}_V$ be defined as in Section 9.3. We write moreover $\overline{F} = F/E$ and we use the bar notation for the subsets of $\overline{F}$. We define additionally $\mathcal{N}_3$ to be the collection of normal subgroups N of F with the property that F/N is a κ-group of class 3.

Lemma 9.33. *The map $c_3 : F \to L/F_3$, defined by $x \mapsto x^3F_3$, is surjective. Moreover, c_3 induces an isomorphism $V \to L/F_3$ and $|L : F_3| = 9$.*

Proof. As a consequence of the Hall-Petrescu formula, the map c_3 is a surjective homomorphism, which, F_2^3 being contained in F_3, factors as a surjective homomorphism $c_2 : V \to L/F_3$. Since V has order 9, the order of L/F_3 is at most 9. Let now $A = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and let $\psi : F \to A$ be a surjective homomorphism. Then F_3 is contained in $\ker\psi$ and, since $L = F^3F_3$, the group $\psi(L)$ is equal to $3\mathbb{Z}/9\mathbb{Z} \times 3\mathbb{Z}/9\mathbb{Z}$, which has order 9. As a consequence, $|L : F_3| = 9$ and c_2 is an isomorphism. □

Lemma 9.34. *The commutator map $F \times F_2 \to F_3$ induces an isomorphism $\delta : F/F_2 \otimes F_2/L \to \overline{F_3}$. Moreover, $|F_3 : E| = 9$.*

Proof. The subgroup $\overline{F_3}$ is central in $\overline{F}$ and so the commutator map $F \times F_2 \to \overline{F_3}$ is bilinear. Moreover, thanks to Lemma 5.27, the quotient F_2/L is cyclic of order 3 and so $[F_2, F_2] = [F_2, L]$. The commutator map induces thus a surjective homomorphism $\delta : F/F_2 \otimes F_2/L \to \overline{F_3}$ and therefore $|F_3 : E| \leq 9$. We now claim that $|F_3 : E| \geq 9$. Thanks to Lemma 9.15, the abelianization of MC(3) has order 9 and thus MC(3) is 2-generated. Let $\phi : F \to \mathrm{MC}(3)$ be a surjective homomorphism and denote by π the natural projection $\mathrm{MC}(3) \to \mathrm{MC}(3) \,/\, \mathrm{MC}(3)_4$. Lemma 5.27 yields $L = (\pi \circ \phi)^{-1}(\mathrm{MC}(3)_3 \,/\, \mathrm{MC}(3)_4)$ and thus, as a consequence, we have $\phi(L) = \mathrm{MC}(3)_3$. Moreover, thanks to Lemma 5.13, the subgroup $\mathrm{MC}(3)_2^3$ is contained in $\mathrm{MC}(3)_4$ and therefore $\phi(F_2^3) \subseteq \mathrm{MC}(3)_4$. It follows that $\phi(F_3) = \mathrm{MC}(3)_3$ and also that $\phi(E) = \mathrm{MC}(3)_4$. Lemma 9.15(1) yields $|F_3 : E| \geq |\,\mathrm{MC}(3)_3 : \mathrm{MC}(3)_4\,| = 9$. This proves the claim and therefore $|F_3 : E| = 9$ and δ is an isomorphism. □

$$\begin{tikzcd}
\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z} \arrow[d, dash, "9"'] & & F \arrow[ll, dashed] \arrow[r, dashed] \arrow[d, dash, "9"'] & \mathrm{MC}(3) \arrow[d, dash, "9"] \\
3\mathbb{Z}/9\mathbb{Z}\times 3\mathbb{Z}/9\mathbb{Z} \arrow[d, dash, "9"'] & & F_2 \arrow[r, dashed] \arrow[d, dash, "3"'] & \mathrm{MC}(3)_2 \arrow[d, dash, "3"] \\
0 & & L = F_3F^3 \arrow[ull, dashed] \arrow[r, dashed] \arrow[dl, dash, "9"'] & \mathrm{MC}(3)_3 \arrow[d, dash, "9"] \\
& F_3 \arrow[ul, dashed] \arrow[urr, dashed] \arrow[dr, dash, "9"'] & & \mathrm{MC}(3)_4 \\
& & E = [F,L]F_2^3 \arrow[ur, dashed] &
\end{tikzcd}$$

LEMMA 9.35. *The group $\overline{L}$ is an $\mathbb{F}_3$-vector space of dimension* 4.

PROOF. The group $\overline{L}$ is central in $\overline{F}$ and so it is abelian. Moreover L^3 is contained in E. It follows that $\overline{L}$ is naturally a vector space over $\mathbb{F}_3$, which has dimension 4, thanks to Lemmas 9.33 and 9.34. □

LEMMA 9.36. *The commutator map $F \times F_2 \to F_3$ induces an isomorphism $\gamma : V \otimes \bigwedge^2 V \to \overline{F_3}$.*

PROOF. The subgroup F_2 is central modulo L so the commutator map $F \times F \to F_2/L$ is bilinear. Since $[F, F_2]$ is contained in L, we get a bilinear map $V \times V \to F_2/L$, which is also alternating. By the universal property of wedge products, the last map factors as a homomorphism $\theta : \bigwedge^2 V \to F_2/L$ mapping $x \wedge y$ to $[x, y]$. By Lemma 5.27, the cardinality of F_2/L is equal to 3, which is the same as the cardinality of $\bigwedge^2 V$ and so, being non-trivial, θ is an isomorphism of groups. We conclude by defining $\gamma = \delta \circ (1 \otimes \theta)$, where δ is as in Lemma 9.34. □

LEMMA 9.37. *Let γ be as in Lemma* 9.36 *and use the additive notation for the vector spaces V and $\overline{L}$. Then the cubing map on $\overline{F}$ induces a map $c : V \to \overline{L}$ such that, for each $x, y \in V$, one has*

$$c(x + y) = c(x) + c(y) + \gamma((x - y) \otimes (x \wedge y)).$$

PROOF. The group $\overline{F}$ has class at most 3 and $[\overline{F}, \overline{F}]$ has exponent dividing 3. By Lemma 9.7, given any two elements x, y of $\overline{F}$, one has $(xy)^3 = x^3y^3[xy^{-1}, [x, y]]$.

Since both F_2^3 and $[F,[F,F_2]]$ are contained in E, cubing on $\overline{F}$ induces a map $c : V \to \overline{L}$. Using the additive notation for V and $\overline{L}$, it follows that, for each $x, y \in V$, one has $c(x+y) = c(x) + c(y) + \gamma((x-y) \otimes (x \wedge y))$. □

Lemma 9.38. *Let $0 \to A \xrightarrow{\iota} B \xrightarrow{\sigma} C \to 0$ be a short exact sequence of abelian groups. Let moreover $s : C \to B$ be a function such that $\sigma \circ s = \mathrm{id}_C$. Write $\mathcal{R} = \{f \in \mathrm{Hom}(B,A) : f \circ \iota = \mathrm{id}_A\}$ and let $\mathcal{H}$ be the collection of maps $g : C \to A$ such that, for all $u, v \in C$, one has*

$$\iota(g(u+v) - g(u) - g(v)) = s(u+v) - s(u) - s(v).$$

Then the function $\mathcal{R} \to \mathcal{H}$ that is defined by $f \mapsto f \circ s$ is bijective.

Proof. Let $\nu : \mathcal{R} \to \mathcal{H}$ be defined by $f \mapsto f \circ s$. We first prove that ν is well-defined. To this end, let $f \in \mathcal{R}$ and let $u, v \in C$. Since $\sigma \circ s = \mathrm{id}_C$, the element $s(u+v) - s(u) - s(v)$ belongs to $\ker \sigma = \iota(A)$. Since $f \circ \iota = \mathrm{id}_A$, we get that $\iota \circ f_{|\iota(A)} = \mathrm{id}_{|\iota(A)}$ and therefore

$$\iota((f \circ s)(u+v) - (f \circ s)(u) - (f \circ s)(v)) = s(u+v) - s(u) - s(v).$$

We have proven that ν is well-defined. We now prove that ν is injective. Let $f, h \in \mathcal{R}$ be such that $\nu(f) = \nu(h)$. Since $f \circ \iota = h \circ \iota = \mathrm{id}_A$, the group $\iota(A)$ is contained in $\ker(f-h)$ and thus $f-h$ induces a homomorphism $B/\iota(A) \to A$. Now, $B/\iota(A) = \{s(c) + \iota(A) : c \in C\}$ and, the maps $f \circ s$ and $h \circ s$ being the same, we get $f - h = 0$. The maps f and g are the same and ν is injective. To conclude, we prove that ν is surjective. Let $g \in \mathcal{H}$. Since each element x of B can be written uniquely as $x = \iota(a) + s(u)$, with $a \in A$ and $u \in C$, we define $f : B \to A$ by

$$x = \iota(a) + s(u) \mapsto f(x) = a + g(u).$$

For each $u \in C$, we have then $f \circ s(u) = g(u)$. Relying on the facts that $g \in \mathcal{H}$ and that $g(C)$ is contained in A, one shows that f is a homomorphism and so ν is surjective. □

Proposition 9.39. *Let c be as in Lemma 9.37 and let γ be as in Lemma 9.36. Set*

$$\mathcal{P} = \{\pi \in \mathrm{Hom}(\overline{L}, \overline{F_3}) : \pi_{|\bar{F}_3} = \mathrm{id}_{\bar{F}_3}, \pi \circ c \textit{ bijective}\}$$

and let $t_V : \mathcal{P} \to \mathcal{K}_V$ be defined by $\pi \mapsto \gamma^{-1} \circ \pi \circ c$. Then t_V is a bijection and $\mathcal{P}$ has cardinality 3.

Proof. Let $c_2 : V \to L/F_3$ be the isomorphism from Lemma 9.33. Composing the canonical projection $\overline{L} \to L/F_3$ with c_2^{-1}, we get the short exact sequence of abelian groups $0 \to \overline{F_3} \to \overline{L} \to V \to 0$. With $A = \overline{F_3}$, $B = \overline{L}$, $C = V$, and $s = c$, Lemma 9.38 applies. Let thus $\mathcal{R} = \{\pi \in \mathrm{Hom}(\overline{L}, \overline{F_3}) : \pi_{|\bar{F}_3} = \mathrm{id}_{\bar{F}_3}\}$ and let $\mathcal{H}$ be the collection of maps $g : V \to \overline{F_3}$ such that, for all $x, y \in V$, one has

$$g(x+y) - g(x) - g(y) = c(x+y) - c(x) - c(y).$$

Then, thanks to Lemma 9.38, each element of $\mathcal{H}$ is of the form $\pi \circ c$, where π belongs to $\mathcal{R}$. In particular, the subset $\mathcal{P}$ of $\mathcal{R}$ is sent bijectively to the subset $\mathcal{H}_{\mathrm{bij}}$ of bijective elements of $\mathcal{H}$. Now, by Lemma 9.37, given any two elements $x, y \in V$, we have $c(x+y) - c(x) - c(y) = \gamma((x-y) \otimes (x \wedge y))$ and therefore each element $\kappa = \gamma^{-1} \circ \pi \circ c$, with $\pi \in \mathcal{P}$, belongs to $\mathcal{K}_V$. The map γ being an isomorphism, t_V is injective. Moreover, since γ is bijective, Lemma 9.37 yields a well-defined injection $\mathcal{K}_V \to \mathcal{H}_{\mathrm{bij}}$, given by $\kappa \mapsto \gamma \circ \kappa$. It follows that $|\mathcal{P}| \leq |\mathcal{K}_V| \leq |\mathcal{H}_{\mathrm{bij}}| = |\mathcal{P}|$

and therefore t_V is a bijection. Thanks to Proposition 9.18, the cardinality of $\mathcal{P}$ is 3. □

We remind the reader that $\mathcal{N}_3$ has been defined to be the collection of normal subgroups N of F such that F/N is a κ-group of class 3.

Lemma 9.40. *Let $\mathcal{P}$ be as in Proposition 9.39 and denote, for each $\pi \in \mathcal{P}$, by K_π the unique normal subgroup of F containing E such that $\overline{K_\pi} = \ker \pi$. Then the map $r : \mathcal{P} \to \mathcal{N}_3$ that is defined by $\pi \mapsto K_\pi$ is a bijection. Moreover, for each $N \in \mathcal{N}_3$, one has $|L : N| = 9$.*

Proof. We first show that r is well-defined. To this end, let π be an element of $\mathcal{P}$ and set $G = F/K_\pi$. Then G_2 is equal to F_2/K_π. Moreover, $\overline{L}$ decomposes as $\ker \pi \oplus \overline{F_3} = \overline{K_\pi} \oplus \overline{F_3}$. In particular, L/K_π and $\overline{F_3}$ are naturally isomorphic and so, as a consequence of Lemma 9.34, the subgroup G_3 coincides with L/K_π. It follows that G has class 3. Now, the map $\pi \circ c$ being bijective, the cubing map induces a bijection $F/F_2 \to \overline{F_3}$ and so, via the natural isomorphism $\overline{F_3} \to L/K_\pi$, the cubing map induces a bijection $G/G_2 \to G_3$. As a result, $|L : K_\pi| = |G_3| = |G : G_2| = |F : F_2| = 9$ and G is a κ-group. The choice of π being arbitrary, r is well-defined. It is now easy to show that r is bijective. From the surjectivity of r one deduces that, for all $N \in \mathcal{N}_3$, the index $|L : N|$ is equal to 9. □

Proposition 9.41. *The set $\mathcal{N}_3$ has cardinality 3 and the natural action of $\mathrm{Aut}(F)$ on $\mathcal{N}_3$ is transitive.*

Proof. Let $\mathcal{I}_V$ be defined as in Section 9.3. Define moreover $\psi : \mathcal{I}_V \to \mathcal{N}_3$ to be $\psi = r \circ t_V^{-1} \circ s_V$, where s_V, t_V, and r are as in Propositions 9.18 and 9.39 and Lemma 9.40. The combination of the just-mentioned results yields that ψ is a bijection and, from its definition, it is easy to check that it respects the action of $\mathrm{Aut}(F)$. Now, by Lemma 9.22, the set $\mathcal{I}_V$ has cardinality 3 and so $\mathcal{N}_3$ has cardinality 3. Again by Lemma 9.22, the action of $\mathrm{Aut}(V)$ on $\mathcal{I}_V$ is transitive and so the action of $\mathrm{Aut}(F)$ on $\mathcal{I}_V$ is transitive. Being ψ an isomorphism of $\mathrm{Aut}(F)$-sets, $\mathrm{Aut}(F)$ acts transitively on $\mathcal{N}_3$. □

We are finally ready to give the proof of Proposition 9.32, which is the same as Theorem 9.3. To this end, let G be a finite 3-group of class 3. The group $\mathrm{MC}(3)$ has class 4, by Lemma 9.14, and it is a κ-group, by Lemma 9.16. There exists thus a normal subgroup M of F such that F/M is isomorphic to $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$. Fix such M. The group G is a κ-group if and only if there exists $N \in \mathcal{N}_3$ such that F/N is isomorphic to G. Proposition 9.41 yields that G is a κ-group if and only if it is isomorphic to $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$. The choice of G being arbitrary, Proposition 9.32, and thus Theorem 9.3, is proven.

9.5. Extensions

We recall here that a κ-group is a finite 3-group G such that $|G : G_2| = 9$ and such that cubing in G induces a bijection $G/G_2 \to G_3/G_4$. We remind the reader that we investigate κ-groups because we aim at classifying 3-groups of class at least 4 and intensity greater than 1: those groups are all κ-groups, as a consequence of Lemma 9.9. The main purpose of the present section is that of proving the following proposition, which is the same as Theorem 9.4.

Proposition 9.42. *Let G be a κ-group such that G_4 has order 3. Then G_2 is elementary abelian.*

Until the end of Section 9.5, we will work under the assumptions of Proposition 9.42. Then G_2 is abelian and, if for each $i \in \mathbb{Z}_{\geq 1}$ we set $w_i = \mathrm{wt}_G(i)$, then $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. Moreover, the group G/G_4 being a κ-group of class 3, Theorem 9.3 yields that G/G_4 is isomorphic to $\mathrm{MC}(3) \,/\, \mathrm{MC}(3)_4$. It follows from Lemma 9.15(2) that there exist generators a, b of G such that, if we define

$$c = [a, b], d = [a, c], e = [b, c], \quad \text{and} \quad f = [a, d]$$

then the following are satified:

i. one has $a^3 \equiv [b, [a, b]]^{-1} \bmod G_4$ and $b^3 \equiv [a, [a, b]] \bmod G_4$; and
ii. the elements d and e generate G_3 modulo G_4; and
iii. one has $a^3 \equiv e^{-1} \bmod G_4$ and $b^3 \equiv d \bmod G_4$.

Lemma 9.43. *One has $G_4 = \langle f \rangle = \langle [b, e] \rangle$.*

Proof. By Lemma 9.11, the centre of G is equal to G_4 and, by Lemma 7.3, the commutator map $G/G_2 \times G_3/G_4 \to G_4$ is non-degenerate. The elements d and e generate G_3 modulo G_4 and we also have $a^3 \equiv e^{-1} \bmod G_4$ and $b^3 \equiv d \bmod G_4$. From the non-degeneracy of the commutator map, it follows that both f and $[b, e]$ are non-trivial elements of G_4, which, being cyclic of order 3, then satisfies $G_4 = \langle f \rangle = \langle [b, e] \rangle$. □

Lemma 9.44. *There exists a pair (u, t) in $\{\pm 1\} \times \mathbb{Z}$ such that $[b, e] = f^u$ and $c^3 = f^t$. Moreover, there exist $r, s \in \mathbb{Z}$ such that $a^3 = e^{-1} f^r$ and $b^3 = d f^s$.*

Proof. By assumption, the order of G_4 is 3 and, by Lemma 9.43, both elements f and $[b, e]$ generate G_4. There exists thus $u \in \{\pm 1\}$ such that $[b, e] = f^u$. Moreover, since $a^3 \equiv e^{-1} \bmod G_4$ and $b^3 \equiv d \bmod G_4$, there exist integers r and s such that $a^3 = e^{-1} f^r$ and $b^3 = d f^s$. To conclude, thanks to Lemma 5.13, the subgroup G_2^3 is contained in G_4 so there exists $t \in \mathbb{Z}$ such that $c^3 = f^t$. □

We are now ready to give the proof of Proposition 9.42. To this end, let u, t, r, s be as in Lemma 9.44. The subgroup G_2 is abelian and, by Lemma 9.13, the exponent of G_3 is equal to 3. It follows that $ab^3 = f^{u+t} b^3 a$, from which we derive $f da f^s = f^{u+t} d f^s a$. The subgroup G_4 is central, thanks to Lemma 9.11, and so one gets

$$f da = f^{u+t} da.$$

Since the exponent of G_3 is equal to 3, we have $u + t \equiv 1 \bmod 3$ and so

$$(u, t) \equiv (1, 0) \bmod 3 \quad \text{or} \quad (u, t) \equiv (-1, -1) \bmod 3.$$

If $(u, t) \equiv (1, 0) \bmod 3$, then we are done. We assume by contradiction that $(u, t) \equiv (-1, -1) \bmod 3$. Then $c^3 = f^{-1}$, from which it follows that $a^3 b = b a^3$ and so a^3 centralizes b in G. Call $C = \langle \{b\} \cup G_2 \rangle$. Then a^3 belongs to $\mathrm{Z}(C)$, which then, thanks to Lemma 9.10, contains $\{a^3, b^3\} \cup G_4$. The group G being a κ-group, it follows that $\mathrm{Z}(C)$ contains G_3, and so $[b, e] = 1$. Contradiction to Lemma 9.43. The proof of Proposition 9.42, and thus that of Theorem 9.4, is now complete.

The subgroup $\mathrm{MC}(3)_2$ of $\mathrm{MC}(3)$ is elementary abelian.

Proof. The group $\mathrm{MC}(3)$ is a κ-group by Lemma 9.16 and, thanks to Lemma 9.15(1), the subgroup $\mathrm{MC}(3)_4$ has order 3. It follows from Proposition 9.42 that $\mathrm{MC}(3)_2$ is elementary abelian. □

Let Q be a finite 3-group with $\mathrm{int}(Q) > 1$. Then Q has nilpotency class at most 4.

Proof. Assume that Q has class at least 4. Thanks to Lemma 3.13, the intensity of Q/Q_5 is greater than 1, and , thanks to Lemma 9.9, the group Q/Q_5 is a κ-group. Moreover, thanks to Theorem 6.1, the quotient Q_4/Q_5 has order 3 and thus Proposition 9.42 yields that Q_2^3 is contained in Q_5. However, because of Proposition 7.13, each finite 3-group H of class at least 5 with $\mathrm{int}(H) > 1$ satisfies $H_2^3 = H_4$ and so it follows that Q has class at most 4. □

9.6. Constructing automorphisms

In this section we aim at understanding the structure of finite 3-groups of class 4 and intensity greater than 1. We recall that a κ-group is a finite 3-group G such that $|G : G_2| = 9$ and the cubing map on G induces a bijection $G/G_2 \to G_3/G_4$ (see Section 9.1 for a closer look at κ-groups). The reason why κ-groups are so special for us is Lemma 9.9, which asserts that any finite 3-group of class 4 and intensity greater than 1 is a κ-group. Moreover, we know from Proposition 5.10, that if we hope to construct a 3-group G of large class and intensity greater than 1, then we need as well to construct an automorphism of order 2 of G that induces the inversion map on the abelianization of G. We will devote the present section to the proof of the following result.

Proposition 9.45. *Let G be a κ-group such that G_4 has order* 3. *Assume that G possesses an automorphism of order* 2 *that induces the inversion map on G/G_2. Then G is isomorphic to* MC(3).

We will prove Proposition 9.45 at the end of the present section and so the following assumptions will hold until the end of Section 9.6. Let G be a κ-group such that G_4 has order 3. Then the group G has class 4 and $(\mathrm{wt}_G(i))_{i=1}^4 = (2, 1, 2, 1)$. Let F be the free group on the set $S = \{a, b\}$ and let $\iota : S \to G$ be such that $G = \langle \iota(S) \rangle$. By the universal property of free groups, there exists a unique homomorphism $\phi : F \to G$ such that $\phi(a) = \iota(a)$ and $\phi(b) = \iota(b)$. As a consequence of its definition, the map ϕ is surjective. Let $(F_i)_{i\geq 1}$ denote the lower 3-series of F, which is defined recursively as

$$F_1 = F \quad\text{and}\quad F_{i+1} = [F, F_i]F_i^3.$$

and, in addition, let

$$L = F^3F_3 \quad\text{and}\quad E = [F, L]F_2^3.$$

All F_i's, L, and E are stabilized by any endomorphism of F. For a visualization of such groups we refer to the end of Section 5.3 or to the diagram appearing later in this section. Let β be the endomorphism of F sending a to a^{-1} and b to b^{-1}. Since $\beta^2 = \mathrm{id}_F$, the map β is an automorphism of F. We remind the reader that we have already worked with such an automorphism β in Section 5.3 and we will thus, in this section, often apply results achieved in Section 5.3. We conclude by defining two specific sets, consisting of normal subgroups of F. Let $\mathcal{N}_3$ denote the collection of normal subgroups N of F such that F/N is a κ-group of class 3, as defined in Section 9.4. For each element N of $\mathcal{N}_3$, we set

$$D_N = [F, N]F_2^3[F_2, F_2].$$

It is not difficult to show that each such D_N is contained in E. We define moreover $\mathcal{N}_4$ to be the collection of normal subgroups M of F such that F/M is a κ-group of class 4 with $\mathrm{wt}_{F/M}(4) = 1$ and such that F/M possesses an automorphism of order 2 that induces the inversion map on the abelianization $(F/M)/(F/M)_2$ of F/M. We will keep this notation until the end of Section 9.6.

