INTENSE AUTOMORPHISMS OF FINITE GROUPS

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 5 september 2017
klokke 10:00 uur

door

Mima Stanojkovski
geboren te Sarajevo, Joegoslavië, in 1989

Samenstelling van de promotiecommissie:

Promotor:

Prof. dr. Hendrik W. Lenstra	Universiteit Leiden

Overige leden:

Dr. Jon González Sánchez	Euskal Herriko Unibertsitatea
Dr. Ellen Henke	University of Aberdeen
Prof. dr. Andrea Lucchini	Università degli Studi di Padova
Prof. dr. Bart de Smit	Universiteit Leiden
Prof. dr. Aad van der Vaart	Universiteit Leiden

Mojim najdražima, mami, tati, i dragom gusaru.

The background image of the cover of this thesis has been drawn by the author. The vertices of the illustrated graph represent equivalence classes of subgroups of MC(3), as defined in Section 9.2, with respect to the equivalence relation $H \sim K$ if and only if, for each $j \in \{1, 2, 3, 4\}$, the j-th widths, as defined in Section 2.3, of H and K in MC(3) are the same. An edge is drawn between two vertices if there are representatives H and K of the given vertices such that H is contained in K with index 3 or vice versa. The color of each vertex is determined by the number of conjugates in MC(3) of any representative of the equivalence class associated to the vertex. Subgroups corresponding to white, blue, red, and yellow vertices have respectively 1, 3, 9, and 27 conjugates in MC(3).

Contents

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 $\langle a,b,c,\ldots\rangle$ instead of $\langle\{a,b,c,\ldots\}\rangle$

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, see Section 1.3

$(G_i)_{i\geq 1}$, the lower central series of G, see Definitions 14 and 409

$G^n = \langle x^n \ : \ x \in G\rangle$

$\mu_n(G) = \langle x \in G \ : \ x^n = 1\rangle$

$|G : H|$, the index of H in G

$\mathrm{C}_G(X) = \bigcap_{x\in X} G_x$, where G_x is the stabilizer of x

$\mathrm{N}_G(H)$, the normalizer of H in G

$\mathrm{End}(G)$, the set of endomorphisms of 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 5.4, 9.4, and 9.6

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 $S_G \rtimes C_G$, 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 86 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 thesis 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. We define the *lower central series* $(G_i)_{i\geq 1}$ of a group G 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 we define the *(nilpotency) class* of G to be

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

In other words, the class of a group G is the number of non-trivial elements of the lower central series. The only group of class 0 is the trivial group and the groups of class 1 are the non-trivial abelian groups. 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 105 and is proven in Section 4.3. As we explain 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 125, which is proven in Section 5.2. 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 124, whose proof is given in Section 5.4. 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. 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 prove 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 164 and Lemma 206(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 results coming from Section 1.5, 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 233 and 234. Our investigation of κ-groups leads to the construction of the following example.

Example. 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 MC(3) has order 729, class 4, and it is a κ-group. Moreover, $\operatorname{int}(\mathrm{MC}(3))=2$.

In Chapter 9 we prove the following result, which is a simplified version of Theorem 231.

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

1. *One has* $\operatorname{int}(G)=2$.

2. *The group G is isomorphic to* 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

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

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 343, 375, and 390. We denote by $\mathrm{C}_G(G_4)$ the centralizer of G_4 in the group G, i.e. $\mathrm{C}_G(G_4) = \bigcap_{g \in G_4} \{x \in G : [x,g] = 1\}$.

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.
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 $\mathrm{Int}_{\mathrm{c}}(G)$ and it is itself profinite. As a consequence, several results concerning

Intensity			
c \ p	2	3	≥ 5
0	1	1	
1		$p-1$	
2		$p-1$ if G extraspecial of exponent p; 1 otherwise	
3		2 if $\lvert G : G_2 \rvert = p^2$; 1 otherwise	
4		2 if $G \cong \mathrm{MC}(3)$; 1 otherwise	2 if G is a p-obelisk with a concrete automorphism; 1 otherwise
≥ 5		1	2 if G is a p-obelisk with $\lvert G_5 \rvert = p$, $\Phi(\mathrm{C}_G(G_4)) = G_3$, and G has a concrete automorphism; 2 if G is framed p-obelisk with $\lvert G_5 : G_6 \rvert = p^2$ and G has a concrete automorphism; 1 in all other cases

intense automorphisms of finite p-groups can be generalized to topologically intense automorphisms of pro-p-groups. For example, Theorem 424 asserts that, if p is a prime number and G is a pro-p-group, then $\mathrm{Int_c}(G)$ decomposes as

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

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 451.