Lemma 9.46. *For each $k \in \mathbb{Z}_{\geq 5}$, one has $\phi(F_k) = \{1\}$.*

Proof. Let $k \in \mathbb{Z}_{\geq 5}$ and recall that $F_k = [F, F_{k-1}]F_{k-1}^3$. By definition of E, one has that $\phi([F, F_{k-1}])$ is contained in $[\phi(F), \phi(E)]$ and so, as a consequence of Lemma 5.28, we get $\phi([F, F_{k-1}]) = \{1\}$. It follows that $\phi(F_k) = \phi(F_{k-1}^3) \subseteq \phi(F_2^3) \subseteq G_2^3$ and so Proposition 9.42 yields $\phi(F_k) = \{1\}$. □

Lemma 9.47. *Let α be an automorphism of order 2 of G that induces the inversion map on G/G_2. Then there exist generators x and y of G such that $\alpha(x) = x^{-1}$ and $\alpha(y) = y^{-1}$.*

Proof. Write $G^- = \{g \in G : \alpha(g) = g^{-1}\}$. Since $(\mathrm{wt}_G(i))_{i=1}^4 = (2, 1, 2, 1)$, Lemma 2.17 yields that the map $G^- \to G/G_2$, defined by $g \mapsto gG_2$, is surjective. Since $G_2 = \Phi(G)$, there exist two elements x and y of G^- that generate G. □

Proposition 9.48. *Let α be an automorphism of order 2 of G that induces the inversion map on G/G_2. Let moreover $k \in \mathbb{Z}_{\geq 5}$ and let $\phi_k : F/F_k \to G$ be the map induced by ϕ. Then there exists $\epsilon \in \mathrm{Aut}(F/F_k)$ of order 2 such that $\alpha\phi_k = \phi_k\epsilon$.*

Proof. For each $k \in \mathbb{Z}_{\geq 5}$, the map $\phi_k : F/F_k \to G$ is well-defined, thanks to Lemma 9.46. Let now x and y be as in Lemma 9.47 and let c and d be elements of F such that $\phi(c) = x$ and $\phi(d) = y$. As a consequence of Lemma 5.26, the map ϕ induces an isomorphism $F/F_2 \to G/G_2$ and therefore c and d generate F modulo F_2. Let now $\psi : F \to F$ be the endomorphism of F sending $a \mapsto c$ and $b \mapsto d$. Fix $k \in \mathbb{Z}_{\geq 5}$. The subgroup F_k being being stabilized by any endomorphism of F, the map ψ induces an endomorphism $\overline{\psi}$ of the 3-group $\overline{F} = F/F_k$. However, since $\Phi(\overline{F}) = \overline{F_2}$, the map $\overline{\psi}$ induces an automorphism of $\overline{F}/\Phi(\overline{F})$ and so $\overline{\psi}$ is in fact an automorphism of $\overline{F}$. Let $\overline{\beta}$ be the automorphism of $\overline{F}$ that is induced by β and define $\epsilon = \overline{\psi\beta\psi^{-1}}$. By construction, the following diagram is commutative.

$$\begin{tikzcd}
F/F_k \arrow[r, "\phi_k"] \arrow[d, "\epsilon"] & G \arrow[d, "\alpha"'] \\
F/F_k \arrow[r, "\phi_k"] & G
\end{tikzcd}$$

Moreover, ϵ has order 2, because it is conjugate in $\mathrm{Aut}(\overline{F})$ to $\overline{\beta}$. □

Lemma 9.49. *Let M be an element of $\mathcal{N}_4$. Then $N = ME$ belongs to $\mathcal{N}_3$ and $D_N \subseteq M$.*

Proof. Let $H = F/M$ and let $\pi : F \to H$ be the canonical projection. Then $\pi(N) = \pi(ME) = \pi(E)$ and so, as a consequence of Lemma 5.28, we have $\pi(N) \subseteq H_4$. The order of H_4 being 3, either $\pi(N) = H_4$ or $N \subseteq M$. Assume first that $\pi(N) = H_4$. Then we have $M \subseteq N \subseteq \pi^{-1}(H_4)$ and $M \neq N$. Further, we also know $|\pi^{-1}(H_4) : M| = |H_4| = 3$ and therefore $N = \pi^{-1}(H_4)$. As a result, F/N is isomorphic to H/H_4 and so N belongs to $\mathcal{N}_3$. From the combination of Lemma 5.26 and Proposition 9.42, we now derive $\pi(D_N) = \{1\}$ and so D_N is contained in

M. We conclude by proving that $\pi(N) = H_4$. Indeed, if by contradiction we had $N \subseteq M$, the subgroup E would be contained in M making F/E of class at least 4. This would however contradict the fact that $[F, [F, [F, F]]] \subseteq E$. □

Lemma 9.50. *Let $N \in \mathcal{N}_3$ and write $H = \mathrm{MC}(3)$. Then there exists a surjective homomorphism $\varphi : F \to G$ such that $N = \varphi^{-1}(G_4)$. Moreover, φ induces isomorphisms $\varphi_1 : F/F_2 \to H/H_2$ and $\varphi_3 : L/N \to H_3/H_4$ and a surjective homomorphism $\varphi_4 : E/D_N \to H_4$.*

Proof. Let $\psi : F \to H$ be a surjective homomorphism and $K = \psi^{-1}(H_4)$. Then K belongs to $\mathcal{N}_3$ and so, thanks to Proposition 9.41, there exists an automorphism r of F such that $r(N) = K$. Define $\varphi = \psi \circ r$. Then φ is a surjective homomorphism $F \to H$ such that $\varphi^{-1}(H_4) = N$. Moreover, φ induces isomorphisms $\varphi_1 : F/F_2 \to H/H_2$ and $\varphi_3 : L/N \to H_3/H_4$ as a consequence of Lemmas 5.26 and 5.27. We conclude by showing that φ induces a surjective homomorphism $E/D_N \to H_4$. Thanks to Lemma 9.49, the subgroup D_N is contained in the kernel of φ. Moreover, since $\varphi(F_2) = H_2$ and $\varphi(L) = H_3$, we get $\varphi(E) = H_4 H_2^3$. Now, the group H is a κ-group and hence $H_2^3 \subseteq H_4$. It follows that $\varphi(E) = H_4$ and therefore φ induces a surjective homomorphism $E/D_N \to H_4$. □

Lemma 9.51. *Let $N \in \mathcal{N}_3$. Then the commutator map $F \times L \to E$ induces a non-degenerate bilinear map $F/F_2 \times L/N \to E/D_N$ whose image generates E/D_N. In addition, one has $E \neq D_N$.*

Proof. Write $\overline{F} = F/D_N$ and use the bar notation for the subgroups of $\overline{F}$. From the definition of E, one sees that $\overline{E} = [\overline{F}, \overline{L}]$. Moreover, by Lemma 5.28, the subgroup E is contained in N and so $[F, E] \subseteq D_N$. In particular, $\overline{E}$ is central in $\overline{F}$ and so the commutator map $F \times L \to \overline{E}$ is bilinear. Since $[F_2, L]$ and $[F, N]$ are both contained in D_N, the last map factors as a bilinear map $\gamma : F/F_2 \times L/N \to \overline{E}$ whose image generates $\overline{E}$. Set $H = \mathrm{MC}(3)$. As a consequence of Lemmas 9.16 and 9.11, the centre of H is equal to H_4 and thus Lemma 7.3 yields that the commutator map induces a non-degenerate map $\nu : H/H_2 \times H_3/H_4 \to H_4$. With the notation from Lemma 9.50, the following diagram is commutative.

$$\begin{tikzcd}
F/F_2 \times L/N \arrow[r, "\gamma"] \arrow[d, shift right, "\varphi_1"'] \arrow[d, shift left, "\varphi_3"] & E/D_N \arrow[d, "\varphi_4"'] \\
H/H_2 \times H_3/H_4 \arrow[r, "\nu"] & H_4
\end{tikzcd}$$

Since the map ν is non-degenerate and both φ_1 and φ_3 are isomorphisms, the map γ is non-degenerate. It follows in particular that $E \neq D_N$. □

Lemma 9.52. *Let V and W be 2-dimensional vector spaces over $\mathbb{F}_3$ and let $\eta : V \to W$ be a bijective map such that, for each $\lambda \in \mathbb{F}_3$ and $v \in V$, one has $\eta(\lambda v) = \lambda \eta(v)$. Define $K = \langle v \otimes \eta(v) : v \in V \rangle$. Then the quotient $(V \otimes W)/K$ has dimension 1 as a vector space over $\mathbb{F}_3$.*

Proof. Without loss of generality we assume that $V = W$. Assume first that η is an automorphism of V and define the automorphism σ of $V \otimes V$ by $x \otimes y \mapsto x \otimes \eta(y)$. Then the subspace $\Delta = \langle v \otimes v : v \in V \rangle$ is mapped isomorphically to K via σ and so $(V \otimes V)/K$ has the same dimension as $(V \otimes V)/\Delta = \bigwedge^2 V$. In particular, $(V \otimes V)/K$ has dimension 1. Let now η be any map satisfying the hypotheses of Lemma 9.52. Then η induces a bijective map $\overline{\eta} : \mathbb{P}V \to \mathbb{P}V$, where $\mathbb{P}V$ denotes the collection of 1-dimensional subspaces of V. As a consequence of Lemma 9.21, there exists an automorphism τ of V such that $\overline{\tau} = \overline{\eta}$ and, for each $v \in V$, one has $\mathbb{F}_3\tau(v) = \mathbb{F}_3\eta(v)$. As a consequence, we get $K = \langle v \otimes \tau(v) : v \in V\rangle$ and therefore $(V \otimes V)/K$ has dimension 1 over $\mathbb{F}_3$. □

Lemma 9.53. *Let $N \in \mathcal{N}_3$. Then $|E : D_N| = 3$.*

Proof. The quotient F/F_2 is a 2-dimensional vector space over $\mathbb{F}_3$, while L/E is a 4-dimensional vector space over $\mathbb{F}_3$, thanks to Lemma 9.35. Moreover, by Lemma 5.28, the subgroup N contains E and, as a consequence of Lemma 9.40, the quotient L/N is a vector space of dimension 2 over $\mathbb{F}_3$. Let $\gamma : F/F_2 \otimes L/N \to E/D_N$ be the surjective homomorphism induced from the non-degenerate map of Lemma 9.51. Let moreover $c : F/F_2 \to L/E$ be the map from Lemma 9.37 and let π denote the canonical projection $L/E \to L/N$. Denote $c_N = \pi \circ c$ and note that, as a consequence of Lemma 9.40, the map $c_N : F/F_2 \to L/N$ is a bijection between vector spaces of dimension 2 over $\mathbb{F}_3$. From Lemma 9.37, it is clear that c commutes with scalar multiplication by elements of $\mathbb{F}_3$. Define now $K = \langle x \otimes c_N(x) : x \in F/F_2\rangle$. As a consequence of the definition of c, each element $x \otimes c_N(x)$, with $x \in F/F_2$, belongs to the kernel of γ, and therefore K is contained in $\ker\gamma$. It follows from Lemma 9.52 that $(F/F_2 \otimes L/N)/K$ has dimension 1 and therefore E/D_N has dimension at most 1 as a vector space over $\mathbb{F}_3$. Lemma 9.51 yields that E/D_N has cardinality 3. □

Lemma 9.54. *Let T be a group and let S be a central subgroup of T. Let moreover Δ denote the subgroup of* $\mathrm{Aut}(T)$ *consisting of all those elements δ such that $\delta(S) = S$ and such that δ induces the identity on both S and T/S. Then the map $\Delta \to \mathrm{Hom}(T/S, S)$ that is defined by $\delta \mapsto (xS \mapsto \delta(x)x^{-1})$ is bijective.*

Proof. Let $\phi : \Delta \to \mathrm{Hom}(T/S, S)$ denote the map $\delta \mapsto (xS \mapsto \delta(x)x^{-1})$, which is well-defined because S is central in T. The map ϕ is clearly injective and it is surjective because, given each homomorphism $f \in \mathrm{Hom}(T, S)$ with $S \subseteq \ker(f)$, the map $x \mapsto xf(x)$ belongs to Δ. □

Lemma 9.55. *Let p be a prime number and let P be an extraspecial p-group. Let Δ denote the subgroup of* $\mathrm{Aut}(P)$ *consisting of those automorphisms of P that induce the identity on the abelianization P/P_2. Then $\Delta = \mathrm{Inn}(P)$.*

Proof. The subgroups $\mathrm{Z}(P)$ and P_2 being equal, the commutator map induces a bilinear non-degenerate map $P/P_2 \times P/P_2 \to P_2$ and so the homomorphism $P/P_2 \to \mathrm{Hom}(P/P_2, P_2)$ that is defined by $t \mapsto (x \mapsto [t, x])$ is injective. The quotient P/P_2 being elementary abelian, $P/P_2 \to \mathrm{Hom}(P/P_2, P_2)$ is an isomorphism. Now, by Lemma 2.5, each element δ of Δ restricts to the identity on P_2 and so we derive from Lemma 9.54 that, for each element $\delta \in \Delta$, there exists $t \in P$ such that, for all $x \in P$, one has $\delta(x) = [t, x]x = txt^{-1}$. In particular, Δ is contained in $\mathrm{Inn}(P)$. The inclusion $\mathrm{Inn}(P) \subseteq \Delta$ is clear and so the proof is complete. □

Lemma 9.56. *Let η be an automorphism of F/L of order* 2 *that induces the inversion map on F/F_2. Then there exists $\varphi_L \in \mathrm{Inn}(F/L)$ such that, for each $x \in F$, one has $\beta(x) \equiv (\varphi_L\eta\varphi_L^{-1})(x) \bmod L$.*

Proof. Write $H = F/L$. As a consequence of Lemma 5.27, the group H is extraspecial of order 27 and exponent 3. Let now β_L be the automorphism of H

that is induced by β. Then $\eta^{-1}\beta_L$ induces the identity on H/H_2 and so, thanks to Lemma 9.55, one gets $\eta^{-1}\beta_L \in \mathrm{Inn}(H)$. The group $\mathrm{Inn}(H)$ being a normal 3-subgroup of $\mathrm{Aut}(H)$, the Schur-Zassenhaus theorem applies to $\mathrm{Inn}(H)\langle\eta\rangle$ and ensures that there exists $\varphi_L \in \mathrm{Inn}(H)$ with the property that $\beta_L = \varphi_L\eta\varphi_L^{-1}$. □

LEMMA 9.57. *Let η be an automorphism of F/E of order 2 that induces the inversion map on F/F_2. Assume that β coincides with η modulo L. Then, for all $x \in F$, one has $\beta(x) \equiv \eta(x) \bmod E$.*

PROOF. Let Δ denote the subgroup of $\mathrm{Aut}(F/E)$ consisting of all those automorphisms of F/E inducing the identity on both F/L and L/E. Let β_E be the automorphism that is induced on F/E by β. As a consequence of Lemma 5.32, the element $\psi = \eta^{-1}\beta_E$ belongs to Δ and so, thanks to Lemma 9.54, there exists a homomorphism $h : F/L \to L/E$ such that, for all $x \in F/E$, one has $\psi(x) = h(x)x$. The quotient L/E being elementary abelian, the groups $\mathrm{Hom}(F/L, L/E)$ and $\mathrm{Hom}(F/F_2, L/E)$ are naturally isomorphic and so h factors as a homomorphism $F/F_2 \to L/E$. Now η coincides with β on F/F_2 and so, thanks to Lemma 5.32, it induces the inversion map on L/E. For each $x \in F/F_2$, it follows that $(\eta h\eta^{-1})(x) = h(x)$. However, the automorphisms η and β_E having order 2, one also has $\eta^2 = 1 = \beta_E^2 = \eta\psi\eta\psi$ and therefore $\eta\psi\eta^{-1} = \psi^{-1}$. For all $x \in F/E$, it follows then that $\psi(x)x^{-1} = \psi^{-1}(x)x^{-1}$ and therefore $\psi(x)^2 = 1$. The group F/E being a 3-group, the map ψ is trivial and therefore η and β_E are equal. □

LEMMA 9.58. *Let $N = \phi^{-1}(G_4)$ and let Δ denote the subgroup of* $\mathrm{Aut}(F/D_N)$ *consisting of all those maps inducing the identity on both F/E and E/D_N. Then Δ is contained in* $\mathrm{Inn}(F/D_N)$.

PROOF. The group N belongs to $\mathcal{N}_3$, because G/G_4 is a κ-group of class 3. As a consequence of Lemma 9.51, the commutator map induces an injective homomorphism $\varphi : L/N \to \mathrm{Hom}(F/F_2, E/D_N)$. Combining Lemmas 9.40 and 9.53, we get that the orders of $\mathrm{Hom}(F/F_2, E/D_N)$ and L/N are the same and therefore φ is also surjective. It follows that, for each element f of $\mathrm{Hom}(F/F_2, E/D_N)$, there exists $l \in L$ such that f equals $xF_2 \mapsto [l, x]D_N$. Set $\overline{F} = F/D_N$ and use the bar notation for the subgroups of $\overline{F}$. We now prove that Δ is contained in $\mathrm{Inn}(\overline{F})$. Let $\delta \in \Delta$. Then, as a consequence of Lemma 9.54, there exists a homomorphism $f : \overline{F} \to \overline{E}$ whose kernel contains $\overline{E}$ and such that, for each $x \in \overline{F}$, one has $\delta(x) = f(x)x$. Fix such f. The group $\overline{E}$ being elementary abelian, the kernel of f contains $\overline{F_2}$ and therefore f factors as a homomorphism $F/F_2 \to \overline{E}$. As a result, there exists $l \in \overline{L}$ such that, for each $x \in \overline{F}$, one has $f(x) = [l, x]$ and thus $\delta(x) = [l, x]x = lxl^{-1}$. In particular, δ is an inner automorphism of $\overline{F}$ and, the choice of δ being arbitrary, Δ is contained in $\mathrm{Inn}(\overline{F})$. □

LEMMA 9.59. *Let $N = \phi^{-1}(G_4)$. Let $\eta \in \mathrm{Aut}(F/D_N)$ be of order 2 and assume that η induces the inversion map on F/F_2. Assume moreover that β and η induce the same automorphism of F/E. Then there exists $\psi_N \in \mathrm{Inn}(F/D_N)$ such that, for all $x \in F$, one has $\beta(x) \equiv (\psi_N\eta\psi_N^{-1})(x) \bmod D_N$.*

PROOF. Set $\overline{F} = F/D_N$ and use the bar notation for the subgroups of $\overline{F}$. As a consequence of Lemma 5.32, the group N is $\langle\beta\rangle$-stable and therefore so is D_N: it follows that the map β induces an automorphism of $\overline{F}$, which we denote by $\overline{\beta}$. Let Δ denote the subgroup of $\mathrm{Aut}(\overline{F})$ consisting of all those elements δ such that δ

induces the identity on both $\overline{E}$ and $\overline{F}/\overline{E}$. Then, as a consequence of Lemmas 9.51 and 2.4, the automorphism $\eta^{-1}\overline{\beta}$ belongs to Δ and thus, thanks to Lemma 9.58, we have $\eta^{-1}\overline{\beta} \in \mathrm{Inn}(\overline{F})$. Applying the Schur-Zassenhaus theorem to $\mathrm{Inn}(\overline{F})\langle\eta\rangle$, we get that there exists $\overline{\psi} \in \mathrm{Inn}(\overline{F})$ such that $\overline{\beta} = \overline{\psi}\eta\overline{\psi}^{-1}$. This concludes the proof. □

Proposition 9.60. *Let α be an automorphism of order 2 of G that induces the inversion map on G/G_2. Then there exists $\gamma \in \mathrm{Inn}(F)$ such that $\alpha\phi = \phi(\gamma\beta\gamma^{-1})$.*

Proof. Thanks to proposition 9.48, there exists an automorphism ϵ of F/F_5 of order 2 such that $\alpha\phi_5 = \phi_5\epsilon$. As a consequence, the map ϵ induces the inversion map on F/F_2. Let now $M = \ker\phi$ and let $N = ME$. Thanks to Lemma 9.49, the group N belongs to $\mathcal{N}_3$ and $D_N \subseteq M$. One easily shows that F_5 is contained in D_N. It follows that ϵ induces an automorphism η of order 2 of F/D_N. Let η_L be the automorphism that η induces on F/L. Then, via the choice of a representative, Lemma 9.56 ensures that there exists an inner automorphism φ_N of F/D_N such that β and $\varphi_N\eta\varphi_N^{-1}$ induce the same automorphism of F/L. Fix such φ_N and define $\eta_1 = \varphi_N\eta\varphi_N^{-1}$. Since η has order 2, the order of η_1 is equal to 2. Lemma 9.57 yields that in fact η_1 and β are the same modulo E. At last, let ψ_N be as in Lemma 9.59 and define $\eta_2 = \psi_N\eta_1\psi_N^{-1}$. As a consequence of Lemma 9.59, the maps η_2 and β induce the same map on F/D_N. Via the choice of a representative, the inner automorphism $\psi_N\varphi_N$ of F/D_N lifts to an inner automorphism γ of F with the property that η and $\gamma\beta\gamma^{-1}$ induce the same automorphism on F/D_N. To conclude, let $\phi_N : F/D_N \to G$ be the map induced by ϕ. Since $\alpha\phi_5 = \phi_5\epsilon$, one gets $\alpha\phi_N = \phi_N\eta$ and therefore $\alpha\phi = \phi(\gamma\beta\gamma^{-1})$. □

Lemma 9.61. *For each $M \in \mathcal{N}_4$, one has $\beta(M) = M$.*

Proof. Let $M \in \mathcal{N}_4$. Without loss of generality $G = F/M$ and so $M = \ker\phi$. Let moreover α be an automorphism of G of order 2 that induces the inversion map on G/G_2. Then, thanks to Proposition 9.60, there exists $\gamma \in \mathrm{Inn}(F)$ such that $\alpha\phi = \phi(\gamma\beta\gamma^{-1})$. It follows that $\{1\} = \alpha(\phi(M)) = \phi\beta(M)$ and therefore $\beta(M)$ is contained in $\ker\phi = M$. Since β induces an automorphism of each quotient F/F_k and since, for large enough k one has $F_k \subseteq M$, we have in fact that $\beta(M) = M$. □

Lemma 9.62. *Let N be an element of $\mathcal{N}_3$ and write $\overline{F} = F/D_N$. Set moreover $\overline{N} = N/D_N$ and $\overline{E} = E/D_N$. Define $\overline{\beta}$ to be the map that is induced by β on $\overline{F}$ and set*

$$\overline{N}^+ = \{\overline{x} \in \overline{N} : \overline{\beta}(\overline{x}) = \overline{x}\} \quad \textit{and} \quad \overline{N}^- = \{\overline{x} \in \overline{N} : \overline{\beta}(\overline{x}) = \overline{x}^{-1}\}.$$

Then $\overline{N}^+ = \overline{E}$ and $\overline{N}^-$ is the unique $\langle\overline{\beta}\rangle$-stable complement of $\overline{E}$ in $\overline{N}$.

Proof. As a consequence of Lemma 5.32, the group $\overline{N}$ is $\langle\overline{\beta}\rangle$-stable and, being central in $\overline{F}$, it is also abelian. Write now $B = \langle\beta\rangle$ and let $\sigma : B \to \{\pm 1\}$ be the isomorphism mapping β to -1. By Lemma 5.29, the group B acts on F/F_2 through σ and, by Lemma 5.32, the induced action of B on L/E is through σ. As a consequence, the induced action of B on both L/N and N/E is through σ. It follows from Lemmas 9.51 and 2.4 that β induces the identity map on $\overline{E}$ and so, thanks to Theorem 2.9, the subgroup $\overline{E}$ has a unique $\langle\overline{\beta}\rangle$-stable complement in $\overline{N}$, which coincides with $\overline{N}^-$. □

$$\begin{tikzcd}
& F \arrow[rrr, dashed] \arrow[d, dash, "-"] & & & G \arrow[d, dash, "-"] \\
& F_2 \arrow[rrr, dashed] \arrow[d, dash, "+"] & & & G_2 \arrow[d, dash, "+"] \\
& L \arrow[rrr, dashed] \arrow[dl, dash, "-"] \arrow[dr, dash, "-"] & & & G_3 \arrow[d, dash, "-"] \\
F_3 \arrow[dr, dash, "-"] & & N \arrow[rr, dashed] \arrow[dl, dash, "-"] \arrow[dr, dash, "+"] & & G_4 \arrow[d, dash, "+"] \\
& E \arrow[dr, dash, "+"] & & M \arrow[r, dashed] \arrow[dl, dash, "-"] & 1 \\
& & D_N & &
\end{tikzcd}$$

Lemma 9.63. *The map $\mathcal{N}_4 \to \mathcal{N}_3$ that is defined by $M \mapsto ME$ is an injection respecting the natural actions of* $\mathrm{Aut}(F)$*.*

Proof. The map $\mathcal{N}_4 \to \mathcal{N}_3$ is well-defined, thanks to Lemma 9.49, and it is clear that it respects the action of $\mathrm{Aut}(F)$. We prove injectivity. To this end, let M_1 and M_2 be elements of $\mathcal{N}_4$ such that $M_1E = M_2E$ and set $N = M_1E = M_2E$. Since M_1 and M_2 belong to $\mathcal{N}_4$, Lemma 9.61 yields $\beta(M_1) = M_1$ and $\beta(M_2) = M_2$. It follows then from Lemma 9.62 that both $\overline{M_1}$ and $\overline{M_2}$ are the unique $\langle\overline{\beta}\rangle$-stable complement of $\overline{E}$ and so $M_1 = M_2$. □

Lemma 9.64. *The map $\mathcal{N}_4 \to \mathcal{N}_3$ that is defined by $M \mapsto ME$ is a bijection respecting the natural actions of* $\mathrm{Aut}(F)$*.*

Proof. The map $\mathcal{N}_4 \to \mathcal{N}_3$ is well-defined, injective, and respects the action of $\mathrm{Aut}(F)$ thanks to Lemma 9.63. We prove surjectivity. To this end, let N be an element of $\mathcal{N}_3$. Write $\overline{F} = F/D_N$ and use the bar notation for the subgroups of $\overline{F}$. Let moreover $\overline{N}^-$ be as in Lemma 9.62. As a consequence of the definition of D_N, the subgroup $\overline{N}$ is central in $\overline{F}$ and so $\overline{N}^-$ is normal in $\overline{F}$. Let M be the unique normal subgroup of F containing D_N such that $\overline{M} = \overline{N}^-$. Then, as a consequence of Lemma 9.62, one has $N = ME$. Write $H = F/M$ and denote by π the canonical projection $F \to H$. We will prove that $M \in \mathcal{N}_4$. Thanks to the isomorphism theorems, the groups $\pi(N)$ and $\overline{E}$ are naturally isomorphic and, by Lemma 9.53, the group $\overline{E}$ has order 3. It follows that $|N : M| = 3$. Moreover, the group N being an element of $\mathcal{N}_3$, the quotient F/N has class 3 and so $M \subseteq \pi^{-1}(H_4) \subseteq N$. Only two cases can occur: either $N = \pi^{-1}(H_4)$ or $M = \pi^{-1}(H_4)$. Assume by contradiction that $M = \pi^{-1}(H_4)$ and so that H has class 3. Since $H/\pi(N)$ is isomorphic to F/N, Lemma 5.27 yields that $\pi(L) = H_3\pi(N)$ and, since N is central modulo D_N, the subgroup $\pi(N)$ is central in H. It follows that $\pi([F, L]) = \{1\}$ and therefore $[F, L]$ is contained in M. As a consequence, E is also contained in M and thus $N = ME = M$, which is a contradiction. We have proven that $N = \pi^{-1}(H_4)$, from which it follows in particular that $|H_4| = |N : M| = 3$ and so H has class 4. Moreover, H is a κ-group, because F/N is. To prove that M belongs to $\mathcal{N}_4$, we are left with proving that H has an automorphism of order 2 that induces the inversion map on H/H_2 and in fact such an automorphism can be gotten, for example, by inducing β to H. We have proven that $M \in \mathcal{N}_4$ and so, the choice of N being arbitrary, the map $\mathcal{N}_3 \to \mathcal{N}_4$ is surjective. □

The set $\mathcal{N}_4$ has 3 elements and the action of $\mathrm{Aut}(F)$ on $\mathcal{N}_4$ is transitive.

Proof. Combine Proposition 9.41 and Lemma 9.64. □

We are now ready to prove Proposition 9.45. The group MC(3) is a κ-group, by Lemma 9.16, and $\mathrm{MC}(3)_4$ has cardinality 3, thanks to Lemma 9.15(1). By Lemma 9.14, the class of MC(3) is 4 and moreover, thanks to Lemma 9.17, the group MC(3) possesses an automorphism that induces the inversion map on the quotient $\mathrm{MC}(3) / \mathrm{MC}(3)_2$. It follows that there exists an element M of $\mathcal{N}_4$ with the property that F/M is isomorphic to MC(3). Corollary 9.6 now yields that G and MC(3) are isomorphic. The proof of Proposition 9.45 is complete.

9.7. Intensity

In Section 9.5 we have proven Corollary 9.5, which asserts that finite 3-groups of intensity larger than 1 have class at most 4. We will prove in this section that the bound is best possible by showing that the group MC(3), introduced at the beginning of this chapter and whose structure we investigated in Section 9.2, has intensity 2. Thanks to results coming from the previous sections, we will, at the end of the current section, finally be able to give the proof of Theorem 9.1.

Proposition 9.65. *The group* MC(3) *has intensity* 2.

We will devote a big part of the present section to the proof of Proposition 9.65. To this end, let the following assumptions hold until the end of Section 9.7. Set $G = \mathrm{MC}(3)$ and denote by $(G_i)_{i\geq 1}$ its lower central series. For all $i \in \mathbb{Z}_{\geq 1}$, write $\mathrm{wt}_G(i) = w_i$. By Lemma 9.14, the group G has class 4 and order 729. Moreover, thanks to Lemmas 9.15(1) and 9.16, the group G is a κ-group satisfying $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. Let α be as in Lemma 9.17 and set $A = \langle\alpha\rangle$. In concordance with the notation from Section 2.2, we define $G^+ = \{x \in G \;:\; \alpha(x) = x\}$ and $G^- = \{x \in G \;:\; \alpha(x) = x^{-1}\}$. Moreover, for each subgroup H of G, we denote $H^+ = H \cap G^+$ and $H^- = H \cap G^-$.

Lemma 9.66. *Let H be a subgroup of G_2 and let g be an element of G. Then the following hold.*

1. *The group G_2 normalizes H.*
2. *If both H and gHg^{-1} are A-stable, then $gHg^{-1} = H$.*

Proof. The group G_2 is abelian so G_2 normalizes each of its subgroups. As a consequence of Lemma 2.17(1), the subgroup G^+ is contained in G_2 and we conclude combining (1) with Lemma 2.15. □

LEMMA 9.67. *Let H be a subgroup of G that contains G_4. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

PROOF. We denote by α_4 the automorphism of G/G_4 that is induced by α. By Proposition 5.11, the automorphism α_4 is intense so, by Lemma 3.5, there exists $g \in G$ such that gHg^{-1}/G_4 is $\langle\alpha_4\rangle$-stable. It follows from the definition of α_4 that gHg^{-1} is A-stable. □

We recall that a positive integer j is a jump of a subgroup H of G if and only if $H \cap G_j \neq H \cap G_{j+1}$. For the theory of jumps we refer to Section 2.3.

LEMMA 9.68. *Let H be a subgroup of G such that $H \cap G_4 = \{1\}$. Assume moreover that H is not contained in G_2. Then there exists $x \in G \setminus G_2$ such that $H = \langle x\rangle$.*

PROOF. The subgroup H is different from G and it is therefore contained in a maximal subgroup C of G. Moreover, H not being contained in G_2, we have $\mathrm{wt}_H^G(1) = 1$. We first show that H is abelian. The subgroup $[H, H]$ is contained in $[C, C] = [C, G_2]$, and so $[H, H]$ is contained in G_3. By Lemma 9.11, the centre of G is equal to G_4 and so, by Lemma 7.3, the map $\gamma : G/G_2 \times G_3/G_4 \to G_4$ that is induced from the commutator map is non-degenerate. Since $C = HG_2$, we get $[C, [H, H]] = [H, [H, H]] \subseteq H \cap G_4$ and so, since $H \cap G_4 = \{1\}$, the subgroup $[H, H]$ is contained in $\mathrm{Z}(C)$. It follows that $[H, H]$ is contained in $\mathrm{Z}(C) \cap [C, C] \cap H$ and so, thanks to Corollary 9.5 and Lemma 9.12, the commutator subgroup of H is trivial. The group H being abelian, it follows, from the non-degeneracy of γ, that $\mathrm{wt}_H^G(3) \leq 1$. Moreover, since the commutator map induces an isomorphism $G/G_2 \otimes G_2/G_3 \to G_3/G_4$, we also know that $\mathrm{wt}_H^G(2) = 0$. Let now x be an element of $H \setminus G_2$. Then 1 is a jump of $\langle x\rangle$ in G and, the group G being a κ-group, it follows that $x^3 \in G_3 \setminus G_4$. As a consequence of Lemma 2.16, we get

$$|\langle x\rangle| \geq 3^{\mathrm{wt}_{\langle x\rangle}^G(1)} 3^{\mathrm{wt}_{\langle x\rangle}^G(3)} \geq 9 \geq 3^{\mathrm{wt}_H^G(1)} 3^{\mathrm{wt}_H^G(3)} = \prod_{i=1}^{4} 3^{\mathrm{wt}_H^G(i)} = |H|$$

and therefore H is cyclic generated by x. □

LEMMA 9.69. *Let H be a subgroup of G such that $H \cap G_4 = \{1\}$. Assume that H is not contained in G_2. Then H and $\alpha(H)$ are conjugate in G.*

PROOF. By Lemma 9.68, the group H is cyclic. We define $T = H \oplus G_4$ so, by Lemma 9.67, there exists $g \in G$ such that gTg^{-1} is A-stable. We fix such g and denote $T' = gTg^{-1}$ and $H' = gHg^{-1}$. The subgroup G_4 being characteristic, it follows that $H' \oplus G_4 = T' = \alpha(H') \oplus G_4$. Let $\mathcal{C}$ denote the collection of complements of G_4 in T'. By Lemma 4.6, the elements of $\mathcal{C}$ are in bijection with the elements of $\mathrm{Hom}(H', G_4)$, which is naturally isomorphic to $\mathrm{Hom}(H'/\Phi(H'), G_4)$. The group G being a κ-group, one has $\Phi(H') = H' \cap G_2$ and thus the restriction map $\mathrm{Hom}(G/G_2, G_4) \to \mathrm{Hom}(H'G_2/G_2, G_4)$ is surjective. Moreover, by Lemma 9.11, the subgroup G_4 coincides with $\mathrm{Z}(G)$ so, as a consequence of Lemma 7.3, the map $G_3/G_4 \to \mathrm{Hom}(G/G_2, G_4)$, defined by $xG_4 \mapsto (tG_2 \mapsto [x, t])$, is an isomorphism. It follows from Lemma 4.6 that, for each $K \in \mathcal{C}$, there exists $x \in G$ such that $K = \{[x, t]t = xtx^{-1} \mid t \in H'\}$. As a consequence, there is $x \in G$ such that $\alpha(H') = xH'x^{-1}$ and so, since $H' = gHg^{-1}$, also $\alpha(H)$ and H are conjugate in G. □

Lemma 9.70. *Let H be a subgroup of G_3 with $H \cap G_4 = \{1\}$. Then H and $\alpha(H)$ are conjugate in G.*

Proof. Let $T = HG_4$. The group G_3 is elementary abelian, as a consequence of Corollary 9.5, and therefore so is $T = H \oplus G_4$. Let $g \in G$ be such that gTg^{-1} is A-stable, as in Lemma 9.67, and set $T' = gTg^{-1}$ and $H' = gHg^{-1}$. Let moreover $\mathcal{C}$ be the set of complements of G_4 in T' and note that both H' and $\alpha(H')$ belong to $\mathcal{C}$. Thanks to Lemma 4.6, the elements of $\mathcal{C}$ are in bijection with the elements of $\mathrm{Hom}(H', G_4)$. Moreover, the restriction map induces a surjection $\mathrm{Hom}(G_3/G_4, G_4) \to \mathrm{Hom}(H', G_4)$. By Lemma 9.11, the subgroup G_4 coincides with $\mathrm{Z}(G)$ so, as a consequence of Lemma 7.3, the map $G/G_2 \to \mathrm{Hom}(G_3/G_4, G_4)$, defined by $xG_4 \mapsto (tG_2 \mapsto [x,t])$ is an isomorphism. It follows from Lemma 4.6 that each element of $\mathcal{C}$ is of the form $\{[x,t]t = xtx^{-1} \mid t \in H'\} = xH'x^{-1}$, for some $x \in G$. In particular, $\alpha(H')$ and H' are conjugate in G and thus so are H and $\alpha(H)$. □

Lemma 9.71. *Let H be a subgroup of G with $H \oplus G_4 = G_2$. Then H has an A-stable conjugate in G.*

Proof. We define X to be the collection of all subgroups K of G for which $G_2 = K \oplus G_4$. The group G_2 is elementary abelian, by Corollary 9.5, so the set X is non-empty. Moreover, as a consequence of Lemma 4.6, the cardinality of X is equal to the cardinality of $\mathrm{Hom}(H, G_4)$, which is 27. We define $X^+ = \{K \in X \ : \ \alpha(K) = K\}$ and we will show, with a counting argument, that H is conjugate to an element of X^+. Let $K \in X^+$. Thanks to Corollary 2.2, we can write $K = K^+ \oplus K^-$ and, as a consequence of Lemma 2.17, the subgroup K^- is equal to G_2^-. Again by Lemma 2.17, the subgroup G_2^+ has order 9 and it contains G_4. It follows that $|X^+|$ is equal to the number of 1-dimensional subspaces of G_2^+ that are different from G_4, i.e. $|X^+| = 3$. By Lemma 9.66(1), the group G_2 normalizes K, but in fact $G_2 = \mathrm{N}_G(K)$, as a consequence of Lemma 7.3. It follows that the orbit of K in X has size $|G : G_2| = 9$ so, thanks to Lemma 9.66(2), the element K is the only element of X^+ belonging to its orbit under G/G_2. The number $|X|/|X^+|$ being equal to 9, it follows that each orbit of the action of G/G_2 on X has a representative in X^+. The same holds for the orbit of H. □

Lemma 9.72. *Let H be a subgroup of G with $H \oplus G_3 = G_2$. Then H has an A-stable conjugate in G.*

Proof. Let X be the collection of all complements of G_3 in G_2. The group G_2 is elementary abelian, by Corollary 9.5, and so, by Lemma 4.6, the cardinality of X is equal to $|\mathrm{Hom}(H, G_3)| = 27$. We define $X^+ = \{K \in X \ : \ \alpha(K) = K\}$. As a consequence of Lemma 2.17, if K is an element of X^+, then $K = K^+$. The elements of X^+ are thus exactly the one-dimensional subspaces of G_2^+ that are different from G_4 and so $|X^+| = 3$. Fix $K \in X^+$. Then the commutator map induces an isomorphism $G/G_2 \otimes K \to G_3/G_4$. It follows that $\mathrm{N}_G(K)$ is contained in G_2 so, thanks to Lemma 9.66(1), one has $\mathrm{N}_G(K) = G_2$. Lemma 9.66(2) yields that K is the only element of X^+ belonging to its orbit under the action of G/G_2 on X. The number $|X|/|X^+|$ being equal to 9, it follows that each orbit of the action of G/G_2 on X has a representative in X^+ so, in particular, H has an A-stable conjugate in G. □

Lemma 9.73. *Let $x \in G \setminus G_2$ and let $a \in G_2^+ \setminus G_3$. Then $[x, a]$ does not belong to G^-.*

Proof. Let $C = \mathrm{C}_G([x, a])$ and $D = \langle x, G_2 \rangle$. Then $[x, a]$ belongs to $G_3 \setminus G_4$ so, as a consequence of Lemmas 9.11 and 7.3, the index of C in G is equal to 3. In particular, both C and D are maximal subgroups of G. Assume now by contradiction that $[x, a] \in G^-$. Since x belongs to $G \setminus G_2$, there exists $\gamma \in G_2$ such that $\alpha(x) = x^{-1}\gamma$ and so we have $[x, a]^{-1} = \alpha([x, a]) = [x^{-1}\gamma, a]$. The group G_2 is elementary abelian, by Corollary 9.5, and so, with the help of multiplication formulas, one gets $[x, a]^{-1} = [x^{-1}, [x, a]^{-1}][x, a]^{-1}$. As a result, the element $[x^{-1}, [x, a]^{-1}]$ is trivial, and so $x \in C$. Then $C = D$, and thus $[x, a]$ belongs to $[C, C] \cap \mathrm{Z}(C)$. Lemma 9.12 yields $[x, a] \in G_4$. Contradiction. □

Lemma 9.74. *Let $x \in G_2 \setminus G_3$ and $y \in G_3 \setminus G_4$. Define $H = \langle x, y \rangle$. Then H has an A-stable conjugate in G.*

Proof. The group G_2 is elementary abelian, by Corollary 9.5, and therefore $H = \langle x \rangle \oplus \langle y \rangle$. Let X be the set consisting of all subgroups of G_2 of the form $\langle u \rangle \oplus \langle v \rangle$, where $u \in G_2 \setminus G_3$ and $v \in G_3 \setminus G_4$. The cardinality of X is then equal to 108. We define $X^+ = \{K \in X \ : \alpha(K) = K\}$ and we fix $K \in X^+$. By Corollary 2.2, the subgroup K decomposes as $K = K^+ \oplus K^-$ and, as a consequence of Lemma 2.17, there exists $a \in G_2^+$ such that $K = \langle a \rangle \oplus K^-$. Fix such a. Again thanks to Lemma 2.17, we get that $|X^+| = 12$. We want to count the conjugates of K. By Lemma 9.66(1), the subgroup G_2 is contained in $\mathrm{N}_G(K)$ and, if $x \in \mathrm{N}_G(K)$, then $[x, a] \in K \cap G_3$. The intersection $K \cap G_3$ being equal to K^-, it follows from Lemma 9.73 that $\mathrm{N}_G(K) = G_2$. As a consequence of Lemma 9.66(2), the element K is the only element of X^+ belonging to its orbit under G/G_2 so, from the equality $|X|/|X^+| = 9$, we can deduce that each orbit in X has a representative in X^+. The same holds for the orbit of H. □

Lemma 9.75. *The automorphism α is intense. Moreover, the intensity of G is equal to* 2.

Proof. Let H be a subgroup of G. If H contains G_4, then, by Lemma 9.67, there exists a conjugate of H that is A-stable. Assume that $H \cap G_4 = \{1\}$. If H is not contained in G_2, then H is conjugate to $\alpha(H)$, thanks to Lemma 9.69. Assume that H is contained in G_2. If 2 is not a jump of H in G, then, by Lemma 9.70, the subgroups H and $\alpha(H)$ are conjugate in G. We suppose that 2 is a jump of H in G. By Corollary 9.5, the group G_2 is elementary abelian and so H is a subspace of G_2, not contained in G_3, that trivially intersects G_4. The combination of Lemmas 9.71, 9.72, and 9.74 guarantees that H has an A-stable conjugate in G. The choice of H being arbitrary, it follows from Lemma 3.5 that α is intense. The intensity of G is at least 2, because α has order 2, but in fact $\mathrm{int}(G) = 2$, as a consequence of Theorem 5.2(1). □

We remark that, thanks to Lemma 9.75, the proof of Proposition 9.65 is complete. Moreover, we are now also able to prove Theorem 9.1. The implication (2) ⇒ (1) is clear and the implication (3) ⇒ (2) is given by the combination of Proposition 9.65 and Lemma 9.14. We now prove (1) ⇒ (2). To this end, let Q be a finite 3-group of class at least 4 with $\mathrm{int}(Q) > 1$. Because of Corollary 9.5, the class of Q is equal to 4 so, as a consequence of Theorem 6.1, the order of Q is equal to 729. The intensity of Q is equal to 2, thanks to Theorem 5.2(1). We have concluded the proof of (1) $\Rightarrow$ (2) and, to finish the proof of Theorem 9.1, we will next prove (2) $\Rightarrow$ (3). Let Q be a finite 3-group of class 4 and intensity 2. Then, by Lemma 9.9, the group Q is a κ-group and, as a consequence of Proposition 5.10, it possesses an automorphism of order 2 that induces the inversion map on Q/Q_2. By Theorem 6.1, the order of Q_4 is 3. Proposition 9.45 yields that Q is isomorphic to MC(3). The proof of Theorem 9.1 is now complete.

CHAPTER 10

Obelisks

Let $p > 3$ be a prime number. A *p-obelisk* is a finite p-group G for which the following hold.

1. The group G is not abelian.
2. One has $|G : G_3| = p^3$ and $G_3 = G^p$.

The following proposition will immediately clarify our interest in p-obelisks.

Proposition 10.1. *Let $p > 3$ be a prime number and let G be a finite p-group of class at least 4. If $\mathrm{int}(G) > 1$, then G is a p-obelisk.*

Proof. Combine Theorems 6.1 and 7.1. □

Chapter 10 will be entirely devoted to understanding the structure of p-obelisks and that of their subgroups. Some of the results, especially coming from Section 10.4, are rather technical and their relevance will become evident in Chapter 11.

10.1. Some properties

We remind the reader that, if p is a prime and G is a finite p-group, then $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$ where $(G_i)_{i\geq 1}$ denotes the lower central series of G. The following lemma collects some straightforward properties of p-belisks. Concerning regularity, we refer to Section 8.1.

Lemma 10.2. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let $(G_i)_{i\geq 1}$ denote the lower central series of G. Then the following hold.*

1. *One has $\mathrm{wt}_G(1) = 2$ and $\mathrm{wt}_G(2) = 1$.*
2. *The group G/G_3 is extraspecial of exponent p.*
3. *The group G is regular.*

Proposition 10.3. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let $(G_i)_{i\geq 1}$ be the lower central series of G and let c denote the class of G. Then the following hold.*

1. *For all $i \in \mathbb{Z}_{\geq 1}$, one has $\mathrm{wt}_G(i)\,\mathrm{wt}_G(i+1) \leq 2$.*
2. *If $\mathrm{wt}_G(i)\,\mathrm{wt}_G(i+1) = 1$, then $i = c - 1$.*
3. *For all positive integers k and l, not both even, one has $[G_k, G_l] = G_{k+l}$.*

Proof. Proposition 10.3 is a simplified version of Theorem 4.3 from [**Bla61**], which can also be found in Chapter 3 of [**Hup67**] as Satz 17.9. □

We remark that the term *p-obelisk* does not appear in [**Bla61**] or [**Hup67**] and is of our own invention. Moreover, originally Proposition 10.3(1-2) was phrased in the following way: if G is a p-obelisk, then

$$(\mathrm{wt}_G(i))_{i\geq 1} = (2, 1, 2, 1, \ldots, 2, 1, f, 0, 0, \ldots) \quad \text{where} \quad f \in \{0, 1, 2\}.$$

The following lemma follows in a straightforward way from Lemma 10.2 and Proposition 10.3.

LEMMA 10.4. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the class of G and let $i \in \{1, \ldots, c-1\}$. Then the following hold.*

1. *The index i is odd if and only if* $\mathrm{wt}_G(i) = 2$.
2. *The index i is even if and only if* $\mathrm{wt}_G(i) = 1$.
3. *If* $\mathrm{wt}_G(c) = 2$, *then c is odd.*
4. *If c is even, then* $\mathrm{wt}_G(c) = 1$.

We recall that, if G is a p-group, then ρ denotes the map $x \mapsto x^p$ on G.

LEMMA 10.5. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then, for all $i, k \in \mathbb{Z}_{>0}$, one has $\rho^k(G_i) = G_{2k+i}$.*

In his original proof of Proposition 10.3, Blackburn also proves Lemma 10.5. Blackburn's proof strongly relies on the fact that p-obelisks are regular and it makes use of some technical lemmas that can be found in [**Hup67**, Ch. III]. The following, for example, is Satz 10.8(a) from [**Hup67**, Ch. III].