We conclude our introductory section by giving a “cohomological context” to intense automorphism. As we already mentioned at the beginning of this thesis, 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. 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. 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. 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 $\{\, |G : H| \,:\, H \leq G \text{ with } \mathrm{Res}^G_H(c) = 0 \,\}$ 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 $G \cong N \rtimes_\phi T$.*

A way to interpret (1) from Theorem I is the following. In some sense, the nonzero elements of a cohomology group are the obstructions to having solutions so, ideally, each subgroup H of G for which $\mathrm{Res}_H^G(c) = 0$ 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].

Generalizing Theorem I to profinite groups is an intriguing problem that is to the present day still open.

Chapter 1

Important tools

This chapter consists of a miscellaneous collection of definitions and easy facts. Throughout the whole chapter we will fully respect the notation given in the List of Symbols.

1.1 Bilinear maps and isotropic spaces

Let K be a field and let V, W, and Z be vector spaces over K. A map $\phi : V \times W \to Z$ is said to be K-*bilinear* (or simply *bilinear*) if, for all $v \in V$, the map ${}_v\phi : W \to Z$, defined by $t \mapsto \phi(v,t)$, is K-linear and, for all $w \in W$, the map $\phi_w : V \to Z$, defined by $u \mapsto \phi(u,w)$, is K-linear.

Definition 1. *Let V, W, and Z be vector spaces over a field K and let $\phi : V \times W \to Z$ be a map. Then ϕ is* non-degenerate *if it is bilinear and both maps $V \to \mathrm{Hom}(W,Z)$, defined by $v \mapsto {}_v\phi$, and $W \to \mathrm{Hom}(V,Z)$, defined by $w \mapsto \phi_w$, are injective.*

Lemma 2. *Let V, W, Z be finite-dimensional vector spaces over a field K and let $\phi : V \times W \to Z$ be a non-degenerate map. Assume moreover that $\dim_K Z = 1$. Then the dimensions of V and W over K are the same.*

Proof. The maps $V \to \mathrm{Hom}(W,Z)$ and $W \to \mathrm{Hom}(V,Z)$ are injective. It follows that $\dim V \leq \dim \mathrm{Hom}(W,Z) = \dim W \leq \dim \mathrm{Hom}(V,Z) = \dim V$, and therefore the dimensions of V and W are the same. ∎

Definition 3. *Let V and Z be vector spaces over a field K. A map $\phi : V \times V \to Z$ is* alternating *if it is bilinear and, for all $v \in V$, one has $\phi(v,v) = 0$.*

A map $\phi : V \times V \to Z$ is *antisymmetric* if it is bilinear and, for every $v, w \in V$ one has $\phi(v,w) = -\phi(w,v)$. As a direct consequence of their definitions, every alternating map is antisymmetric.

Lemma 4. *Let K be a field and let U be a K-vector space of dimension 3. Then $\wedge : U \times U \to \bigwedge^2 U$ is surjective.*

Proof. Let (x, y, z) be a basis for U over K. Then $(x \wedge y, y \wedge z, x \wedge z)$ is a basis for $\bigwedge^2 U$. Let now $a = \lambda(x \wedge y) + \mu(y \wedge z) + \nu(x \wedge z)$ be an arbitrary element of $\bigwedge^2 U$. If $a = 0$, then clearly a belongs to the image of $\wedge$, so, without loss of generality, we assume that $\lambda \in K \setminus \{0\}$. Since $(\lambda x - \mu z) \wedge (y + \lambda^{-1} \nu z) = a$, we are done. ■

Definition 5. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map. A subspace T of V is called* isotropic *if ϕ restricted to $T \times T$ equals the zero map. A subspace T is said to be* maximal isotropic *if it is isotropic and it is not properly contained in any other isotropic subspace of V.*

Definition 6. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map and let T be an isotropic subspace of V. Then $\phi_T : V/T \to \mathrm{Hom}(T, Z)$ is defined by $v + T \mapsto (t \mapsto \phi(v, t))$.*

The map ϕ_T is well defined for every isotropic subspace T of V, because $\phi(T \times T) = 0$, and it is linear.

Lemma 7. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map and let T be an isotropic subspace of V. Then T is maximal isotropic if and only if ϕ_T is injective.*

Proof. The subspace T is not maximal isotropic if and only if there exists an element $v \in V \setminus T$ such that $T \oplus Kv$ is isotropic, which happens if and only if $v + T$ belongs to the kernel of ϕ_T. ■

Definition 8. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map. Let moreover W be a linear subspace of V. The* orthogonal complement *$W^\perp$ of W with respect to ϕ is the kernel of the map $V \to \mathrm{Hom}(W, Z)$ that is defined by $v \mapsto (w \mapsto \phi(v, w))$.*

With the notation of Definition 8, the orthogonal complement of a subspace W of V is itself a subspace of V. Moreover, an alternating map being antisymmetric, $W^\perp$ is equal to the collection of all vectors $v \in V$, such that, for all $w \in W$, one has $\phi(w, v) = 0$. It follows directly from the definition that $W \subseteq (W^\perp)^\perp$ and that, if $U \subseteq W$, then $U^\perp \supseteq W^\perp$.