LEMMA 10.6. *Let p be a prime number and let G be a finite regular p-group. Let M, N be normal subgroups of G and let r, s be non-negative integers. Then $[\rho^r(M), \rho^s(N)] = \rho^{r+s}([M, N])$.*

PROPOSITION 10.7. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let $(G_i)_{i \geq 1}$ be the lower central series of G and let c denote its nilpotency class. Then $\mathrm{Z}(G) = G_c$.*

PROOF. We work by induction on c. If $c = 2$, then, by Lemma 10.2(2), the group G is extraspecial so $G_2 = \mathrm{Z}(G)$. Assume now that $c > 2$. The subgroup G_c is central and, by the induction hypothesis, $\mathrm{Z}(G/G_c) = G_{c-1}/G_c$. It follows that $G_c \subseteq \mathrm{Z}(G) \subseteq G_{c-1}$ and $\mathrm{Z}(G) \neq G_{c-1}$. Moreover, by Proposition 10.3(1), the width $\mathrm{wt}_G(c-1)$ is either 1 or 2. If $\mathrm{wt}_G(c-1) = 1$, then $\mathrm{Z}(G) = G_c$; we assume thus that $\mathrm{wt}_G(c-1) = 2$. By Lemma 10.4(1), there exists a positive integer k such that $c - 1 = 2k + 1$ so, from Lemma 10.5, we get $G_{c-1} = \rho^k(G)$ and $G_c = \rho^k(G_2)$. As a consequence of Proposition 10.3(1), the subgroup G_c has order p. Let us assume by contradiction that $\mathrm{Z}(G) \neq G_c$, in other words $|G_{c-1} : \mathrm{Z}(G)| = |\,\mathrm{Z}(G) : G_c| = p$. Let $N = \mathrm{C}_G(G_{c-1})$. The commutator map $G/G_2 \times G_{c-1}/G_c \to G_c$ is bilinear and it factors as a surjective non-degenerate map $G/N \times G_{c-1}/\,\mathrm{Z}(G) \to G_c$. It follows that G/N is cyclic of order p so $G_2 = [N, G]$. Lemma 10.6 yields $\rho^k([N, G]) = [N, \rho^k(G)] = [N, G_{c-1}] = \{1\}$ and so $G_c = \rho^k(G_2) = \{1\}$. Contradiction. □

LEMMA 10.8. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then each non-abelian quotient of G is a p-obelisk.*

PROOF. Let N be a normal subgroup of G such that G/N is not abelian. We claim that N is contained in G_3. Denote first $H = G/N$. Then we have $p^2 \leq |H : H_2| \leq |G : G_2|$ and therefore, from Lemma 10.2(1), it follows that $N \subseteq G_2$. If $N \cap G_3 = N$, then N is contained in G_3 and we are done. Assume by contradiction that $N \cap G_3 \neq N$. As a consequence of Lemma 10.2(1), the subgroup N does not contain G_3. Let now M be a normal subgroup of G such that $N \cap G_3 \subseteq M \subseteq G_3$ and $|G_3 : M| = p$. Then $\overline{G} = G/M$ has class 3 and $\overline{N} \neq \{1\}$. However, by Lemma 5.12, the centre of $\overline{G}$ is equal to $\overline{G_3}$ so, $\overline{G_3}$ having order p, we get $\overline{G_3} \subseteq \overline{N}$. In particular, G_3 is contained in MN. It follows that $G_3 = G_3 \cap (MN) = (G_3 \cap N)M = M$, which gives a contradiction. Then $N \subseteq G_3$, as claimed, and thus we have $|H : H_3| = |G : G_3|$. It is moreover clear that $H^p = H_3$, and so H is a p-obelisk. □

LEMMA 10.9. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then the following hold.*

1. *If $i \in \mathbb{Z}_{\geq 1}$ and H is a quotient of G of class i, then $\mathrm{Z}(H) = H_i$.*
2. *Let N be a subgroup of G. Then N is normal in G if and only if there exists $i \in \mathbb{Z}_{>0}$ such that $G_{i+1} \subseteq N \subseteq G_i$.*

PROOF. (1) Let c denote the class of G. Let moreover $i \in \{1, \ldots, c\}$ and let H be a quotient of G of class i. If $i = 1$, the group H is abelian and $\mathrm{Z}(H) = H$. Assume now that $i > 1$. Then H is a non-abelian quotient of a p-obelisk so, by Lemma 10.8, it is a p-obelisk itself. To conclude, apply Proposition 10.7. For the proof of (2), we combine (1) with Lemma 6.8. □

10.2. Power maps and commutators

Throughout Section 10.2 we will faithfully follow the notation from the List of Symbols. In particular, if p is a prime number and G is a finite p-group, then ρ will denote the map $G \to G$ that is defined by $x \mapsto x^p$. We remind the reader that ρ is in general not a homomorphism.

LEMMA 10.10. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then the following hold.*

1. *For all $i, k \in \mathbb{Z}_{>0}$ the map $\rho^k : G_i \to G_i$ induces a surjective homomorphism*
$$\rho_i^k : G_i/G_{i+1} \to G_{2k+i}/G_{2k+i+1}.$$
2. *For all $h, k \in \mathbb{Z}_{>0}$ not both even, the commutator map induces a bilinear map*
$$\gamma_{h,k} : G_h/G_{h+1} \times G_k/G_{k+1} \to G_{h+k}/G_{h+k+1}$$
whose image generates G_{h+k}/G_{h+k+1}.

PROOF. (1) Let i and k be positive integers and, without loss of generality, assume that $G_{2k+i+1} = \{1\}$. We work by induction on k and we start by taking $k = 1$. Since $[G_i, G_i]$ is contained in G_{2i}, Lemma 10.5 yields that $[G_i, G_i]^p$ is contained in G_{2i+2}. The index i being positive, G_{2i+2} is contained in $G_{i+3} = \{1\}$. Now, the prime p is larger than 3 so G_{ip} is also contained in $G_{i+3} = \{1\}$. Moreover, $(G_i)_p$ is contained in G_{ip}, and so, as a consequence of the Hall-Petrescu formula, the map $\rho : G_i \to G_i$ is a homomorphism. The function ρ factors as a surjective homomorphism $\rho_i^1 : G_i/G_{i+1} \to G_{i+2}$, thanks to Lemma 10.5. This finishes the proof for $k = 1$. Assume now that $k > 1$ and define

$$\rho_i^k = \rho_{2k+i-1}^1 \circ \rho_{2k+i-3}^1 \circ \ldots \circ \rho_{i+2}^1 \circ \rho_i^1.$$

As a consequence of the base case, ρ_i^k is a surjective homomorphism $\rho_i^k : G_i/G_{i+1} \to G_{2k+i}/G_{2k+i+1}$ and, by its definition, it is induced by ρ^k. This proves (1). Point (2) follows from Proposition 10.3(3). □

Let $p > 3$ be a prime number and let G be a p-obelisk. Let c be the class of G. Let moreover i and j be integers of the same parity such that $1 \leq i \leq j \leq c$ and one of the following holds.

1. The number j is even.
2. One has $\mathrm{wt}_G(j) = 2$.

Define $m = \frac{j-i}{2}$. Then the map $\rho^m : G_i \to G_i$ induces an isomorphism $\rho_i^m : G_i/G_{i+1} \to G_j/G_{j+1}$.

Proof. Let $\rho_i^m : G_i/G_{i+1} \to G_j/G_{j+1}$ be the surjective homomorphism from Lemma 10.10(1). Since i and j have the same parity, it follows from Lemma 10.4 that $\mathrm{wt}_G(i) = \mathrm{wt}_G(j)$ and ρ_i^m is a bijection. $\square$

Lemma 10.11. *Let $p > 3$ be a prime number and let G be a p-obelisk. Denote by c the class of G. Let moreover h and k be positive integers, not both even, such that $h + k \leq c$. Assume additionally that, if $h + k$ is odd, then $\mathrm{wt}_G(h + k) = 2$. Then the map $\gamma_{h,k}$ from Lemma 10.10 is non-degenerate.*

Proof. Without loss of generality, assume that $c = h+k$ and so $G_{h+k+1} = \{1\}$. We prove non-degeneracy of $\gamma_{h,k}$ by looking at the parity of $h+k$. Assume first that $h+k$ is odd and, without loss of generality, h is odd and k is even. From Lemma 10.4, it follows that $\mathrm{wt}_G(h) = 2$ and $\mathrm{wt}_G(k) = 1$. Moreover, by assumption, $\mathrm{wt}_G(h+k) = 2$. Since the image of $\gamma_{h,k}$ generates G_{h+k}, the map $\gamma_{h,k}$ is non-degenerate. Let now $h+k$ be even. The numbers h and k are both odd so $\mathrm{wt}_G(h) = \mathrm{wt}_G(k) = 2$, by Lemma 10.4(2). Assume without loss of generality that $h \leq k$. Then, by Lemma 10.5, the set $\rho^{\frac{k-h}{2}}(G_h)$ coincides with the subgroup G_k. Let now $C = \mathrm{C}_{G_h}(G_k)$ and $D = \mathrm{C}_{G_k}(G_h)$. Since $\gamma_{h,k} \neq 1$, we have that $G_{h+1} \subseteq CG_h$ and $G_{k+1} \subseteq DG_k$. The commutator map induces a non-degenerate map $G_h/C \times G_k/D \to G_{h+k}$ so, $\mathrm{wt}_G(h + k)$ being equal to 1, one derives $|G_h : C| = |G_k : D|$. Now, by Lemma 10.2(3), the group G is regular, and therefore so is C. Thanks to Lemma 8.3(1), the set $\rho^{\frac{k-h}{2}}(C)$ is a subgroup of C and so, thanks to Lemma 10.6, one has $[\rho^{\frac{k-h}{2}}(C), G_h] = [C, \rho^{\frac{k-h}{2}}(G_h)] = [C, G_k] = \{1\}$. In particular, $\rho^{\frac{k-h}{2}}(C) \subseteq D$. Since $|G_h : C| = |G_k : D|$ and $\mathrm{wt}_G(h) = \mathrm{wt}_G(k) = 2$, we derive from Corollary 10.2 that $\rho^{\frac{k-h}{2}}(C) = D$. Assume now by contradiction that there exists $x \in G_h$ such that $G_h = \langle x, C\rangle$. Then $G_k = \langle \rho^{\frac{k-h}{2}}(x), D\rangle$ and therefore, the commutator map being alternating, one has $G_{h+k} = [G_k, G_h] = \langle [x, \rho^{\frac{k-h}{2}}(x)]\rangle = \{1\}$. Contradiction to the class of G being $h + k$. It follows that the quotient G_h/C is not cyclic and so $C = G_{h+1}$ and $D = G_{k+1}$. In particular, $\gamma_{h,k}$ is non-degenerate. $\square$

Let $p > 3$ be a prime number and let G be a p-obelisk. Denote by c the class of G. Let moreover $l \in \{1, \ldots, c - 1\}$ be such that $c - l$ is odd. Then the map $G_{c-l}/G_{c-l+1} \to \mathrm{Hom}(G_l/G_{l+1}, G_c)$ that is defined by $t\, G_{c-l+1} \mapsto (x\, G_{l+1} \mapsto [t, x])$ is a surjective homomorphism of groups.

Proof. As a consequence of Lemma 10.5, the groups G_l/G_{l+1}, G_{c-l}/G_{c-l+1}, and G_c are elementary abelian and the map $\gamma_{c-l,l}$ from Lemma 10.10 is thus a bilinear map of $\mathbb{F}_p$-vector spaces. We define $\delta : G_{c-l}/G_{c-l+1} \to \mathrm{Hom}(G_l/G_{l+1}, G_c)$ to be the map sending each element $v \in G_{c-l}/G_{c-l+1}$ to the map $x \mapsto \gamma_{c-l,l}(v, x)$. In other words, if $v = t\, G_{c-l+1}$, then $\delta(v) : G_l/G_{l+1} \to G_c$ is defined by $x\, G_{l+1} \mapsto [t, x]$. As a consequence of Lemma 10.10(2), the function δ is a homomorphism of groups and δ differs from the zero map. Let us now, for all $i \in \{1, \ldots, c\}$, denote $w_i = \mathrm{wt}_G(i)$. It follows that the dimension of $\mathrm{Hom}(G_l/G_{l+1}, G_c)$ is equal to $w_l w_c$ and, if $w_l w_c = 1$, then δ is surjective. We assume that $w_l w_c \neq 1$. The index $c - l$ being odd, it follows that either l or c is even. Proposition 10.3 yields $w_{c-l} = w_l w_c$

and, if l is even, then $w_c = 2$. As a consequence of Lemma 10.11, the map δ is injective and so δ is also surjective. □

10.3. Framed obelisks

Let $p > 3$ be a prime number and let G be a p-obelisk. If $(G_i)_{i\geq 1}$ denotes the lower central series of G, then G is *framed* if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$. The following is an elementary result, whose proof is mostly computational and therefore omitted.

Proposition 10.12. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let moreover $h, k \in \mathbb{Z}_{>0}$, with h odd and k even, and let $m, n \in \mathbb{Z}_{\geq 0}$. Then the following diagram is commutative.*

$$\begin{tikzcd}
G_h/G_{h+1} \times G_k/G_{k+1} \arrow[r, "\gamma_{h,k}"] \arrow[d, "(\rho_h^m\ ,\ \rho_k^n)"] & G_{h+k}/G_{h+k+1} \arrow[d, "\rho_{h+k}^{m+n}"'] \\
G_{h+2m}/G_{h+2m+1} \times G_{k+2n}/G_{k+2n+1} \arrow[r, "\gamma_{h+2m,k+2n}"] & G_{h+k+2(m+n)}/G_{h+k+2(m+n)+1}
\end{tikzcd}$$

Lemma 10.13. *Let $p > 3$ be a prime number and let G be a p-obelisk of class at least 3. Let moreover M be a maximal subgroup of G. Then $[M, M] = [M, G_2]$ and, whenever $\mathrm{wt}_G(3) = 2$, the following are equivalent.*

1. *One has $\Phi(M) \neq G_3$.*
2. *One has $[M, M] = M^p = \Phi(M)$.*

Proof. The subgroups M^p and $[M, M]$ are both normal in G. By Lemma 10.2(1), the quotient G/G_2 has order p^2 and so $|G : M| = |M : G_2| = p$. It follows that $[M, M] = [M, G_2]$ and so, as a consequence of Corollary 10.2 and Lemma 10.11, the least jumps of $[M, M]$ and M^p in G are both equal to 3 and of width 1. In particular, $\Phi(M)$ is contained in G_3 and Lemma 10.9(2) yields $G_4 \subseteq M^p \cap [M, M]$. If the third width of G is equal to 2, then it follows that $\Phi(M) \neq G_3$ if and only if $[M, M] = \Phi(M) = M^p$. □

We remark that, as a consequence of Lemma 10.5, quotients of consecutive elements of the lower central series of a p-obelisk are vector spaces over $\mathbb{F}_p$ and therefore, in (2) and (3) from Proposition 10.14, it makes sense, for each positive integer i, to talk about subspaces of G_i/G_{i+1}.

Proposition 10.14. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then the following conditions are equivalent.*

1. *The p-obelisk G is framed.*
2. *For each 1-dimensional subspace ℓ of G/G_2, the quotient G_3/G_4 is generated by $\rho_1^1(\ell)$ and $\gamma_{1,2}(\{\ell\} \times G_2/G_3)$.*
3. *For each $h, k \in \mathbb{Z}_{>0}$, with h odd and k even, and for each 1-dimensional subspace ℓ in G_h/G_{h+1}, the spaces $\rho_h^{k/2}(\ell)$ and $\gamma_{h,k}(\{\ell\} \times G_k/G_{k+1})$ generate G_{h+k}/G_{h+k+1}.*

Proof. (1) ⇔ (2) Let $\pi : G \to G/G_2$ denote the natural projection. Then, through π, there is a bijection between the maximal subgroups of G and the 1-dimensional subspaces of G/G_2. For any maximal subgroup M of G, we know that $[M, G_2] = [M, M]$ and so Lemma 10.13 ensures that (2) holds if and only if, given any maximal subgroup M of G, one has $\Phi(M)G_4 = G_3$. Lemma 10.9(2) yields that

(2) is satisfied if and only if, for any maximal subgroup M of G, one has $\Phi(M) = G_3$. We now deal with (2) $\Leftrightarrow$ (3). The implication $\Leftarrow$ is proven by taking $h = 1$ and $k = 2$, so we will prove that (2) implies (3). Let ℓ be a 1-dimensional subspace of G_h/G_{h+1}. Define moreover $m = \frac{h-1}{2}$, $n = \frac{k-2}{2}$, and $S = m + n = \frac{h+k-3}{2}$. Thanks to Lemma 10.10(1), there exists a 1-dimensional subspace ℓ' of G/G_2 such that $\rho_1^m(\ell') = \ell$ and, moreover, $\rho_2^n(G_2/G_3) = G_k/G_{k+1}$. By assumption G_3/G_4 is generated by $\rho_1^1(\ell')$ and $\gamma_{1,2}(\{\ell'\} \times G_2/G_3)$, so it follows from Lemma 10.10(1) that $\rho_3^S(\rho_1^1(\ell'))$ and $\rho_3^S(\gamma_{1,2}(\{\ell'\} \times G_2/G_3))$ together span G_{h+k}/G_{h+k+1}. We now have $\rho_3^S(\rho_1^1(\ell')) = \rho_1^{S+1}(\ell') = \rho_h^{k/2}(\ell)$ and, thanks to Proposition 10.12, we also have

$$\rho_3^S(\gamma_{1,2}(\{\ell'\} \times G_2/G_3)) = \gamma_{h,k}(\rho_1^m(\ell') \times \rho_2^n(G_2/G_3)) = \gamma_{h,k}(\{\ell\} \times G_k/G_{k+1}).$$

This completes the proof. □

10.4. Subgroups of obelisks

The major goal of this section is to link structural properties of subgroups of a p-obelisk to the parities and widths of their jumps (see Section 2.3). The importance of Section 10.4 will become clear in Chapter 13.

Proposition 10.15. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let H be a subgroup of G that is itself a p-obelisk. Then $H = G$.*

Proof. The subgroup H is non-abelian and so non-trivial. Let l denote the least jump of H in G. Then $H_2 = [H, H]$ is contained in G_{2l} and moreover, since H is a p-obelisk, H^p is contained in H_2. It follows from Corollary 10.2 that the minimum jump of H_2 is at most $l + 2$: we get that $2l \leq l + 2$ and therefore $l \leq 2$. We will show that $HG_2 = G$. Assume by contradiction that $G \neq HG_2$. Then, as a consequence of Lemma 10.2(1), the width $\mathrm{wt}_H^G(l)$ is equal to 1 and so $H_2 = [H, H \cap G_{l+1}]$. Then H_2 is contained in G_{2l+1} and therefore $2l + 1 \leq l + 2$. It follows that $l = 1$ and that H_2 is contained in G_3. Define now $\overline{G} = G/G_4$ and use the bar notation for the subgroups of $\overline{G}$. The groups $\overline{H}$ and $H/(H \cap G_4)$ are isomorphic and so, as a consequence of Lemma 10.8, the group $\overline{H}$ is abelian or a p-obelisk. The minimum jump of H^p in G being equal to 3, we have that 3 is a jump of $\overline{H_2}$ in $\overline{G}$ and so $\overline{H}$ is a p-obelisk. Now, the group $\overline{G_3}$ is central in $\overline{G}$ and so, the group $\overline{H_2}$ being non-trivial, the quotient $\overline{H}/(\overline{H} \cap \overline{G_3})$ is not cyclic. It follows that 2 is a jump of $\overline{H}$ in $\overline{G}$ and, from the combination of Lemmas 10.4 and 10.10(2), that $\overline{H_2}$ has order p. Since $\overline{H_2}$ contains $\overline{H}^p$, we get $\overline{H_2} = \overline{H}^p = \overline{H_3}$. Contradiction to $\overline{H}$ being non-abelian. We have proven that $G = HG_2 = H\Phi(G)$, from which it follows that $H = G$. □

Lemma 10.16. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let H be a cyclic subgroup of G. Then all jumps of H in G have the same parity and width 1.*

Proof. Let H be a cyclic subgroup of G. Then, for all $i \in \mathbb{Z}_{>0}$, there exists $k \in \mathbb{Z}_{\geq 0}$ such that $H \cap G_i = H^{p^k}$. Moreover, $i \in \mathbb{Z}_{>0}$ is a jump of H in G if and only if there exists $k \in \{0, 1, \ldots, \log_p |H| - 1\}$ such that $H \cap G_i = H^{p^k}$ and $H \cap G_{i+1} = H^{p^{k+1}}$. We conclude thanks to Lemma 10.10(1). □

Lemma 10.17. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the nilpotency class of G and assume that one of the following holds.*

1. *The number c is even.*
2. *One has $\mathrm{wt}_G(c) = 2$.*

If H is a subgroup such that all of its jumps in G have the same parity and width 1, then H is cyclic.

Proof. Without loss of generality we assume that H is non-trivial and we take l to be the least jump of H in G. Let moreover $\mathcal{J}(H)$ denote the collection of jumps of H in G and define the set $J = \{l + 2k \ : \ k \in \mathbb{Z}_{\geq 0},\ k \leq (c-l)/2\}$. Let x be an element of H such that $\mathrm{dpt}_G(x) = l$; the existence of x is guaranteed by Lemma 2.16. Write $K = \langle x \rangle$ and let $\mathcal{J}(K)$ be the collection of jumps of K in G. By assumption J contains $\mathcal{J}(H)$ and, as a consequence of Corollary 10.2, the set J is contained in $\mathcal{J}(K)$. Keeping in mind that each jump of H in G has width 1, one derives

$$|K| = \prod_{j \in \mathcal{J}(K)} p^{\mathrm{wt}_K^G(j)} \geq \prod_{j \in J} p^{\mathrm{wt}_K^G(j)} \geq \prod_{j \in J} p^{\mathrm{wt}_H^G(j)} \geq \prod_{j \in \mathcal{J}(H)} p^{\mathrm{wt}_H^G(j)} = |H|.$$

It follows that $K = H$ and H is cyclic. □

Lemma 10.18. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the nilpotency class of G and let H be a subgroup of G such that $H \cap G_c = \{1\}$. If all jumps of H in G have the same parity and width 1, then H is cyclic.*

Proof. We denote $\overline{G} = G/G_c$ and we will use the bar notation for the subgroups of $\overline{G}$. As a consequence of Lemma 10.8, the group $\overline{G}$ is abelian or it is a p-obelisk. If $\overline{G}$ is abelian, then $c = 2$ and so, by Lemma 10.17, the subgroup H is cyclic. Assume now that $\overline{G}$ is non-abelian and thus a p-obelisk. The group $\overline{G}$ has class $c - 1$ and, as a consequence of Corollary 10.4, either $c - 1$ is even or $\mathrm{wt}_{\overline{G}}(c-1) = 2$. It follows from Lemma 10.17 that $\overline{H}$ is cyclic and, the intersection $H \cap G_c$ being trivial, so is H. □

Lemma 10.19. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the nilpotency class of G and let H be a non-trivial subgroup of G such that $H \cap G_c = \{1\}$. Let l be the least jump of H in G and assume that all jumps of H in G have the same parity and the same width. Then the following hold.*

1. *The group H is abelian.*
2. *One has $\Phi(H) = H \cap G_{l+1}$.*

Proof. Let $\mathcal{J}(H)$ denote the collection of jumps of H in G. We first assume $\mathrm{wt}_H^G(l) = 1$. By Lemma 10.18, the subgroup H is cyclic and $\Phi(H)$ has index p in H. It follows that $\Phi(H) = H \cap G_{l+1}$. Assume now that $\mathrm{wt}_H^G(l) = 2$. Then, thanks to Lemma 10.4(3), the jump l is odd. The subgroup $[H, H]$ is contained in G_{2l} and therefore, $2l$ being even, Lemma 10.10(2) yields $2l > c$. In particular, one has $[H, H] = \{1\}$ so $\Phi(H) = H^p$. Moreover, as a consequence of Lemma 10.10(1), the set of jumps of H^p in G is equal to $\mathcal{J}(H) \setminus \{l\}$ and each jump of H^p has width 2. It follows that $H^p = H \cap G_{l+1}$. Thanks to Proposition 10.3 the width $\mathrm{wt}_H^G(l)$ is either 1 or 2 and the proof is thus complete. □

Lemma 10.20. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c be the class of G and let H be a non-trivial subgroup of G such that $H \cap G_c = \{1\}$. Denote by l the least jump of H and assume that $H \cap G_{l+1} = \Phi(H)$. Finally, assume that $c - l$ is odd. Then, for each complement K of G_c in HG_c, there exists $t \in G_{c-l}$ such that $K = tHt^{-1}$.*

Proof. The subgroup G_c is central in G and so, by Lemma 4.6, all complements of G_c in $T = HG_c$ are of the form $\{f(h)h : h \in H\}$ as f varies in $\mathrm{Hom}(H, G_c)$. By Lemma 10.5, the subgroup G_c is elementary abelian and therefore the group $\mathrm{Hom}(H, G_c)$ is naturally isomorphic to $\mathrm{Hom}(H/(H \cap G_{l+1}), G_c)$. By assumption, $c - l$ is odd so, thanks to Corollary 10.2, the homomorphism $G_{c-l}/G_{c-l+1} \to \mathrm{Hom}(G_l/G_{l+1}, G_c)$, defined by $tG_{c-l} \mapsto (xG_{l+1} \mapsto [t, x])$, is surjective. By Lemma 10.5, the quotient G_l/G_{l+1} is elementary abelian and therefore the restriction map $\mathrm{Hom}(G_l/G_{l+1}, G_c) \to \mathrm{Hom}(HG_{l+1}/G_{l+1}, G_c)$ is surjective. The quotients HG_{l+1}/G_{l+1} and $H/(H \cap G_{l+1})$ being isomorphic, every homomorphism $H \to G_c$ is of the form $x \mapsto [t, x]$, for some $t \in G_{c-l}$, and thus, for each complement K of G_c in T, there exists $t \in G_{c-l}$ such that $K = \{[t, x]x : x \in H\} = \{txt^{-1} : x \in H\} = tHt^{-1}$. □

CHAPTER 11

The Most Intense Chapter

Let $p > 3$ be a prime number. We recall that a *p-obelisk* is a finite p-group G of class at least 2 that satisfies $G_3 = G^p$ and $|G : G_3| = p^3$. A p-obelisk G is *framed* if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$. Some theory about p-obelisks is developed in Chapter 10.

The main results of this chapter are summarized in Theorems 11.1 and 11.2, which are proven in Section 11.4.

Theorem 11.1. *Let $p > 3$ be a prime number and let G be a finite p-group of class 4. Let α be an automorphism of order 2 of G. Then the following conditions are equivalent.*

1. *The group G is a p-obelisk and the automorphism $G/G_2 \to G/G_2$ that is induced by α is equal to the inversion map $\overline{x} \mapsto \overline{x}^{-1}$.*
2. *The automorphism α is intense.*

An analogue of Theorem 11.1 for higher nilpotency classes is proven in Chapter 12: the next theorem gives an essential contribution to its proof.

Theorem 11.2. *Let $p > 3$ be a prime number and let G be a framed p-obelisk. Let α be an automorphism of order 2 of G and assume that the automorphism $G/G_2 \to G/G_2$ that is induced by α is equal to the inversion map $\overline{x} \mapsto \overline{x}^{-1}$. Then α is intense.*

We remark that the structure of Chapter 11 is quite rigid and is meant to ease the understanding of the strategy behind the proof of Theorem 11.2. We will prove Theorem 11.2 by induction on the nilpotency class c of the group G and we will separate the cases according to the parity of c. Propositions 11.3, 11.12, and 11.22 will be the building blocks of the whole theory and will be verified respectively in Sections 11.1, 11.2, and 11.3. We will use several results from Section 10.4 to understand the structure of the subgroups of G, according to the size of their intersection with G_c. Moreover, the arguments that we will apply will heavily depend on the knowledge of the jumps of each subgroup in G. For more detailed information about jumps, we refer to Section 2.3.

11.1. The even case

The next proposition is proven for any p-obelisk, where p is a prime number greater than 3. We want to stress that, on the contrary, in Propositions 11.12 and 11.22 we ask for the p-obelisk to be framed.

Proposition 11.3. *Let $p > 3$ be a prime number and let G be a p-obelisk of class c. Assume that c is even. Let moreover α be an automorphism of G of order*

2 and assume that the map $\alpha_c : G/G_c \to G/G_c$ that is induced by α is intense. Then α is intense.

We will prove Proposition 11.3 at the end of the present section. To this end, let G, c, and α be as in Proposition 11.3: then, Lemma 10.4(4) yields that G_c has order p. Set moreover $A = \langle\alpha\rangle$ and let H be a subgroup of G: we will show that H has an A-stable conjugate. Since the case in which H contains G_c follows directly from the intensity of α_c and Lemma 3.5, we assume, wihout loss of generality, that $H \cap G_c = \{1\}$ and that H is non-trivial. Then, as a consequence of Corollary 10.2, all jumps of H in G are odd. We will work under these assumptions until the end of Section 11.1.

Lemma 11.4. *Define $T = HG_c$ and assume that $\alpha(T) = T$. Then, for each subgroup K of T, one has $\alpha(KG_c) = KG_c$. Moreover, for each $x \in H$, there exists $\gamma \in G_c$ such that $\alpha(x) = x^{-1}\gamma$ and $\alpha(\gamma) = \gamma$.*

Proof. The $\langle\alpha_c\rangle$-stable subgroup T/G_c having only odd jumps, Lemma 2.17 yields that each element of T/G_c is inverted by α_c. In particular, every subgroup of T/G_c is $\langle\alpha_c\rangle$-stable and thus KG_c is A-stable. Every element of $G \setminus G_2$ being inverted by α modulo G_c, it follows from Lemma 2.5 that α restricts to the identity map on G_c. □

Lemma 11.5. *Let l be the least jump of H and assume that all jumps of H in G have the same width. Assume moreover that $\alpha(HG_c) = HG_c$. Then there exists $g \in G_{c-l}$ such that gHg^{-1} is A-stable.*

Proof. Define $T = HG_c$. All jumps of H in G are odd and H is abelian, by Lemma 10.19(1). Then, the subgroup G_c being central, one has $T = H \oplus G_c$. As a consequence, $T = \alpha(T) = \alpha(H) \oplus G_c$ and $\alpha(H)$ is a complement of G_c in T. By Lemma 10.19(2), the Frattini subgroup of H is equal to $H \cap G_{l+1}$ so it follows from Lemma 10.20 that there exists $t \in G_{c-l}$ such that $\alpha(H) = tHt^{-1}$. Thanks to Lemma 3.5, there exists $g \in G_{c-l}$ such that gHg^{-1} is A-stable. □

Lemma 11.6. *Assume that all jumps of H in G have the same width. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. Denote $T = HG_c$. Then there exists $a \in G$ such that aTa^{-1} is A-stable. Write $T' = aTa^{-1}$ and $H' = aHa^{-1}$. Then $T' = H'G_c$ and, thanks to Lemma 11.5, there exists $b \in G$ such that $bH'b^{-1}$ is A-stable. To conclude, define $g = ba$. □

Lemma 11.7. *There exists $g \in G$ such that gHg^{-1} is A-stable.*

We devote the remaining part of this section to the proof of Lemma 11.7. To this end, write $T = HG_c$. In view of Lemma 11.6, we assume without loss of generality that the jumps of H in G do not all have the same width. As a consequence of Proposition 10.3(1), each jump of H in G will have width 1 or 2, so we denote by l and j respectively the least jump of width 1 and the least jump of width 2 of H in G. It follows from our assumptions that the following are satisfied.

i. If $i, h \in \mathbb{Z}_{>0}$ are such that $\mathrm{wt}_H^G(i) = 1$ and that $\mathrm{wt}_H^G(h) = 2$, then $i < h$.
ii. One has $l < j$ and $j + l > c$.
iii. The subgroup H is abelian.

Lemma 11.8. *There exist cyclic subgroups J and L of H such that $H = J \oplus L$ and j and l are respectively the least jump of J and the least jump of L in G.*

Proof. The smallest jump of H in G is l so, thanks to Lemma 2.16, there is an element z in H with $\mathrm{dpt}_G(z) = l$. Define $L = \langle z \rangle$. Then L is a subgroup of H and l is the least jump of L in G. Moreover, thanks to Lemma 10.16, all jumps of L are odd and of width 1 in G and, since $l < j$, Corollary 10.2 ensures that j is a jump of L in G. However, j is a jump of width 2 of H, and thus there exists an element x in $H \setminus L$ such that $\mathrm{dpt}_G(x) = j$. Define $J = \langle x \rangle$. The group H being abelian, Corollary 10.2 yields $L \cap J = \{1\}$. Now, every jump $l \leq i < j$ of L in G is also a jump of H and it has width 1. Moreover, each jump $j \leq i < c$ of $J \oplus L$ is a jump of width 2 of H. Corollary 10.2 guarantees that all odd integers $l \leq i < c$ are jumps of H in G, so Lemma 2.16 yields

$$|J \oplus L| = \prod_{i=l}^{c-1} p^{\dim_{J\oplus L}^G(i)} = \prod_{i=l}^{c-1} p^{\dim_H^G(i)} = |H|.$$

□

Lemma 11.9. *Let J and L be as in Lemma* 11.8. *Assume that $\alpha(T) = T$. Then there exists $g \in G_{c-l}$ such that the following hold.*

1. *The group gLg^{-1} is A-stable.*
2. *One has $gTg^{-1} = T$ and $gJg^{-1} = J$.*

Proof. We define $R = LG_c$. By Lemma 11.4, the group R is A-stable. The subgroup L is cyclic so, by Lemma 10.16, all its jumps in G are odd and of width 1. With L in the role of H, it follows from Lemma 11.5 that there exists $g \in G_{c-l}$ such that gLg^{-1} is A-stable. We fix such an element g and prove that g normalizes both J and T. The least jump of J being j, one has that $[g, J] = \{[g, x] : x \in J\}$ is contained in $[G_{c-l}, G_j]$. Moreover, $[g, L]$ is contained in $G_{c-l+j} \subseteq G_{c+1} = \{1\}$ and so g centralizes J. To conclude, since T is contained in G_l, the set $[g, T]$ is contained in $[G_{c-l}, G_l] \subseteq G_c$ and hence g normalizes T. □

Lemma 11.10. *Let J and L be as in Lemma* 11.8. *Assume that $\alpha(T) = T$ and $\alpha(L) = L$. Then there exists $g \in G_{c-j}$ such that gHg^{-1} is A-stable.*

Proof. We will construct g. Let $x, z \in H$ be such that $J = \langle x \rangle$ and $L = \langle z \rangle$: then, by Lemma 11.8, one has $\mathrm{dpt}_G(x) = j$ and $\mathrm{dpt}_G(z) = l$. Let moreover $\gamma \in G_c$ be such that $\alpha(x) = x^{-1}\gamma$ and $\alpha(\gamma) = \gamma$, as given by Lemma 11.4. Define $m = (j+l-c)/2$. By Lemma 10.5, there exists a of depth $c-j$ in G such that $\rho^m(a) = z$. We fix a and remark that a belongs to $\mathrm{C}_G(L)$. Since $\mathrm{wt}_G(j) = 2$, it follows from Lemma 10.11 that there exists $s \in \mathbb{Z}$ such that $[a^s, x] = \gamma^{\frac{p-1}{2}}$. We define $g = a^s$ and claim that gHg^{-1} is A-stable. We recall that γ belongs to the central subgroup G_c and that the exponent of G_c is p: it follows that $\alpha(gxg^{-1}) = (gxg^{-1})^{-1}$ and so gJg^{-1} is A-stable. Moreover, g centralizes L and therefore $gHg^{-1} = gJg^{-1} \oplus L$. As a consequence, gHg^{-1} is itself A-stable. □

Lemma 11.11. *Let J and L be as in Lemma* 11.8. *Assume that $\alpha(T) = T$. Then there exists $g \in G_{c-j}$ such that gHg^{-1} is A-stable.*

Proof. As a consequence of Lemma 11.9, there exists $a \in G_{c-l}$ such that aLa^{-1} is A-stable, $aTa^{-1} = T$, and $aHa^{-1} = J \oplus aLa^{-1}$. We fix such a and we take $h \in G_{c-j}$ making $h(aHa^{-1})h^{-1}$ stable under the action of A. With H replaced by aHa^{-1}, Lemma 11.10 guarantees the existence of h. We conclude by defining $g = ha$, which belongs to $G_{c-j}G_{c-l} = G_{c-j}$. □

To conclude the proof of Lemma 11.7, let $b \in G$ be such that bTb^{-1} is A-stable and note that such element b exists because T contains G_c. Lemma 11.11, with H replaced by bHb^{-1}, provides an element $a \in G$ such that $a(bHb^{-1})a^{-1}$ is A-stable. To conclude the proof of Lemma 11.7, we define $g = ab$. Now that Lemma 11.7 is proven, Lemma 3.5 yields that α is intense and, the choice of H being arbitrary, the proof of Proposition 11.3 is complete.

11.2. The odd case, part I

In Proposition 11.12 an additional assumption compared to Proposition 11.3 is made: that G be a *framed* p-obelisk. We recall that, if p is a prime number, then a p-obelisk G is framed if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$. We refer to Section 10.3 for useful facts related to framed p-obelisks.

Proposition 11.12. *Let $p > 3$ be a prime number and let G be a framed p-obelisk of class c. Assume that c is odd and that G_c has order p. Let α be an automorphism of G of order 2 and assume that the map $\alpha_c : G/G_c \to G/G_c$ that is induced by α is intense. Then α is intense.*

The goal of this section is to give the proof of Proposition 11.12 so we will keep the following assumptions until the end of Section 11.2. Let $p > 3$ be a prime number and let G be a p-obelisk of class c. Assume that c is odd and that G_c has order p. Let moreover α be an automorphism of G of order 2 and assume that the map $\alpha_c : G/G_c \to G/G_c$ that is induced by α is intense. Set $A = \langle\alpha\rangle$ and, in concordance with Section 2.2, write $G^+ = \{x \in G : \alpha(x) = x\}$ and $G^- = \{x \in G : \alpha(x) = x^{-1}\}$. For a subgroup H of G, we denote $H^+ = H \cap G^+$ and $H^- = H \cap G^-$ and we use the same "plus-minus" notation for any subgroup of G/G_c with respect to α_c. We have intentionally not yet asked for G to be framed: we will make such assumption right after stating Lemma 11.16.

Let H be a subgroup of G: we will show that H has an A-stable conjugate. If H contains G_c, then Lemma 3.5 guarantees the existence of $g \in G$ such that $(gHg^{-1})/G_c$ is $\langle\alpha_c\rangle$-stable: then gHg^{-1} is A-stable. We assume thus, without loss of generality, that $H \cap G_c = \{1\}$ and that H is non-trivial.

Lemma 11.13. *All jumps of H in G have width 1.*

Proof. As a consequence of Proposition 10.3(1), every jump of H in G has width at most 2. Assume by contradiction that l is a jump of H in G of width 2. The jump l is odd, thanks to Lemma 10.4(1), and $G_l/G_{l+1} = (H \cap G_l)G_{l+1}/G_{l+1}$. Looking at $\rho_l^{(c-l)/2} : G_l/G_{l+1} \to G_c$, it follows from Lemma 10.10(1) that $H \cap G_c \neq \{1\}$. Contradiction. □

Lemma 11.14. *Assume that all jumps of H in G are even. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. All jumps of H in G are even so, by Lemma 11.13, they also all have width 1. Let now l be the least jump of H in G. Then, by Lemma 10.18, the subgroup H is cyclic and, by Lemma 10.19, the subgroups $\Phi(H)$ and $H \cap G_{l+1}$ are the same. Let $T = H \oplus G_c$. Assume first that $\alpha(T) = T$. Then $T = \alpha(H) \oplus G_c$

and, by Lemma 10.20, there exists $t \in G$ such that $\alpha(H) = tHt^{-1}$. Thanks to Lemma 3.5, there exists thus $t \in G$ such that tHt^{-1} is A-stable. In general, since T contains G_c, there exists $a \in G$ such that aTa^{-1} is A-stable and so we are done. □

LEMMA 11.15. *Assume that all jumps of H in G are odd. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

PROOF. Let $T = HG_c$. The class of G being odd, it follows that all jumps of T in G are odd. Moreover, since T contains G_c, there exists $g \in G$ such that gTg^{-1} is A-stable. By Lemma 2.16, the subgroups gTg^{-1} and T have the same jumps in G so Lemma 2.17 yields $gTg^{-1} = (gTg^{-1})^-$. In particular, $gHg^{-1} = (gHg^{-1})^-$ and gHg^{-1} is A-stable. □

LEMMA 11.16. *Assume that G is framed. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

The remaining part of Section 11.2 will be entirely dedicated to the proof of Lemma 11.16. For this purpose, all assumptions that we now make will hold until the end of the very same section.

Assume that G is a framed p-obelisk. Moreover, in view of Lemmas 11.14 and 11.15, assume that H has jumps of each parity and define i and j respectively to be the least odd jump and the least even jump of H in G. Write $T = HG_c$.

LEMMA 11.17. *The following hold.*

1. *One has $i + j > c$.*
2. *The subgroups H and T are abelian.*

PROOF. The numbers i and j having different parities, their sum $m = i + j$ is odd. Let $k = \max\{i, j\}$. Then, as a consequence of Lemma 11.13, all jumps of H in G that are smaller than k have width 1 and so, by Lemma 10.17, the group $H/(H \cap G_k)$ is cyclic. Then $[H, H] = [H, H \cap G_k]$ and so $[H, H]$ is contained in G_m. If $m > c$, then $G_m \subseteq G_{c+1} = \{1\}$, and thus (1) and (2) are proven. Assume by contradiction that $m \leq c$ and let y and x be elements of H respectively of depth i and j in G. Then the image of $\langle y \rangle$ under the natural projection $G \to G/G_{i+1}$ is a 1-dimensional subspace of G_i/G_{i+1}. Thanks to Proposition 10.14(3), with $h = i$ and $k = j$, the elements $y^{p^{j/2}}$ and $[y, x]$ of H span G_m/G_{m+1}. It follows from Lemma 11.13 that m is a jump of H of width 1 in G so, from Lemma 10.4(1), we derive $m = c$. Contradiction to H trivially intersecting G_c. □

LEMMA 11.18. *Let $\pi : G \to G/G_c$ denote the natural projection. Assume that $\alpha(T) = T$. Then $\pi(H)$ is $\langle \alpha_c \rangle$-stable and $\pi(H) = \pi(H)^+ \oplus \pi(H)^-$. Moreover, both $\pi(H)^+$ and $\pi(H)^-$ are cyclic.*

PROOF. To lighten the notation, we will denote $\overline{G} = \pi(G)$ and we will use the bar notation for the subgroups of $\overline{G}$. By assumption, $\alpha(T) = T$ and thus $\alpha_c(\overline{T}) = \overline{T}$. Moreover, $\overline{H}$ is equal to $\overline{T}$, so $\overline{H}$ is itself $\langle \alpha_c \rangle$-stable. As a consequence of Lemma 11.17(2), the group $\overline{H}$ is abelian so, by Corollary 2.2, it decomposes as $\overline{H} = \overline{H}^+ \oplus \overline{H}^-$. It follows from Lemma 2.17 that $\overline{H}^+$ and $\overline{H}^-$ have respectively only even jumps and only odd jumps in $\overline{G}$. Moreover, thanks to Lemma 11.13, all jumps of $\overline{H}$, and thus of its subgroups, in $\overline{G}$ have width 1. Lemma 10.17 yields that both $\overline{H}^+$ and $\overline{H}^-$ are cyclic. □

Lemma 11.19. *Assume that $\alpha(T) = T$. Then there exist cyclic subgroups I and J of H, with least jumps in G respectively equal to i and j, such that the following hold.*

1. *One has $H = I \oplus J$.*
2. *The group I is A-stable and $I = I^-$.*
3. *The group $S = J \oplus G_c$ is A-stable and $S = S^+ \oplus G_c$.*

Proof. We denote $\overline{G} = G/G_c$ and we will use the bar notation for the subgroups of $\overline{G}$. By Lemma 11.18, the subgroup $\overline{H}$ is $\langle \alpha_c \rangle$-stable and it decomposes as $\overline{H} = \overline{H}^+ \oplus \overline{H}^-$, where both $\overline{H}^+$ and $\overline{H}^-$ are cyclic. Let R and S be subgroups of G, containing G_c, such that $\overline{S} = \overline{H}^+$ and $\overline{R} = \overline{H}^-$. Because of their definitions, both R and S are A-stable. The subgroup G_c is contained in G^- as a consequence of Lemma 2.5, so it follows from Lemma 2.12 that $R = R^-$. Moreover, by Corollary 2.2, one has $S = S^+ \oplus S^-$. However, as $\overline{S} = \overline{S}^+$, the subgroups S^- and G_c are equal, and hence $S = S^+ \oplus G_c$. We define $I = H \cap R$ and $J = H \cap S$. The subgroup I, being contained in $R = R^-$, is itself A-stable and $I = I^-$. Moreover, one has $JG_c = (H \cap S)G_c = S \cap (HG_c) = S$ and so, since $H \cap G_c = \{1\}$, we get $S = J \oplus G_c$. In the same way, we have $R = I \oplus G_c$. It follows that J and I are respectively isomorphic to $\overline{H}^+$ and $\overline{H}^-$, and therefore they are cyclic. We conclude by observing that

$$\overline{I \oplus J} = \overline{I} \oplus \overline{J} = \overline{R} \oplus \overline{S} = \overline{H}^+ \oplus \overline{H}^- = \overline{H},$$

and therefore $H = I \oplus J$. □

Lemma 11.20. *Let $\gamma \in G_c$ and let x, y be elements of G be such that $\mathrm{dpt}_G(x) = j$ and $\mathrm{dpt}_G(y) = i$. Then there exist $n \in \mathbb{Z}$ and $d \in \mathrm{C}_G(y) \cap G_{c-j}$ such that $\gamma = y^n[d, x]$.*

Proof. By Lemma 11.17 the sum $i+j$ is larger than c and so $i > c-j$. Define

$$r = \frac{i-(c-j)}{2} \quad \text{and} \quad s = \frac{j}{2} - r.$$

Let now $a \in G_{c-j} \setminus G_{c-j+1}$ be such that $\rho^r(a) = y$; the existence of a is granted by Lemma 10.5. As a consequence of Proposition 10.14, the subgroup G_c is generated by $\rho^{\frac{j}{2}}(a)$ and $[a, x]$. There exist thus $A, B \in \mathbb{Z}$ such that

$$\gamma = \rho^{\frac{j}{2}}(a)^A [a, x]^B.$$

We recall that, for any $k \in \mathbb{Z}_{\geq 0}$, the map ρ^k is given by $z \mapsto z^{p^k}$, hence

$$\rho^{\frac{j}{2}}(a) = \rho^{s+r}(a) = \rho^s(\rho^r(a)) = \rho^s(y) = y^{p^s}.$$

The commutator map $G_{c-j} \times G_j \to G_c$ being bilinear, we have moreover that $[a, x]^B = [a^B, x]$. We define

$$n = Ap^s \quad \text{and} \quad d = a^B$$

and get $\gamma = y^n[d, x]$. The element d belongs to $\mathrm{C}_G(y)$, because d and y belong to $\langle a \rangle$. □

Lemma 11.21. *Assume that $\alpha(T) = T$. Let I and J be as in Lemma 11.19. Then there exists $g \in \mathrm{C}_G(I)$ such that $\alpha(gJg^{-1}) \subseteq gHg^{-1}$.*

PROOF. Let y be a generator of I and let x be a generator of J: then $\mathrm{dpt}_G(y) = i$ and $\mathrm{dpt}_G(x) = j$. Let moreover $\gamma \in G_c$ be such that $\alpha(x) = x\gamma$, as given by Lemma 11.19(3), and let $n \in \mathbb{Z}$ and $d \in \mathrm{C}_G(y) \cap G_{c-j}$ be such that $\gamma = y^n[d, x]$, as in Lemma 11.20. We define $g = d^{\frac{p+1}{2}}$ and we claim that $\alpha(gxg^{-1})$ belongs to gHg^{-1}. We will use some properties of G_c that we list here. The group G_c is central and annihilated by p, by hypothesis. Moreover, as a consequence of Lemma 2.5, the restriction of α to G_c coincides with the map $z \mapsto z^{-1}$. The commutator map $G_{c-j} \times G_j \to G_c$ being bilinear, we compute

$$\alpha(gxg^{-1}) = \alpha([g, x]x) = \alpha([g, x])\alpha(x) = [g, x]^{-1}x\gamma = [g^{-1}, x]x\gamma =$$
$$[g^{-1}, x]xy^n[d, x] = [g^{-1}, x][d, x]xy^n = [g^{-1}d, x]xy^n = [d^{\frac{p-1}{2}}d, x]xy^n =$$
$$[d^{\frac{p+1}{2}}, x]xy^n = [g, x]xy^n = (gxg^{-1})y^n.$$

The element g centralizes y, because d does, so $\alpha(gxg^{-1}) = g(xy^n)g^{-1}$ belongs to gHg^{-1}. In particular, $\alpha(gJg^{-1}) \subseteq gHg^{-1}$. □

We conclude the proof of Lemma 11.16. Since T contains G_c, there exists $a \in G$ such that aTa^{-1} is A-stable. We fix a and write $aHa^{-1} = I \oplus J$, with I and J as in Lemma 11.19 and H replaced by aHa^{-1}. By Lemma 11.21, there exists an element $b \in G$ such that $bIb^{-1} = I$ and $\alpha(bJb^{-1})$ is contained in $baHa^{-1}b^{-1}$. We select such an element b and define $g = ba$. Then I is contained in gHg^{-1} and $\alpha(gHg^{-1}) = I \oplus \alpha(bJb^{-1}) \subseteq gHg^{-1}$. It follows that $\alpha(gHg^{-1}) = gHg^{-1}$ and gHg^{-1} is itself A-stable. The proof of Lemma 11.16 is now complete and thus, as a consequence of Lemma 3.5, Proposition 11.12 is also proven.

11.3. The odd case, part II

The present section is entirely dedicated to the proof of Proposition 11.22.

PROPOSITION 11.22. *Let $p > 3$ be a prime number and let G be a framed p-obelisk of class c. Assume that c is odd and that G_c has order p^2. Let α be an automorphism of G of order 2 and assume that the map $\alpha_c : G/G_c \to G/G_c$ that is induced by α is intense. Then α is intense.*

Until the end of Section 11.3, we will work under the following assumptions. Let $p > 3$ be a prime number and let G, c, and α be as in Proposition 11.22. Denote $A = \langle \alpha \rangle$. Let moreover H be a subgroup of G: we will show that H is stable under the action of A.

If the subgroup H contains G_c, then the intensity of α and Lemma 3.5 yield the existence of $g \in G$ such that gHg^{-1} is A-stable. We assume without loss of generality that H does not contain G_c.

LEMMA 11.23. *Assume that $H \cap G_c \neq \{1\}$. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

PROOF. Let $N = H \cap G_c$. The group N being non-trivial, it follows from Proposition 10.3(1) that G_c and N have orders respectively p^2 and p. Moreover, the group G_c being central, N is normal in G. It follows from Lemma 3.2(2) that the action of A on G induces an action of A on $\overline{G} = G/N$. Moreover, $\overline{G}$ has class c and the subgroup $\overline{H} = H/N$ has trivial intersection with $\overline{G_c} = G_c/N$. By Lemma 11.16, there exists $g \in G$ such that $\overline{gHg^{-1}}$ is A-stable, and so gHg^{-1} is A-stable. □

Lemma 11.24. *Assume that $H \cap G_c = \{1\}$. Let $T = HG_c$ and assume that $\alpha(T) = T$. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. Let l denote the least jump of H in G. As a consequence of Corollary 10.2, all jumps of H in G are even so, as a consequence of Lemma 10.4(2), all jumps of H have width 1. It follows from Lemma 10.19 that H is abelian and $\Phi(H) = H \cap G_{l+1}$. The subgroup G_c being central, we get $T = H \oplus G_c$. Now, by Lemma 2.17, the subgroup $T^+ = \{t \in T : \alpha(t) = t\}$ has the same jumps as H, and it is therefore a complement of G_c in T. Thanks to Lemma 10.20, the subgroups H and T^+ are conjugate in G. In particular, H has an A-stable conjugate. □

Lemma 11.25. *Assume that $H \cap G_c = \{1\}$. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. Define $S = HG_c$ so that there exists $a \in G$ such that aSa^{-1} is A-stable. Let now $T = aSa^{-1}$. Then $\alpha(T) = T$ and $T = a(HG_c)a^{-1} = aHa^{-1}G_c$. Moreover, the intersection $aHa^{-1} \cap G_c$ is trivial. Thanks to Lemma 11.24 (with aHa^{-1} in the place of H), there exists $b \in G$ such that $b(aHa^{-1})b^{-1}$ is A-stable. To conclude, we define $g = ba$. □

We conclude here the proof of Proposition 11.22. If H trivially intersects G_c, then, by Lemma 11.25, there exists $g \in G$ such that gHg^{-1} is A-stable. If, on the contrary, $H \cap G_c \neq \{1\}$, then, by Lemma 11.23, there exists a conjugate of H in G that is A-stable. We have proven that, in any case, H has an A-stable conjugate and, by Lemma 3.5, the subgroups H and $\alpha(H)$ are conjugate in G. The choice of H being arbitrary, the automorphism α is intense and we have proven Proposition 11.22.

11.4. Proving the main theorems

In Sections 11.4.1 and 11.4.2 we finally prove the two main results of this Chapter, which were stated at the beginning of it.

11.4.1. The proof of Theorem 11.1. We work under the assumptions of Theorem 11.1. The implication (2) ⇒ (1) follows from the combination of Propositions 10.1 and 5.10. We now prove (1) ⇒ (2). To this end, denote by $\overline{G}$ the quotient G/G_4 and by α_4 the automorphism of $\overline{G}$ that is induced by α. The map α induces the inversion map on G/G_2 and thus so does α_4 on $\overline{G}/\overline{G}_2$. It follows from Proposition 5.11 that α_4 is intense and consequently, from Proposition 11.3, that α is intense too. The proof of Theorem 11.1 is complete.

11.4.2. The proof of Theorem 11.2. Under the hypotheses of Theorem 11.2, we will work by induction on the class c of G. As a consequence of Lemma 10.2(2), the group G has class at least 2 and G/G_3 is extraspecial of exponent p. If $c = 2$, then Lemma 4.10 yields that α is intense. We assume that $c > 2$ and denote by $\overline{G}$ the quotient G/G_c. We denote moreover by α_c the automorphism of $\overline{G}$ that is induced by α and assume that α_c is intense. The group $\overline{G}$ is a framed obelisk, because $c > 2$, and α_c induces the inversion map on $\overline{G}/\overline{G}_2$, because α does. If c is even, then, by Proposition 11.3, the map α is intense. Suppose that c is odd. From Proposition 10.3(1) it follows that the cardinality of G_c is p or p^2. In the first case we apply Proposition 11.12, in the second Proposition 11.22. Theorem 11.2 is now proven.

CHAPTER 12

High Class Intensity

Let $p > 3$ be a prime number and let G be a finite p-group. We recall that, for each positive integer i, the *i-th width* of G is $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$. The group G is a *p-obelisk* if it is non-abelian, satisfying $G_3 = G^p$ and $|G : G_3| = p^3$. A p-obelisk G is *framed* if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$. For more information about p-obelisks, we refer to Chapter 10.

In this chapter we prove the following two results: the first will be proven in Section 12.2, while the second is proven at the end of Chapter 12.

Theorem 12.1. *Let p be a prime number and let G be a finite p-group with $\mathrm{wt}_G(5) = 1$. In addition, write $C = \mathrm{C}_G(G_4)$. Then the following are equivalent.*

1. *One has $\mathrm{int}(G) > 1$.*
2. *One has $p > 3$, the group G is a p-obelisk of class 5, and $\Phi(C) = G_3$. Moreover, there exists an automorphism α of G of order 2 that induces the inversion map on G/G_2.*

Theorem 12.2. *Let p be a prime number and let G be a finite p-group with $\mathrm{wt}_G(5) = 2$. Then the following are equivalent.*

1. *One has $\mathrm{int}(G) > 1$.*
2. *One has $p > 3$, the group G is a framed p-obelisk, and there exists an automorphism α of G of order 2 that induces the inversion map on G/G_2.*

We would like to stress that, from the combination of Theorem 12.1 with Theorem 12.2, it follows that each finite p-group G of class at least 6 with $\mathrm{int}(G) > 1$ is a framed p-obelisk.

12.1. A special case

The main result of this section is the following.

Proposition 12.3. *Let $p > 3$ be a prime number and let G be a p-obelisk such that $\mathrm{wt}_G(5) = 1$ and $\mathrm{int}(G) > 1$. Set $C = \mathrm{C}_G(G_4)$. Then one has $\Phi(C) = G_3$.*

The goal of Section 12.1 is proving Proposition 12.3, so all assumption that we will make throughout the text (right now and right after Lemma 12.4) will hold until the end of Section 12.1.

Let $p > 3$ be a prime number and let G be a p-obelisk. Let $(G_i)_{i \geq 1}$ denote the lower central series of G. Assume that $\mathrm{wt}_G(5) = 1$ so, thanks to Proposition 10.3(2), the class of G is equal to 5. Write $C = \mathrm{C}_G(G_4)$.

Lemma 12.4. *The subgroup C is maximal in G and C^p is contained in $\mathrm{Z}(C)$.*

Proof. To show that C is maximal in G is an easy exercise, so we prove that C^p is central in C. Corollary 10.2 ensures that 3 is a 1-dimensional jump of C^p in G and so, the subgroup C^p being normal in G, Lemma 10.9(2) yields $G_4 \subseteq C^p \subseteq G_3$. Thanks to Lemma 10.4(2), we get $|G_3 : C^p| = |C^p : G_4| = p$. Now, each p-obelisk is regular, by Lemma 10.2, so, as a consequence of Lemma 10.6, one has $[C^p, G_2] = [C, G_2^p]$, which is equal to $[C, G_4] = \{1\}$, by Lemma 10.5. It follows that the commutator map $C \times C^p \to G_4$ factors as a bilinear map $\gamma : C/G_2 \times C^p/G_4 \to G_4$. Moreover, thanks to Corollary 10.2, if $C = \langle \{x\} \cup G_2 \rangle$ then $C^p = \langle \{x^p\} \cup G_4 \rangle$. The map γ being alternating, it follows that γ is the trivial map and so C^p centralizes C. □

Let now α be an intense automorphism of G of order 2 and write $A = \langle \alpha \rangle$. In concordance with the notation from Section 2.2, set $G^+ = \{x \in G : \alpha(x) = x\}$ and $G^- = \{x \in G : \alpha(x) = x^{-1}\}$ and, for each subgroup H of G, denote $H^+ = H \cap G^+$ and $H^- = H \cap G^-$. Let X be the collection of subgroups H of C of the form $H = \langle x, y \rangle$, where $x \in C \setminus G_2$ and $y \in G_4 \setminus G_5$, and let X^+ be the collection of fixed points of X under the action of A. We will prove Proposition 12.3 *by contradiction* and, to this end, we assume that $\Phi(C) \neq G_3$.

Lemma 12.5. *Let $H \in X$. Then H is abelian of exponent p^2 and $H \cap G_5 = \{1\}$. Moreover, if x and y are elements of H satisfying $\mathrm{dpt}_G(x) = 1$ and $\mathrm{dpt}_G(y) = 4$, then $H = \langle x \rangle \oplus \langle y \rangle$.*

Proof. We first claim that the exponent of C divides p^2. By Lemma 10.13, we have $[C, C] = C^p$ so it follows from Lemma 10.6 that $(C^p)^p = [C, C]^p = [C, C^p]$. As a consequence of Lemma 12.4, the subgroup $[C, C^p]$ is trivial, and thus $C^{p^2} \subseteq (C^p)^p = \{1\}$. This proves the claim. Let now $(x, y) \in (C \setminus G_2) \times (G_4 \setminus G_5)$ be such that $H = \langle x, y \rangle$. Then $y \in \mathrm{Z}(C)$ and the group H is commutative. Moreover, as a consequence of Lemma 6.5, the subgroups $\langle x \rangle$ and $\langle y \rangle$ have respectively only odd and only even jumps. In particular, $\langle x \rangle \cap \langle y \rangle = \{1\}$ and $H = \langle x \rangle \oplus \langle y \rangle$. In addition, it follows from Lemma 10.10(1) that 5 is a jump of H in G if and only if $x^{p^2} \neq 1$. We have thus $H \cap G_5 = \{1\}$ and, as a consequence of Corollary 10.2, the exponent of H is p^2. □

Lemma 12.6. *Let $H \in X$ and, for each $i \in \mathbb{Z}_{\geq 1}$, denote $u_i = \mathrm{wt}_H^G(i)$. Then H has order p^3 and $(u_1, u_2, u_3, u_4, u_5) = (1, 0, 1, 1, 0)$.*

Proof. For each $i \in \mathbb{Z}_{\geq 1}$, write $w_i = \mathrm{wt}_G(i)$. Thanks to Lemma 10.4, we have $(w_1, w_2, w_3, w_4, w_5) = (2, 1, 2, 1, 1)$. Let x, y be as in Lemma 12.5: then $u_1, u_4 \geq 1$ and $u_5 = 0$. Since, for each $i \geq 1$, one has $u_i \leq w_i$, we get $u_4 = 1$. Moreover, Lemma 10.10(1) ensures that $u_3 \geq 1$. Let now $N = \langle y \rangle G_5$, which is a normal subgroup of G thanks to Lemma 10.9. Then $N \cap H = \langle y \rangle$ and, the quotient $H/\langle y \rangle$ being cyclic, so is HN/N. Thanks to Lemma 10.16, all jumps of HN/N have the same dimension and width 1 in G/N. As a result, 2 is not a jump of HN/N in G/N and, since $\langle y \rangle$ is contained in G_4, we have $u_2 = 0$ and $u_1 = u_3 = 1$. The group H has order p^3, by Lemma 2.16. □

Lemma 12.7. *The cardinality of X is p^4.*

Proof. Thanks to Lemma 12.5, the set X consists of subgroups of the form $\langle x \rangle \oplus \langle y \rangle$, with $x \in C \setminus G_2$ and $y \in G_4 \setminus G_5$. The cardinality of X will be thus equal to the quotient $\frac{n}{m}$, where n is the cardinality of $(C \setminus G_2) \times (G_4 \setminus G_5)$ and m denotes the number of elements of $(C \setminus G_2) \times (G_4 \setminus G_5)$ that generate the same subgroup. Let H be in X and let x and y be generators of H, as described before. Then, as a consequence of Lemmas 12.5 and 12.6, the orders of x and y are respectively p^2 and p. It follows that $m = (p^3 - p^2)(p - 1)$ so, in view of Lemmas 12.6 and 10.2, we get

$$|X| = \frac{n}{m} = \frac{(p^6 - p^5)(p^2 - p)}{(p^3 - p^2)(p - 1)} = p^4.$$

□

Lemma 12.8. *Let $H \in X$. Then the following are equivalent.*

1. *The subgroup H is A-stable.*
2. *There exists $x \in C^- \setminus G_2$ such that $H = \langle x \rangle \oplus G_4^+$.*

Proof. To prove that (2) implies (1) is an easy exercise; we prove the other implication. Assume (1). The group H is abelian, by Lemma 12.5, and it is A-stable. By Corollary 2.2, it decomposes as $H = H^+ \oplus H^-$. In view of Lemmas 12.6 and 2.17(1), we have that $H^+ = G_4^+$ and that $H \cap G_4 = G_4^+$. It follows from Lemma 12.5 that there exists a cyclic subgroup Q of H such that $H = Q(H \cap G_4)$, and thus H^- is cyclic. The proof is now complete. □

Lemma 12.9. *The cardinality of X^+ is p^2.*

Proof. Let $\mathcal{C}$ denote the collection of subgroups $\langle x \rangle$ of C, where x is an element of $C^- \setminus G_2$. Thanks to Lemma 12.8, one can define the map $\mathcal{C} \to X^+$, by $Q \mapsto Q \oplus G_4^+$, which is easily shown to be a bijection. In particular, the cardinality of X^+ is equal to that of $\mathcal{C}$. Now, the group C is normal in G, as a consequence of Lemma 12.4, and therefore it is A-stable. Thanks to Lemma 12.5, each element of $C^- \setminus G_2$ has order p^2 and, as a consequence of Proposition 5.10, the set $C^- \setminus G_2$ is equal to $C^- \setminus G_3^-$. It follows from Lemma 2.17 that

$$|X^+| = \frac{|C^-| - |G_3^-|}{p^2 - p} = \frac{p^4 - p^3}{p^2 - p} = p^2.$$

□

Lemma 12.10. *Let $H \in X^+$. Then $G_3 \subseteq \mathrm{N}_G(H)$.*

Proof. By Lemma 12.8, the subgroup H is of the form $\langle x \rangle \oplus G_4^+$, for some element $x \in C^- \setminus G_2$. Moreover, Since $[G_3, G_4^+] \subseteq G_7 = \{1\}$, we have that $[G_3, H] = [G_3, \langle x \rangle]$. Now, the commutator map $\langle x \rangle \times G_3 \to G_4$ is bilinear and, since x belongs to C, it factors as $\langle x \rangle \times G_3/G_4 \to G_4$. Thanks to Proposition 5.10, the map α induces the inversion map on G_3/G_4 and so, thanks to Lemma 2.4, we get $[\langle x \rangle, G_3] = [\langle x \rangle, G_3]^+$. In particular, $[G_3, \langle x \rangle]$ is contained in G_4^+, a subgroup of H, and so G_3 normalizes H. □

We will now prove Proposition 12.3 by building a contradiction. We remind the reader that we have assumed that $\Phi(C) \neq G_3$.

Let H be an element of X^+ with the property that $|G : \mathrm{N}_G(H)|$ is maximal. Let moreover $\mathcal{J}$ denote the collection of jumps of $\mathrm{N}_G(H)$ in G. As a consequence of Lemma 12.10, the normalizer of H contains HG_3. It follows from Lemma 12.6 that $\{1, 3, 4, 5\}$ is contained in $\mathcal{J}$ and, thanks also to Lemma 10.2(2), that

$|G:\mathrm{N}_G(H)| \leq |G:HG_3| = p^2$. Now, by Lemmas 12.7 and 12.9, the cardinalities of X and X^+ are respectively p^4 and p^2, so it follows from Lemma 3.6 that

$$p^4 = |X| \leq \sum_{K\in X^+} |G:\mathrm{N}_G(K)| \leq |X^+||G:\mathrm{N}_G(H)| \leq p^4,$$

and therefore $|G:\mathrm{N}_G(H)| = p^2$. In particular, we get $\mathrm{N}_G(H) = HG_3$ and $\mathcal{J} = \{1,3,4,5\}$. Moreover, again by Lemma 3.6, no two elements of X^+ are conjugate in G. As a consequence of Lemma 2.15, the subgroup G^+ is contained in $\mathrm{N}_G(H) = HG_3$ and so, thanks to Lemma 2.17(1), the number 2 is a jump of $\mathrm{N}_G(H)$ in G. Contradiction.

12.2. The last exotic case

The aim of Section 12.2 is that of exploring the last exotic case for what concerns the structure of finite p-groups of intensity greater than 1. As a consequence of Theorem 12.2, the finite p-groups of "high class" and intensity greater than 1 all need to be framed obelisks. Proposition 12.11, which coincides with Theorem 12.1, is the last result we present that still allows some "structural freedom" to p-obelisks of intensity greater than 1.

Proposition 12.11. *Let p be a prime number and let G be a finite p-group with $\mathrm{wt}_G(5) = 1$. Write $C = \mathrm{C}_G(G_4)$. Then the following are equivalent.*

1. *One has $\mathrm{int}(G) > 1$.*
2. *One has $p > 3$, the group G is a p-obelisk of class 5, and $\Phi(C) = G_3$. Moreover, there exists an automorphism α of G of order 2 that induces the inversion map on G/G_2.*

The remaining part of Section 12.2 will be devoted to the proof of Proposition 12.11 and we will thus work under its hypotheses.

Assume first (1). As a consequence of Proposition 3.7 and Corollary 9.5, the prime p is larger than 3 and so, thanks to Proposition 10.1, the group G is a p-obelisk which has class 5, as a consequence of Proposition 10.3. Thanks to Theorem 5.2(1), there exists an intense automorphism α of order 2 of G, which induces the inversion map on G/G_2 by Proposition 5.10. Proposition 12.3 yields $\Phi(C) = G_3$.

Assume now that $p > 3$, that G is a p-obelisk with $\mathrm{wt}_G(5) = 1$, and that $\Phi(C) = G_3$. Let moreover α be an automorphism of order 2 of G that induces the inversion map on G/G_2. We will prove (1). Set $A = \langle\alpha\rangle$ and, for each $i \in \mathbb{Z}_{\geq 1}$, denote $w_i = \mathrm{wt}_G(i)$. Thanks to Lemma 10.4, we have $(w_1,w_2,w_3,w_4,w_5) = (2,1,2,1,1)$ and so, thanks to Proposition 10.3(2), the class of G is equal to 5. We remind the reader that, for each $k \in \mathbb{Z}_{\geq 0}$, the map $G \to G$ sending x to x^{p^k} is denoted by ρ^k. Furthermore, by Lemma 10.2, the group G is regular and so, given any subgroup K of G, Lemma 8.3 yields that $\rho^k(K) = K^{p^k}$.

Lemma 12.12. *One has $\rho^2(C) = G_5$.*

Proof. The group C is maximal in G, by Lemma 12.4, and so, as a consequence of Lemma 10.2(2), the quotient C/G_2 is cyclic. Then $[C,C] = [C,G_2]$ and so, since $\Phi(C) = G_3$, Lemmas 10.6 and 10.10(1) yield $G_5 = \rho(G_3) = \rho(\Phi(C)) = \rho([C,C]C^p) = [C,G_2]^p\rho^2(C) = [C,G_4]\rho^2(C) = \rho^2(C)$. □

Let H be a subgroup of G and, for each $i \in \mathbb{Z}_{\geq 1}$, write $u_i = \mathrm{wt}_H^G(i)$. We will show that H has an A-stable conjugate in G. We assume, without loss of generality, that H is non-trivial. As a consequence of Theorem 11.1, the automorphism that α induces on G/G_5 is intense and so, if G_5 is contained in H, then there exists $g \in G$ such that gHg^{-1} is A-stable. Since G_5 has order p, we now assume that $H \cap G_5 = \{1\}$. By Lemma 11.13, all jumps of H in G have dimension 1 and, if they all have the same parity, Lemmas 11.14 and 11.15 yield that H has an A-stable conjugate. We assume now that H has jumps of both parities and we denote by i and j respectively the least odd and the least even jump of H in G. It then follows from Corollary 10.2 that $u_4 = 1$.

Lemma 12.13. *One has $i = 3$.*

Proof. Since $u_5 = 0$, the index i is different from 5 and so $i \in \{1, 3\}$. Assume by contradiction that $i = 1$. Since $G_4 = (H \cap G_4)G_5$ and G_5 is central, we then have that $G_5 = [G, H \cap G_4]$. Moreover, the group $[G_2, G_4]$ is trivial ans so it follows that $[HG_2, G_4] = [H, G_4] = [H, H \cap G_4] \subseteq H \cap G_5 = \{1\}$. In particular, H is contained in C and so, as a consequence of Lemma 10.10(1), we get $\rho^2(H) = \rho^2(C)$. It follows from Lemma 12.12 that H contains G_5. Contradiction to $H \cap G_5 = \{1\}$. □

Let D be a maximal subgroup of G with the property that $(H \cap G_3)G_4 = D^p G_4$ and note that, thanks to Corollary 10.2, the subgroup D is uniquely determined by H. Since D^p is normal in G, Lemma 10.9 yields $D^p = D^p G_4$ and therefore, from Corollary 10.2, one gets $|D^p : G_4| = p$.

Lemma 12.14. *One has $C \neq D$ and $[D, G_4] = [G_2, D^p] = G_5$. In addition, one has $\rho^2(D) = \{1\}$.*

Proof. Thanks to Lemma 10.10(1), one has $\rho^2(D) = \rho(D^p) = \rho(H \cap G_3)$ and so, as a consequence of Lemma 10.5, the subgroup $\rho(H \cap G_3)$ is contained in $H \cap G_5 = \{1\}$. It follows that $\rho^2(D) = \{1\}$. Moreover, the subgroups D and C are both maximal in G and so, as a consequence of Lemmas 12.12 and 12.14, they are distinct. Now, the class of G being 5, the subgroup $[D, G_4]$ is non-trivial and, since $w_5 = 1$, we get $[D, G_4] = G_5$. The subgroups $[G_2, D^p]$ and $[G_2^p, D]$ are equal, by Lemma 10.6, and so, from Lemma 10.5, we derive $[G_2, D^p] = G_5$. □

Lemma 12.15. *The subgroup H is abelian and $(i, j) = (3, 4)$.*

Proof. We first show that H is abelian. As a consequence of Lemma 12.13, the subgroup H is contained in G_2 and, since $w_2 = 1$, the quotient $H/(H \cap G_3)$ is cyclic. It follows that $[H, H] = [H, H \cap G_3] \subseteq H \cap G_5 = \{1\}$ and so H is abelian. We now show that $(i, j) = (3, 4)$. By Lemma 12.13, the jump i is equal to 3 and, by definition of D, we have $D^p = (H \cap G_3)G_4$. Moreover, since G has class 5, the jump j belongs to $\{2, 4\}$. Assume by contradiction that $j = 2$. Then $u_2 = w_2 = 1$ and so $G_2 = HG_3$. By Lemma 12.14, the subgroups $[G_2, D^p]$ and G_5 coincide and so, the group G_5 being central, the commutator map $G_2 \times D^p \to G_5$ is bilinear and non-trivial. It follows that the induced map $G_2/G_3 \times D^p/G_4 \to G_5$ is non-trivial and so $[H, H \cap G_3] \neq 1$. Contradiction. □

Lemma 12.16. *Let x and y be elements of H, respectively belonging to $D^p \setminus G_4$ and $G_4 \setminus G_5$. Then $H = \langle x \rangle \oplus \langle y \rangle$ and $(u_1, u_2, u_3, u_4, u_5) = (0, 0, 1, 1, 0)$.*

Proof. Thanks to Lemma 12.15 and Corollary 10.2, we have $u_1 = u_2 = u_5 = 0$ and $u_3 = u_4 = 1$. The subgroup H is thus contained in G_3 and so, by Lemma 10.5, one has $H^p \subseteq G_5 \cap H = \{1\}$. It follows from Lemma 12.15 that H is elementary abelian. Given any two elements x and y of H, satisfying $x \in D^p \setminus G_4$ and $y \in G_4 \setminus G_5$, Lemma 2.16 now yields $H = \langle x \rangle \oplus \langle y \rangle$. □

We define X to be the collection of all subgroups of G of the form $\langle x \rangle \oplus \langle y \rangle$, where (x, y) belongs to $(D^p \setminus G_4) \times (G_4 \setminus G_5)$. Thanks to Lemmas 12.14 and 12.15, each such subgroup is elementary abelian and thus X is well defined. We remark that, the group D^p being normal in G, the group G acts naturally on X by conjugation. Write $X^+ = \{K \in X : \alpha(K) = K\}$.

Lemma 12.17. *The cardinality of X is p^2.*

Proof. Let K be an element of X. Then there exist elements x and y of order p, respectively of depth 3 and 4 in G, such that $x \in D^p$ and $K = \langle x \rangle \oplus \langle y \rangle$. Since $|D^p : G_4| = p$ and $(w_4, w_5) = (1, 1)$, we get

$$|X| = \frac{(p^3 - p^2)(p^2 - p)}{(p-1)p(p-1)} = p^2.$$

□

Lemma 12.18. *One has $\mathrm{N}_G(H) \cap D = \mathrm{N}_G(H) \cap G_2 = G_3$.*

Proof. We first claim that $\mathrm{N}_G(H) \cap D = \mathrm{N}_G(H) \cap G_2$. We work by contradiction, assuming that $\mathrm{N}_G(H) \cap D \neq \mathrm{N}_G(H) \cap G_2$. Since $(H \cap G_4)G_5 = G_4$ and G_5 is central, we then have that $[D, G_4] = [D, H \cap G_4]$ is contained in H and thus, thanks to Lemma 12.14, the subgroup G_5 is contained in H. This contradicts the hypotheses on H and so the claim is proven. We now prove that $\mathrm{N}_G(H) \cap G_2 = G_3$. As a consequence of Lemma 12.15, the subgroup H is contained in G_3 and so, since G_3 is abelian, G_3 normalizes H. Assume now by contradiction that 2 is a jump of $\mathrm{N}_G(H)$ in G. Since G_2 centralizes G_4 and $(H \cap G_3)G_4 = D^p$, we have that $[G_2, D^p] = [G_2, H \cap G_3]$ and therefore the subgroup $[G_2, D^p]$ is contained in H. Lemma 12.14 yields $G_5 \subseteq H$. Contradiction. □

We claim that the action of G on X is transitive. As a consequence of Lemma 12.17, we have that $p^2 = |X| \geq |G : \mathrm{N}_G(H)|$ and therefore, applying Lemma 12.18, we get

$$p^2 \geq |G : \mathrm{N}_G(H)| \geq |D : G_2||G_2 : G_3| = |D : G_3|.$$

By Lemma 10.2(2), the index $|D : G_3|$ is equal to p^2 and therefore the number of conjugates of H in G is equal to p^2. This proves the claim. To conclude, we remark that $\alpha(H)$ is an element of X and therefore $\alpha(H)$ and H are conjugate. The choice of H being arbitrary, Lemma 3.5 yields that α is intense and so $\mathrm{int}(G) > 1$. The proof of Proposition 12.11 is now complete.

12.3. Proving the main theorem

In this section we prove Proposition 12.19 and Theorem 12.2. We remind the reader that a p-obelisk G is framed if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$.

PROPOSITION 12.19. *Let $p > 3$ be a prime number and let G be a finite p-group of class at least* 5. *Assume that* $\mathrm{int}(G) > 1$. *Then G is a p-obelisk and one of the following holds.*

1. *One has* $\mathrm{wt}_G(5) = 1$ *and G has class* 5.
2. *One has* $\mathrm{wt}_G(5) = 2$ *and G is framed.*

PROOF. By Proposition 10.1, the group G is a p-obelisk so, thanks to Proposition 10.3(1), the width $\mathrm{wt}_G(5)$ is either 1 or 2. If $\mathrm{wt}_G(5) = 1$, then Theorem 12.1 yields that G has class 5. Assume now that $\mathrm{wt}_G(5) = 2$. We will show that, for each maximal subgroup M of G, one has $\Phi(M) = G_3$. To this end, let M be a maximal subgroup of G. By Lemma 10.4, the widths $\mathrm{wt}_G(1)$ and $\mathrm{wt}_G(4)$ are respectively 2 and 1 so, the index $|G : M|$ being p, it follows from Lemma 10.11, that 5 is a jump of $[M, G_4]$ of width 1 in G. Moreover, 5 is the smallest jump of $[M, G_4]$ in G, and so Lemma 10.9 yields $G_6 \subseteq [M, G_4]$. We denote $\overline{G} = G/[M, G_4]$ and use the bar notation for the subgroups and the elements of $\overline{G}$. We remark that, by construction, we have $\overline{M} \subseteq \mathrm{C}_{\overline{G}}(\overline{G_4})$ and $\mathrm{wt}_{\overline{G}}(5) = 1$. The class of $\overline{G}$ being 5, we have in fact that $\overline{M} = \mathrm{C}_{\overline{G}}(\overline{G_4})$ and so Proposition 12.3 yields $\Phi(\overline{M}) = \overline{G_3}$. The subgroup $\Phi(M)$ being normal in G, it follows from Lemma 10.9 that $\Phi(M) = \{x \in G : \overline{x} \in \Phi(\overline{M})\}$ and therefore $\Phi(M) = G_3$. The choice of M being arbitrary, the proof is complete. □

We are finally ready to prove Theorem 12.2. Let p be a prime number and let G be a finite p-group with $\mathrm{wt}_G(5) = 2$. The implication (2) ⇒ (1) is given by Theorem 11.2. Assume now (1). Since $\mathrm{wt}_G(5) \neq 1$, the class of G is at least 5. Moreover, thanks to Proposition 3.7 and Corollary 9.5, the prime p is larger than 3. Proposition 12.19 yields that G is a framed p-obelisk. As a consequence of Theorem 5.2, the intensity of G is equal to 2 and so, thanks to the Schur-Zassenhaus theorem, G has an intense automorphism of order 2 that, by Proposition 5.10, induces the inversion map on G/G_2. The proof of Theorem 12.2 is complete.

CHAPTER 13

Intense Automorphisms of Profinite Groups

Let G be a profinite group and let α be an automorphism of G. Then α is *topologically intense* if, for every closed subgroup H of G, there exists $x \in G$ such that $\alpha(H) = xHx^{-1}$. Topologically intense automorphisms are automatically continuous, because they stabilize each open normal subgroup of the group on which they are defined. We denote by $\mathrm{Int_c}(G)$ the group of topologically intense automorphisms of a profinite group G.

Topologically intense automorphisms are a generalization of intense automorphisms to profinite groups. In Section 13.2, we will show that, the group of topologically intense automorphisms of a profinite group is itself profinite and moreover, if p is a prime number and G is a pro-p-group, then $\mathrm{Int_c}(G)$ is isomorphic to SC, where S is a pro-p-subgroup of $\mathrm{Int_c}(G)$ and C is a subgroup of $\mathbb{F}_p^*$. The *intensity* of a pro-p-group G is then defined to be the cardinality of C and it is denoted by $\mathrm{int}(G)$. The question we ask is: *What are the infinite pro-p-groups that have intensity greater than* 1*?* We answer this question with Theorem 13.1, which we state after fixing some notation. Let p be an odd prime number and take $t \in \mathbb{Z}_p$ to be a quadratic non-residue modulo p. We define Δ_p to be the quaternion algebra $\mathbb{Z}_p \oplus \mathbb{Z}_p\mathrm{i} \oplus \mathbb{Z}_p\mathrm{j} \oplus \mathbb{Z}_p\mathrm{k}$ with defining relations $\mathrm{i}^2 = t$, $\mathrm{j}^2 = p$, and $\mathrm{k} = \mathrm{ij} = -\mathrm{ji}$ and we denote by $\mathrm{S}(\Delta_p)$ the pro-p-subgroup of the multiplicative group $(1 + \mathrm{j}\Delta_p)$ that consists of all elements $x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ satisfying $a^2 - tb^2 - pc^2 + tpd^2 = 1$.

Theorem 13.1. *Let p be a prime number and let G be an infinite pro-p-group. Then* $\mathrm{int}(G) > 1$ *if and only if exactly one of the following holds.*

1. *One has $p > 2$ and G is abelian.*
2. *One has $p > 3$ and G is topologically isomorphic to* $\mathrm{S}(\Delta_p)$.

Moreover, one has $\mathrm{int}(\mathrm{S}(\Delta_p)) = 2$ *and, if G is abelian, then* $\mathrm{int}(G) = p - 1$.

Let p be a prime number and let G be a pro-p-group. We will show, in Section 13.2, that

$$\mathrm{int}(G) = \gcd\{\mathrm{int}(G/N) : N \text{ normal open in } G,\ N \neq G\}$$

and, thanks to this last characterization, we will derive the following theorem as a corollary of Theorem 13.1.

Theorem 13.2. *Let $p > 3$ be a prime number. Then, for any positive integer c, there exists a finite p-group of class c and intensity greater than* 1.

The pace of Chapter 13 will be slightly faster, compared to the previous ones, in the sense that we will assume the reader is familiar with some basic facts about profinite groups (which can however all be found in Chapters 0 and 1 from [**DdSMS91**]). We will give some extra background in Section 13.1. In Section 13.2, we will prove several properties of topologically intense automorphisms and give an analogue of Theorem 3.1 for pro-p-groups. In the subsequent sections we will pave the way to proving Theorem 13.1. In Section 13.3, we will give some limitations, for $p > 3$, to the structure of infinite non-abelian pro-p-groups of intensity greater than 1. In Section 13.5, we will discover that, if such groups exist, they can be continuously embedded in one of two infinite pro-p-groups (one of them being $\mathrm{S}(\Delta_p)$). We will study the structure of those two groups in Section 13.4 and, in Section 13.5, we will prove that, if $p > 3$ is a prime number and G is an infinite non-abelian pro-p-group with $\mathrm{int}(G) > 1$, then G is topologically isomorphic to $\mathrm{S}(\Delta_p)$. The results from Section 13.4.2 will ensure that $\mathrm{int}(\mathrm{S}(\Delta_p)) > 1$. We will conclude the proof of Theorem 13.1 in Section 13.6.1 and give that of Theorem 13.2 in Section 13.6.2. We will close Chapter 13 with Section 13.6.3, where we will draw a bridge between Theorem 13.1 and Theorem 13.2.

13.1. Some background

This section is a collection of definitions and results from [**DdSMS91**]. If G is a profinite group and S is a subset of it, we denote by $\mathrm{cl}(S)$ the closure of S in G.

Definition 13.3. Let G be a profinite group. A *discrete quotient* of G is a quotient of G by an open normal subgroup. A *proper quotient* of G is a quotient of G by a closed normal subgroup that is different from $\{1\}$.

Definition 13.4. Let G be a profinite group. Then a set X is a *set of topological generators* of G if $G = \mathrm{cl}(\langle X\rangle)$. The group G is *topologically finitely generated* if it admits a finite set of topological generators.

Definition 13.5. Let G be a profinite group. The *lower central series* $(G_i)_{i\geq 1}$ of G is defined by

$$G_1 = G \quad\text{and}\quad G_{i+1} = \mathrm{cl}([G, G_i]).$$

We recall that, as defined in Section 8.2, the rank of a finite group H is the smallest integer r such that every subgroup of H can be generated by r elements.

Definition 13.6. Let G be a profinite group. The *rank* of G is

$$\mathrm{rk}(G) = \sup\{\mathrm{rk}(G/N) : N \text{ is normal open in } G\}.$$

Let G be a profinite group. It follows from the definition that $\mathrm{rk}(G)$ belongs to $\mathbb{Z}\cup\{\infty\}$ and, if G has finite rank, that G is also finitely generated. Moreover, when G is finite, the definition of rank given in Section 8.2 is equivalent to the one from Definition 13.6. In [**DdSMS91**, Proposition 3.11], a series of equivalent definitions of rank is given.

Definition 13.7. A *p-adic analytic* group is a profinite group that contains an open pro-p-subgroup of finite rank.

Our definition of a p-adic analytic group is not among the standard ones, but it serves our purposes the best. In general, p-adic analytic groups are defined to be topological groups that present the structure of a p-adic manifold. The equivalence of the two definitions, for profinite groups, is given by Corollary 9.35 from [**DdSMS91**]. For more information about the topic, see [**DdSMS91**, Ch. 9].

Definition 13.8. Let p be an odd prime number and let U be a pro-p-group. Then U is *uniform* if the following hold.

1. The group U is topologically finitely generated.
2. The quotient $U/\operatorname{cl}(U^p)$ is abelian.
3. The group U is torsion-free.

The definition of uniform group we give is slightly different from the one that is given in [**DdSMS91**]. However, the equivalence of the two is proven in [**DdSMS91**, Theorem 4.8].

Definition 13.9. Let p be an odd prime number and let U be a uniform pro-p-group. The *dimension* of U is the cardinality of a minimal set of topological generators of U. The dimension of U is denoted $\dim(U)$.

Definition 13.10. Let p be an odd prime number and let G be a pro-p-group of finite rank. The *dimension* of G is the dimension of any of its open uniform subgroups.

Corollary 4.3 and Corollary 4.6 from [**DdSMS91**] guarantee the consistency of Definition 13.10.

13.2. Properties and intensity

In the present section we give several properties of topologically intense automorphisms and, for a given prime number p, we define the intensity of a pro-p-group. The following lemma is straightforward.

Lemma 13.11. *Let G be a profinite group and let α be a topologically intense automorphism of G. Then α induces an intense automorphism on each discrete quotient of G.*

If G is a profinite group and Υ denotes the set of open normal subgroups of G, then $\operatorname{Aut}(G)$ has a natural topology, the "congruence topology", for which a basis of open neighbourhoods of the identity is $\{\Gamma(N) = \{\alpha \in \operatorname{Aut}(G) : \alpha \equiv \operatorname{id} \operatorname{mod} N\}\}_{N\in\Upsilon}$. For more information on the subject see for example [**DdSMS91**, Ch. 5.2]. Using Lemma 13.11, one then easily proves the following.

Proposition 13.12. *Let G be a profinite group and let Υ denote the collection of open normal subgroups of G. Then one has*

$$\operatorname{Int_c}(G) = \varprojlim_{N\in\Upsilon} \operatorname{Int}(G/N).$$

Lemma 13.13. *Let $\{X_\lambda\}_{\lambda\in\Lambda}$ be an inverse system of finite non-empty sets over a directed set Λ. Then $\varprojlim X_\lambda$ is non-empty.*

Proof. This is Proposition 1.4 from [**DdSMS91**]. □

Proposition 13.14. *Let G be a profinite group and let α be an automorphism of G. Then the following are equivalent.*

1. *The automorphism α is topologically intense.*
2. *For every open subgroup H of G, there exists an element $x \in G$ such that $\alpha(H) = xHx^{-1}$.*

Proof. As every open subgroup is also closed, (1) clearly implies (2). Assume now (2) and let H be a closed subgroup of G. We will construct $x \in G$ such that $\alpha(H) = xHx^{-1}$. Let Λ denote the collection of all discrete quotients of G and let moreover Υ be the collection of all open normal subgroups of G. Then there is a natural bijection $\Upsilon \to \Lambda$, given by $N \mapsto G/N$. Now, thanks to Lemma 13.11, the automorphism α induces an intense automorphism on each element of Λ. Hence, if $\overline{G}$ is an element of Λ and $\overline{H}$ denotes the image of H in $\overline{G}$, then there exists $x \in \overline{G}$ such that $\overline{\alpha(H)} = x\overline{H}x^{-1}$. For each $\overline{G} \in \Lambda$ define $X_{\overline{G}} = \{x \in \overline{G} : \overline{\alpha(H)} = x\overline{H}x^{-1}\}$ and observe that $X_{\overline{G}}$ is finite and non-empty. Let now $\overline{G}$ and $\overline{G}\,'$ be elements of Λ such that $\overline{G}\,'$ is a quotient of $\overline{G}$. Then the natural projection $\overline{G} \to \overline{G}\,'$ induces a well-defined map $X_{\overline{G}} \to X_{\overline{G}\,'}$. It follows that $\{X_{\overline{G}}\}_{\overline{G}\in\Lambda}$ is an inverse system of finite non-empty sets so, by Lemma 13.13, the set $X = \varprojlim X_{\overline{G}}$ is non-empty. Let $x \in X$. Then, for each element N of Υ, the element xN belongs to $X_{G/N}$ and thus, for each $N \in \Upsilon$, we have $\alpha(HN) = xHx^{-1}N$. The map α is continuous, because it stabilizes each open normal subgroup, and so it follows that

$$\alpha(H) = \bigcap_{N\in\Upsilon} \alpha(H)N = \bigcap_{N\in\Upsilon} \alpha(HN) = \bigcap_{N\in\Upsilon} xHx^{-1}N = xHx^{-1}.$$

This proves (1), and therefore the proof is complete. □

In the proof of the following result we will use the generalization to profinite groups of Schur-Zassenhaus's theorem (see for example Theorem 2.3.15 from [**RZ10**]).

Proposition 13.15. *Let p be a prime number and let G be a pro-p-group. Then*

$$\mathrm{Int_c}(G) = SC,$$

where S is a Sylow pro-p-subgroup of $\mathrm{Int_c}(G)$ *and C is isomorphic to a subgroup of $\mathbb{F}_p^*$. Moreover, one has*

$$|C| = \gcd\{\mathrm{int}(G/N) : N \textit{ normal open in } G,\ N \neq G\}.$$

Proof. Let Υ denote the collection of open normal subgroups of G. For each $N \in \Upsilon$, denote by $\pi_N : \mathrm{Int}(G/N) \to \mathrm{Int}((G/N)/\Phi(G/N))$ the map from Lemma 3.2(2) and set $K_N = \ker \pi_N$ and $I_N = \pi_N(\mathrm{Int}(G/N))$. For each $N \in \Upsilon$, we then get a short exact sequence

$$1 \to K_N \to \mathrm{Int}(G/N) \to I_N \to 1$$

which induces, thanks to Proposition 13.12 and the exactness of $\varprojlim$, the short exact sequence

$$1 \to \varprojlim_{N\in\Upsilon} K_N \to \mathrm{Int_c}(G) \to \varprojlim_{N\in\Upsilon} I_N \to 1.$$

Define $S = \varprojlim_{N\in\Upsilon} K_N$ and $C = \varprojlim_{N\in\Upsilon} I_N$. As a consequence of Lemma 3.13, whenever $M, N \in \Upsilon \setminus \{G\}$ and $N \subseteq M$, the natural map $I_N \to I_M$ is injective and therefore, $\varprojlim_{N\in\Upsilon} \mathrm{Int}((G/N)/\Phi(G/N))$ being equal to $\mathrm{Int}(G/\Phi(G))$, Lemma 3.3 yields that C is isomorphic to a subgroup of $\mathbb{F}_p^*$. Moreover, thanks to Lemma 3.9, the group S is a pro-p-subgroup of $\mathrm{Int_c}(G)$. The order of C being coprime to p, it follows that in fact S is a Sylow pro-p-subgroup of $\mathrm{Int_c}(G)$ and, from the generalization of Schur-Zassenhaus's theorem to profinite groups, that $\mathrm{Int_c}(G) = SC$. Moreover, the fact that $|C|$ is equal to the greatest common divisor of the $\mathrm{int}(G/N)$, as N varies in $\Upsilon \setminus \{G\}$, is a direct consequence of Lemma 3.13. □

Let p be a prime number and let G be a pro-p-group. Let moreover C be as in Proposition 13.15. The *intensity* $\mathrm{int}(G)$ of G is defined to be the cardinality of C.

Thanks to Proposition 13.15, the intensity of G is also equal to the greatest common divisor of the set $\{\mathrm{int}(G/N) : N \text{ normal open in } G,\ N \neq G\}$. The following directly follows from Proposition 13.15 and Theorem 3.1.

Let p be a prime number and let G be an abelian pro-p-group. If G is non-trivial, then $\mathrm{int}(G) = p - 1$.

13.3. Non-abelian groups, part I

The main purpose of the present section is to give a proof of Proposition 13.16. We refer to Section 13.1 for the definitions of p-adic analytic groups and their dimensions.

Proposition 13.16. *Let $p > 3$ be a prime number and let G be a non-abelian infinite pro-p-group. Assume that* $\mathrm{int}(G) > 1$. *Then G is a just-infinite p-adic analytic group of dimension* 3.

The following assumptions will be valid until the end of Section 13.3. Let p be an odd prime number and let G be an infinite non-abelian pro-p-group of intensity greater than 1. Let $(G_i)_{i\geq 1}$ denote the lower central series of G, as defined in Section 13.1, and let α be a topologically intense automorphism of G of order 2. The existence of α is guaranteed by the combination of Proposition 13.15 with our classification of finite p-groups of intensity greater than 1. Moreover, α induces an intense automorphism of order 2 on each non-trivial discrete quotient of G. Indeed, without loss of generality, $\alpha \in C$ with C is as in Proposition 13.15 and, given open normal subgroups N and M of G such that $N \subseteq M \neq G$, Lemma 13.11 yields a commutative diagram

$$\begin{tikzcd} C \arrow[r] \arrow[d] & \mathrm{Int}(G/M) . \\ \mathrm{Int}(G/N) \arrow[ur] & \end{tikzcd}$$

The map α being non-trivial, there exists a discrete quotient of G on which α induces an automorphism of order 2 so α induces an intense automorphism of order 2 on each non-trivial discrete quotient of G. In particular, each non-trivial discrete quotient of G has intensity greater than 1.

Lemma 13.17. *Assume that $p > 3$. Then each discrete quotient of G of class at least* 4 *is a p-obelisk.*

Proof. This follows from Proposition 10.1. □

Lemma 13.18. *Let c be a non-negative integer. Then G has a discrete quotient of class c.*

Proof. Assume by contradiction that there exists an upper bound on the class of the discrete quotients of G and let $C \in \mathbb{Z}_{\geq 0}$ be minimal with this property. Since G is non-abelian, one has $C \geq 2$. Let us now denote by Υ the collection of open normal subgroups of G. Then $G = \varprojlim_{N\in\Upsilon} G/N$ and so G has class C. The group G being infinite, it follows from Theorem 6.2 that $C < 3$ and so $C = 2$. Let now $M, N \in \Upsilon$ be such that G/N has class 2 and MN. Let $K = G/M$ and let $\pi : G \to K$ denote the canonical projection. Then K has class 2 and the intensity of K is greater than 1. By Theorem 4.1, the group K is extraspecial and, $\pi(N)$

being non-trivial and normal in K, it follows that $\pi(N)$ contains $\mathrm{Z}(K) = [K,K]$. In particular, $K/\pi(N)$ is abelian and therefore so is G/N. Contradiction. □

Lemma 13.19. *The lower central series $(G_i)_{i\geq 1}$ of G is a base of open neighbourhoods of 1 in G.*

Proof. Let Υ denote the collection of open normal subgroups N of G such that G/N has class at least 3. As a consequence of Lemma 13.18, the group G is equal to $\varprojlim_{N\in\Upsilon} G/N$ and, each subgroup G_i being closed, we also have $G_i = \varprojlim_{N\in\Upsilon} (G/N)_i$. For each $N \in \Upsilon$, the quotient G/N has intensity greater than 1 and so Theorem 8.1 yields that $(G_i)_{i\geq 1}$ is a base of open neighbourhoods of 1 in G. □

Lemma 13.20. *Assume that $p > 3$. Then $\mathrm{rk}(G) = 3$ and G is p-adic analytic.*

Proof. As a consequence of Lemma 13.18, the rank of G coincides with $\sup\{\mathrm{rk}(G/N) : G/N \text{ has class at least } 4\}$. Proposition 8.7 yields $\mathrm{rk}(G) = 3$ and thus G is p-adic analytic. □

Lemma 13.21. *Assume that $p > 3$. Let N be a non-trivial closed subgroup of G. Then the following are equivalent.*

1. *The subgroup N is normal.*
2. *There exists $l \in \mathbb{Z}_{\geq 1}$ such that $G_{l+1} \subseteq N \subseteq G_l$.*

Moreover, P is just-infinite.

Proof. The implication (2) ⇒ (1) is clear; we prove (1) ⇒ (2). Thanks to Lemma 13.19, every element of the lower central series of G is open and $(G_i)_{i\geq 1}$ is a base of open neighbourhoods of 1. For all $k \in \mathbb{Z}_{\geq 1}$, denote by $\pi_k : G \to G/G_k$ the canonical projection and set $l = \max\{k : \pi_k(N) = 1\}$. The index l is well-defined, because $N \neq 1$, and N is contained in G_l, but not in G_{l+1}, by the maximality of l. In particular, for each $k > l$, the minimum jump (see Section 2.3) of $\pi_k(N)$ in G/G_k is l. Now, by Lemma 13.17, whenever $k \geq 5$, the quotient G/G_k is a p-obelisk. It follows from Lemma 10.9(2) that, if $k > \max\{l, 5\}$, then G_{l+1} is contained in NG_k, and therefore

$$G_{l+1} \subseteq \bigcap_{k>\max\{l,5\}} NG_k = \bigcap_{k\geq 1} NG_k = \mathrm{cl}(N) = N.$$

We have proven that $G_{l+1} \subseteq N \subseteq G_l$ and thus also that (1) implies (2). Each subgroup G_k being open in G, the group G is just-infinite. □

Lemma 13.22. *Assume that $p > 3$. Then G is torsion-free.*

Proof. By Lemma 13.17, whenever k is at least 5, the quotient G/G_k is a p-obelisk. It follows from Corollary 10.2 that, for each non-negative integer i, raising to the power p induces a well-defined isomorphism $G_i/G_{i+1} \to G_{i+2}/G_{i+3}$. By Lemma 13.18, there is no bound on the class of the finite quotients of G, and therefore G is torsion-free. □

Lemma 13.23. *Assume that $p > 3$. Then G_2 is open, uniform, and has dimension 3.*

Proof. Let $\overline{G}$ be a discrete quotient of class at least 5 of G, which exists by Lemma 13.18. As a consequence of Lemma 13.17, the group $\overline{G}$ is a p-obelisk and so Lemma 10.4 yields $|\overline{G}_2 : \overline{G}_4| = p^3$. The subgroup $\overline{G}_2^p$ is equal to $\overline{G}_4$, thanks to

Lemma 10.5, and so $\overline{G}_2/\overline{G}_2^p = \overline{G}_2/\overline{G}_4$ is elementary abelian. It follows that each generating set of $\overline{G}_2$ has at least 3 elements. However, the rank of G is equal to 3, thanks to Lemma 13.20, and therefore $\overline{G}_2$ is generated by exactly 3 elements. Since $\overline{G}$ was chosen arbitrarily, the quotient $G_2/\operatorname{cl}(G_2^p)$ is abelian and any minimal set of topological generators of G_2 has 3 elements. Now, as a consequence of Lemma 13.22, the torsion of G_2 is trivial and hence G_2 is uniform of dimension 3. Moreover, the subgroup G_2 is open thanks to Lemma 13.19. □

We conclude Section 13.3 by giving the proof of Proposition 13.16. Assume that $p > 3$. Then G is p-adic analytic, by Lemma 13.20, and it has dimension 3 thanks to Lemma 13.23. Moreover, G is just-infinite by Lemma 13.21. The proof of Proposition 13.16 is now complete.

13.4. Two infinite groups

In this section we present two infinite pro-p-groups, which are p-adic analytic. We will see, in Section 13.5, the role they play in the proof of Theorem 13.1.

13.4.1. The first group. Let $p > 3$ be a prime number and let $\pi : \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ be the canonical projection. Let $\mathrm{SL}_2^{\triangle}(\mathbb{F}_p)$ denote the subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ consisting of those elements of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad x \in \mathbb{F}_p.$$

We define $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p) = \pi^{-1}(\mathrm{SL}_2^{\triangle}(\mathbb{F}_p))$ and remark that $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ is a pro-p-group. Our notation is consistent with that of [**GSK09**]; however, we will make use of several facts coming from [**Hup67**, Ch. III.17], where the group $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ is denoted by $\mathfrak{M}_{0,1,1}$.

We recall that a p-obelisk is a non-abelian finite p-group G satisfying $G_3 = G^p$ and $|G : G_3| = p^3$. A p-obelisk G is framed if, given any maximal subgroup M of G, one has $\Phi(M) = G_3$. For more information about p-obelisks, we refer to Chapter 10.

Lemma 13.24. *Let $p > 3$ be a prime number and let $G = \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $k \in \mathbb{Z}_{\geq 3}$, the quotient G/G_k is a p-obelisk.*

Proof. This is a reformulation of Satz 17.8 from [**Hup67**, Ch. III]. □

Lemma 13.25. *Let $p > 3$ be a prime number and let $G = \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then there exist $x \in G \setminus G_2$ and $a \in G_2 \setminus G_3$ such that $[x, a] \in \operatorname{cl}(\langle x \rangle)$.*

Proof. This proof relies on several lemmas from [**Hup67**, Ch. III.17]; we will respect Huppert's notation. Let

$$x = B(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad a = D(1+p) = \begin{pmatrix} (1+p)^{-1} & 0 \\ 0 & (1+p) \end{pmatrix}.$$

Satz 17.4 from [**Hup67**, Ch. III.17] gives a concrete characterization of the lower central series of G, from which it directly follows that $x \in G \setminus G_2$ and $a \in G_2 \setminus G_3$.

As a consequence of Hilfssatz 17.2(a), the element x generates topologically the subgroup $\mathfrak{B}_0$ consisting of all matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad x \in \mathbb{Z}_p.$$

To conclude, Hilfssatz 17.3 guarantees that there exists an element $b \in \mathbb{Z}_p$ such that

$$[x, a] = \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix}$$

so, in particular, $[x, a]$ belongs to the subgroup $\mathfrak{B}_0 = \mathrm{cl}(\langle x \rangle)$. □

LEMMA 13.26. *The group* $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ *has a discrete quotient of class* 6 *that is not a framed p-obelisk.*

PROOF. Let $G = \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ and denote by $(G_i)_{i \geq 1}$ the lower central series of G, as defined in Section 13.1. We define $\overline{G} = G/G_7$ and we use the bar notation for subgroups and elements of $\overline{G}$. The group $\overline{G}$ has class 6 and it is a p-obelisk, by Lemma 13.24. Let now $x \in G$ be as in Lemma 13.25 and set $\ell = \langle \overline{xG_2} \rangle$, which is a 1-dimensional subspace of $\overline{G}/\overline{G}_2$. Let moreover

$$\rho_1^1 : \overline{G}/\overline{G}_2 \to \overline{G_3}/\overline{G}_4$$

and

$$\gamma_{1,2} : \overline{G}/\overline{G}_2 \times \overline{G_2}/\overline{G_3} \to \overline{G_3}/\overline{G}_4$$

denote the maps from Lemma 10.10. As a consequence of Lemma 13.25, the elments $\rho_1^1(\ell)$ and $\gamma_{1,2}(\{\ell\} \times \overline{G}_2/\overline{G}_3)$ generate a 1-dimensional subspace ℓ' of $\overline{G}_3/\overline{G}_4$. By Lemma 10.4(1), the width $\mathrm{wt}_{\overline{G}}(3)$ is equal to 2 so ℓ' is different from $\overline{G}_3/\overline{G}_4$. Proposition 10.14 yields that $\overline{G}$ is not framed. □

13.4.2. The second group. Let $p > 3$ be a prime number and let $t \in \mathbb{Z}_p$ be a quadratic non-residue modulo p. Define Δ_p to be $\left(\frac{t,\,p}{\mathbb{Z}_p}\right)$, i.e., the quaternion algebra

$$\Delta_p = \mathbb{Z}_p \oplus \mathbb{Z}_p\mathrm{i} \oplus \mathbb{Z}_p\mathrm{j} \oplus \mathbb{Z}_p\mathrm{k}$$

with defining relations

$$\mathrm{i}^2 = t,\ \mathrm{j}^2 = p,\ \text{and}\ \mathrm{k} = \mathrm{ij} = -\mathrm{ji}.$$

The quaternion algebra Δ_p is equipped with a bar map, defined by

$$x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \ \mapsto\ \overline{x} = a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k},$$

which is an anti-homomorphism of order 2. The algebra Δ_p has, in addition, a unique maximal (left/right/two-sided) ideal $\mathfrak{m}$, which is principal generated by j, i.e. $\mathfrak{m} = \Delta_p\mathrm{j}$. It follows that an element $x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ belongs to $\mathfrak{m}$ if and only if both a and b belong to $p\mathbb{Z}_p$. Moreover, for each $k \in \mathbb{Z}_{\geq 1}$, the ideal $\mathfrak{m}^k$ is principal generated by j^k and therefore, for each $s \in \mathbb{Z}_{\geq 0}$, one has

$$\mathfrak{m}^{2s} = p^s\Delta_p \quad \text{and} \quad \mathfrak{m}^{2s+1} = p^s\mathfrak{m}.$$

As a result, for each $k \in \mathbb{Z}_{\geq 1}$, the quotient $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a vector space over $\mathbb{F}_p$ of dimension 2. Now, for each $k \in \mathbb{Z}_{\geq 1}$, the set $1 + \mathfrak{m}^k$ is easily seen to be a subgroup of Δ_p^* and the natural map $(1 + \mathfrak{m}^k)/(1 + \mathfrak{m}^{k+1}) \to \mathfrak{m}^k/\mathfrak{m}^{k+1}$ is an isomorphism of groups. It follows that $1 + \mathfrak{m}$ is a pro-p-subgroup of Δ_p^*. Define

$$\mathrm{S}(\Delta_p) = (1 + \mathfrak{m}) \cap \{x \in \Delta_p : \overline{x} = x^{-1}\}.$$

Then $\mathrm{S}(\Delta_p)$ is a closed subgroup of $1+\mathfrak{m}$ and thus a pro-p-group itself. We have here lightened the notation from [**GSK09**], where the group $\mathrm{S}(\Delta_p)$ is denoted by $\mathrm{SL}_1^1(\Delta_p)$.

Lemma 13.27. *Let $p>3$ be a prime number and let $G=\mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $k\in\mathbb{Z}_{\geq 1}$, one has $G_k=(1+\mathfrak{m}^k)\cap G$.*

Proof. We sketch here the proof, but leave out the computations. For all $i\in\mathbb{Z}_{\geq 1}$, denote $M_i=(1+\mathfrak{m}^i)\cap G$. We remark that all M_i are normal in G and they form a base of open neighbourhoods of 1 in G. It is easy to check that $(M_i)_{i\geq 1}$ is a central series, in other words for all $i\in\mathbb{Z}_{\geq 1}$ the subgroup $[M_1,M_i]$ is contained in M_{i+1}. Then, for each index i, the commutator map induces a bilinear map $\gamma_i : M_1/M_2\times M_i/M_{i+1}\to M_{i+1}/M_{i+2}$. Next, by direct computation, one gets that, for every $i\in\mathbb{Z}_{\geq 1}$, the image of γ_i generates M_i/M_{i+1}, and therefore $M_{i+1}=[M_1,M_i]M_{i+2}$. Fix i. By induction one shows that, for each positive integer n, one has $M_{i+1}=[M_1,M_i]M_{i+n}$, and hence

$$M_{i+1}=\bigcap_{n\geq 1}[M_1,M_i]M_{i+n}=\mathrm{cl}([M_1,M_i]).$$

Since $M_1=G$, we get that $M_{i+1}=\mathrm{cl}([G,G_i])=G_{i+1}$ and the proof is complete. □

Lemma 13.28. *Let $p>3$ be a prime number and let $G=\mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $i\in\mathbb{Z}_{\geq 1}$, the map $x\mapsto x^p$ on G induces an isomorphism $\rho_i : G_i/G_{i+1}\to G_{i+2}/G_{i+3}$.*

Proof. By Lemma 13.27, given any positive integer i, one has $G_i=(1+\mathfrak{m}^i)\cap G$. Fix $i\in\mathbb{Z}_{\geq 1}$ and let $1+x$ be an element of G_i. One shows that $(1+x)^p\equiv 1+px \bmod G_{i+3}$. It is now easy to conclude. □

Lemma 13.29. *Let $p>3$ be a prime number and let $G=\mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Let $x\in G\setminus G_2$ and let $y\in G_2\setminus G_3$. Then G_3 is generated by x^p and $[x,y]$ modulo G_4.*

Proof. Straightforward computation. □

We remind the reader that, as defined in Chapter 10, a p-obelisk is a finite non-abelian p-group G such that $|G:G_3|=p^3$ and $G^p=G_3$. A p-obelisk is said to be framed if, for each maximal subgroup M of G, one has $\Phi(M)=G_3$.

Lemma 13.30. *Let $p>3$ be a prime number and let $G=\mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $k\in\mathbb{Z}_{\geq 3}$, the quotient G/G_k is a framed p-obelisk.*

Proof. Let $k\in\mathbb{Z}_{\geq 3}$ and denote $\overline{G}=G/G_k$. The group $\overline{G}$ is non-abelian and it is finite. Moreover, as a consequence of Lemma 13.27, one can easily compute that $|\overline{G}:\overline{G}_3|=|G:G_3|=p^3$ and, thanks to Lemma 13.28, one has $\overline{G}^p=\overline{G}_3$. It follows that $\overline{G}$ is a p-obelisk. To show that $\overline{G}$ is framed, combine Lemma 13.29 and Proposition 10.14. □

Lemma 13.31. *Let $p>3$ be a prime number and let $G=\mathrm{S}(\Delta_p)$. Let moreover $\alpha : G\to G$ be defined by*

$$a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}\ \mapsto\ a+b\mathrm{i}-c\mathrm{j}-d\mathrm{k}.$$

Then α is a continuous automorphism of G and the map $G/G_2 \to G/G_2$ that is induced by α is equal to the inversion map $a \mapsto a^{-1}$.

Proof. The map α coincides with conjugation by i and it is therefore a continuous automorphism. Moreover, thanks to Lemma 13.27, the subgroup G_2 coincides with $(1+\mathfrak{m}^2) \cap G$. Since each element x of G can be written in the form $x = 1 + c\mathrm{j} + d\mathrm{k} + m$, with $c, d \in \mathbb{Z}_p$ and $m \in \mathfrak{m}^2$, we get that $\alpha(x) \equiv \overline{x} \bmod G_2$. The elements $\overline{x}$ and x^{-1} being equal, it follows that $\alpha(x) \equiv x^{-1} \bmod G_2$. □

Lemma 13.32. *Let $p > 3$ be a prime number and let $G = \mathrm{S}(\Delta_p)$. Define moreover $\alpha : G \to G$ by*

$$a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \ \mapsto \ a + b\mathrm{i} - c\mathrm{j} - d\mathrm{k}.$$

Then α is a topologically intense automorphism of G of order 2 and $\mathrm{int}(G) = 2$.

Proof. By Lemma 13.31, the map α is a continuous automorphism of G and, by its definition, it clearly has order 2. We prove that α is topologically intense. To this end, let H be an open subgroup of G. As a consequence of Lemma 13.19, there exists a positive integer k such that G_k is contained in H. Fix such integer k and define $K = \max\{k, 4\}$. Denote $\overline{G} = G/G_K$ and use the bar notation for the subgroups of $\overline{G}$. Denote moreover by α_K the automorphism that is induced on $\overline{G}$ by α. Then α_K induces the inversion map on $\overline{G}/\overline{G_2}$, as a consequence of Lemma 13.31 and the definition of α_K. Moreover, the class of $\overline{G}$ is at least 3 so, thanks to Lemma 13.30, the group $\overline{G}$ is a framed obelisk. It follows from Theorem 11.2 that α_K is intense, so there exists $g \in G$ such that $\alpha_K(\overline{H}) = \overline{gHg^{-1}}$. Furthermore, we have that $\alpha(H) = gHg^{-1}$ and, the choice of H being arbitrary, it follows from Proposition 13.14 that α is topologically intense. In particular, $\mathrm{int}(G)$ is even. The intensity of G is equal to 2, as a consequence of Proposition 13.15 and Theorem 5.2. □

13.5. Non-abelian groups, part II

The aim of this section is to give a proof of the following proposition. We remind the reader that, for each prime number $p > 3$, the groups $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ and $\mathrm{S}(\Delta_p)$ have been defined in Section 13.4.

Proposition 13.33. *Let $p > 3$ be a prime number and let G be a non-abelian infinite pro-p-group. Assume that $\mathrm{int}(G) > 1$. Then G is topologically isomorphic to $\mathrm{S}(\Delta_p)$.*

Until the end of Section 13.5, let the following assumptions be valid. Let $p > 3$ be a prime number and let G be an infinite non-abelian pro-p-group of intensity greater than 1. Let $(G_i)_{i\geq 1}$ denote the lower central series of G and let α be a topologically intense automorphism of G of order 2. In the proof of Proposition 13.33, we will make heavy use of results coming from Chapters 10 and 11.

Lemma 13.34. *Every solvable just-infinite pro-p-group other than $\mathbb{Z}_p$ has torsion.*

Proof. This is Proposition 6.1 in [**GSK09**]. □

Lemma 13.35. *Let P be a p-adic analytic group of dimension 3. Assume that P is both torsion-free and non-solvable. Then P is topologically isomorphic to an open subgroup of $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.*

Proof. See [**GSK09**, Section 7.3]. □

Lemma 13.36. *The group G is topologically isomorphic to an open subgroup of $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.*

Proof. The group G is a just-infinite p-adic analytic group of dimension 3, by Proposition 13.16. By Lemma 13.22, the torsion of G is trivial and so, by Lemma 13.34, the group G is not solvable. It follows from Lemma 13.35 that G is isomorphic to an open subgroup of $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. □

Lemma 13.37. *The group G is topologically isomorphic to $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.*

Proof. Let $P \in \{\mathrm{S}(\Delta_p), \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)\}$ and let $(P_i)_{i\geq 1}$ denote the lower central series of P. From the combination of Lemmas 13.24 and 13.30, we know that, for each $k \geq 3$, the quotient P/P_k is a p-obelisk. Let now H be an open subgroup of P such that G is topologically isomorphic to H as given by Lemma 13.36. By Lemma 13.18, the group H has discrete quotients of any class and, thanks to Lemma 13.17, each such quotient, of class at least 4, is a p-obelisk. The subgroup H being open, it follows from Lemma 13.19 that there exists $k \in \mathbb{Z}_{>4}$ such that P_k is contained in H so H/P_k is a p-obelisk. Proposition 10.15 yields $P = H$. □

Lemma 13.38. *Each discrete quotient of G of class at least* 6 *is a framed p-obelisk.*

Proof. Let $\overline{G}$ be a discrete quotient of G of class at least 6. Since α induces an intense automorphism of order 2 on $\overline{G}$, Lemma 13.17 yields that $\overline{G}$ is a p-obelisk. By Lemma 10.4(1), the number $\mathrm{wt}_{\overline{G}}(5)$ is equal to 2 so, by Theorem 12.2, the p-obelisk $\overline{G}$ is framed. □

We are finally ready to give the proof of Proposition 13.33. Thanks to Lemma 13.37, there are only two possibilities for the isomorphism type of G: that of $\mathrm{S}(\Delta_p)$ or that of $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. By Lemma 13.38, every discrete quotient of G of class 6 is a framed p-obelisk so, in view of Lemma 13.26, the group $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ is not isomorphic to G. It follows that G is topologically isomorphic to $\mathrm{S}(\Delta_p)$ and so the proof of Proposition 13.33 is complete.

13.6. Proving the main theorems and more

In Sections 13.6.1 and 13.6.2 we prove respectively Theorem 13.1 and Theorem 13.2. The last two theorems are the most important results of Chapter 13: we are able to draw a bridge between the two thanks to Proposition 13.39, which is proven in Section 13.6.3.

13.6.1. The proof of Theorem 13.1. Let p be a prime number. As a consequence of Proposition 13.15, the intensity of a pro-p-group divides $p-1$ and so there are no pro-2-groups of intensity greater than 1. Assume now that p is odd. Then, thanks to Corollary 13.2, each infinite abelian pro-p-group has intensity $p-1$, which, p being odd, is greater than 1. Let now G be a non-abelian infinite pro-p-group with $\mathrm{int}(G) > 1$. Then G has a discrete quotient of any class, thanks to Lemma 13.18, so Theorem 9.1 yields that p is larger than 3. By Proposition 13.33, the group G is topologically isomorphic to $\mathrm{S}(\Delta_p)$, which, by Lemma 13.32, has indeed intensity 2. The proof of Theorem 13.1 is now complete.

13.6.2. The proof of Theorem 13.2. Let $p > 3$ be a prime number and let c be a positive integer. Write $G = \mathrm{S}(\Delta_p)$ and let $(G_i)_{i\geq 1}$ denote the lower central series of G, as defined in Section 13.1. Then the group G/G_{c+1} has class c and it is finite, as a consequence of Lemma 13.19. The group G being a pro-p-group, G/G_{c+1} is a finite p-group. Moreover, by Theorem 13.1, the intensity of G is greater than 1 and so, thanks to Proposition 13.15, we get $\mathrm{int}(G/G_{c+1}) > 1$. The number c was chosen arbitrarily and therefore Theorem 13.2 is proven.

13.6.3. A bridge between finite and infinite. The purpose of Section 13.6.3 is to compare, for a fixed prime $p > 3$, the finite p-groups of intensity greater than 1 with the discrete quotients of $\mathrm{S}(\Delta_p)$.

Proposition 13.39. *Let $p > 3$ be a prime number and write $P = \mathrm{S}(\Delta_p)$. Denote by $(P_i)_{i\geq 1}$ the lower central series of P. Then there exists a function $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ with the following properties.*

1. *One has $\lim_{c\to\infty} f(c) = \infty$.*
2. *For each finite p-group G of class c with $\mathrm{int}(G) > 1$, the quotients $G/G_{f(c)}$ and $P/P_{f(c)}$ are isomorphic.*

Proof. For each positive integer c, let $\mathrm{Int}(p, c)$ denote the collection of all finite p-groups of class c and intensity greater than 1. We define $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ by mapping each element $c \in \mathbb{Z}_{>0}$ to the maximum index $m \in \mathbb{Z}_{>0}$ for which, whenever $G \in \mathrm{Int}(p, c)$, the quotients G/G_m and P/P_m are isomorphic. The map f is well-defined, thanks to Theorem 13.2, and it follows directly from the definition of f that (2) is satisfied. Moreover, thanks to Lemma 3.13, the function f is non-decreasing. We prove (1) by contradiction. Let $C \in \mathbb{Z}_{\geq 0}$ be such that, for all $c \geq C$, one has $f(c) = f(C)$. In other words, for each $c \in \mathbb{Z}_{\geq C}$, there exists $G \in \mathrm{Int}(p, c)$ such that $G/G_{f(C)}$ and $P/P_{f(C)}$ are isomorphic, but $G/G_{f(C)+1}$ and $P/P_{f(C)+1}$ are not. For all $c \geq C$, call X_c the collection of such G and note that, for each $c \geq C$, the set X_c is non-empty. Thanks to Lemma 3.13, for each $c \in \mathbb{Z}_{>C}$, we have a natural map $X_{c+1} \to X_c$, which is defined by $G \mapsto G/G_{c+1}$. The collection $\{X_c\}_{c>C}$ is thus an inverse system of non-empty sets. As a consequence of Theorem 5.1, the constant C is at least 3 and so, for each $c > C$, Theorem 8.1 yields that X_c is finite. By Lemma 13.13, the set $X = \varprojlim_{c>C} X_c$ is non-empty and therefore there exists an infinite non-abelian pro-p-group of intensity larger than 1 and which is, by construction, not isomorphic to P. Contradiction to Theorem 13.1. It follows that (2) is satisfied and the proof is complete. □

In summary, Proposition 13.39 states that, for $p > 3$, each finite p-group G with $\mathrm{int}(G) > 1$ shares a “relatively big” quotient (growing in size with the class of G) with the infinite group $\mathrm{S}(\Delta_p)$. One can then ask: if $p > 3$ and G is a finite p-group of intensity greater than 1, then “how far is G from being a quotient of $\mathrm{S}(\Delta_p)$”? More precisely, if G is a finite p-group of class c with $\mathrm{int}(G) > 1$ and f is as in Proposition 13.39, then what is the average size of $G_{f(c)}$? Is there an absolute constant B such that, for each $c \in \mathbb{Z}_{>0}$ and for each finite p-group G of class c and intensity greater than 1, one has $|G_{f(c)}| \leq p^B$? In view of Theorem 12.2, we can surely answer this question if we manage to classify, for each given prime $p > 3$, all framed p-obelisks that have an automorphism of order 2 that induces the inversion map on the Frattini quotient of the group.

Bibliography

[Ben27] H. A. Bender. A determination of the groups of order p^5. *Ann. of Math. (2) no. 1-4*, 29:61–72, 1927.

[Bla61] N. Blackburn. Generalization of certain elementary theorems on p-groups. *Proc. London Math. Soc. (3)*, 11:1–22, 1961.

[Coh07] H. Cohen. *Number theory, Volume I: Tools and Diophantine equations.* Graduate Texts in Mathematics, 239. Springer, 2007.

[DdSMS91] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p-groups.* London Mathematical Society Lecture Note Series, 157. Cambridge University Press, 1991.

[GSK09] J. Gonzalez-Sanchez and B. Klopsch. Analytic pro-p-groups of small dimensions. *J. Group Theory*, 12:711–734, 2009.

[GT06] P. Gille and Szamuely T. *Central simple algebras and Galois cohomology.* Cambridge Studies in Advanced Mathematics, 101. Cambridge University Press, 2006.

[Hup67] B. Huppert. *Endliche Gruppen I.* Springer-Verlag, 1967.

[Isa08] M. Isaacs. *Finite group theory.* Graduate Studies in Mathematics, 92. American Mathematical Society, 2008.

[KLGP97] G. Klaas, C. R. Leedham-Green, and W. Plesken. *Linear pro-p-groups of finite width.* Lecture Notes in Mathematics, 1674. Springer-Verlag, 1997.

[Laf73] T. J. Laffey. The minimum number of generators of a finite p-group. *Bull. London Math. Soc.*, 5:288–290, 1973.

[LT58] S. Lang and J. Tate. Principal homogeneous spaces over abelian varieties. *Amer. J. Math.*, 80:659–684, 1958.

[RZ10] L. Ribes and P. Zalesski. *Profinite groups. Second edition.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 40. Springer-Verlag, 2010.

[Sta13] M. Stanojkovski. Evolving groups. Master's thesis, retrieved from http://www.math.leidenuniv.nl/nl/theses/358/, 2013.

Index