Lemma 9. *Let K be a field and let V and Z be vector spaces over K. Let $\phi : V \times V \to Z$ be an alternating map. Let moreover W be a linear subspace of V. Then W is isotropic if and only if $W \subseteq W^\perp$. Moreover, W is maximal isotropic if and only if $W = W^\perp$.*

Proof. Easy exercise. ■

Lemma 10. *Let V and Z be finite-dimensional vector spaces over a field K and let $\phi : V \times V \to Z$ be a non-degenerate alternating map. Assume that Z has dimension 1. Let W be a linear subspace of V. Then $\dim W + \dim W^\perp = \dim V$. Moreover, if W is maximal isotropic, then $2 \dim W = \dim V$.*

Proof. By definition of orthogonal complement, we have $\phi(W^\perp \times W) = \{0\}$, and hence the bilinear map $V/W^\perp \times W \to Z$ that is induced from ϕ is non-degenerate. It follows from Lemma 2 that $\dim V - \dim W^\perp = \dim W$. If W is maximal isotropic, then Lemma 9 yields $\dim V = 2 \dim W$. ■

Lemma 11. *Let V and Z be finite-dimensional vector spaces over a field K and let $\phi : V \times V \to Z$ be a non-degenerate alternating map. Assume that Z has dimension 1. Let W be a linear subspace of V. Then $(W^\perp)^\perp = W$.*

Proof. The subspace W is always contained in $(W^\perp)^\perp$, and therefore we always have $\dim W \leq \dim(W^\perp)^\perp$. By Lemma 10, the dimension of V is equal to both $\dim W + \dim W^\perp$ and $\dim W^\perp + \dim(W^\perp)^\perp$, and therefore $\dim W = \dim(W^\perp)^\perp$. It follows that $W = (W^\perp)^\perp$. ■

Lemma 12. *Let V and Z be finite-dimensional vector spaces over a field K and let $\phi : V \times V \to Z$ be a non-degenerate alternating map. Assume that Z has dimension 1. Let moreover X be a maximal isotropic subspace of V. Then there exists a maximal isotropic subspace Y of V such that $V = X \oplus Y$.*

Proof. Let Y be maximal among the isotropic subspaces of V that intersect X trivially. We will show that Y is maximal isotropic and that $V = X + Y$. Lemma 9 guarantees $Y \subseteq Y^\perp$ and $X = X^\perp$. We now claim that $Y^\perp$ is contained in $X + Y$. Indeed, if $v \in Y^\perp$, then $Y + Kv$ is an isotropic subspace containing Y. From the maximality of Y, it follows that $(Y + Kv) \cap X$ is non-trivial. Since $Y \cap X = \{0\}$, the element v belongs to $X + Y$, as claimed. Now, by Lemma 11, the subspaces $(Y^\perp)^\perp$ and Y are the same and, $Y^\perp$ being contained in $X + Y$, it follows that

$$Y = (Y^\perp)^\perp \supseteq (X + Y)^\perp \supseteq X^\perp \cap Y^\perp = X \cap Y^\perp.$$

In particular, $X \cap Y^\perp$ is contained in $X \cap Y$, which is trivial by definition of Y. As a consequence of Lemma 10, we get that

$$2 \dim X = \dim V \geq \dim(X \oplus Y^\perp) = \dim X + \dim Y^\perp =$$

$$\dim X + \dim V - \dim Y = 3 \dim X - \dim Y \geq 2 \dim X,$$

and therefore $\dim Y^\perp = \dim X = \dim Y$. As a result, $Y = Y^\perp$, and thus $V = X \oplus Y$. The subspace Y is maximal isotropic, by Lemma 9, and the proof is complete. ■

1.2 Commutators and the lower central series

Let G be a group. The *commutator map* on G is the map $G \times G \to G$ that is defined by

$$(x, y) \mapsto [x, y] = xyx^{-1}y^{-1}.$$

Given two subgroups H and K of G, we define $[H, K]$ to be the subgroup of G that is generated by all elements $[h, k]$, where $h \in H$, $k \in K$. The groups $[H, K]$ and $[K, H]$ are equal, because, for all $(h, k) \in H \times K$, the inverse of $[h, k]$ is $[k, h]$.

Lemma 13. *Let G be a group and let H be a subgroup of G. Let $g \in G$ and denote $[g, H] = \{[g, h] : h \in H\}$. Then $g \in \mathrm{N}_G(H)$ if and only if $[g, H]$ is contained in H.*

Proof. Let $h \in H$. Then $ghg^{-1} = [g, h]h$ and ghg^{-1} is in H if and only if $[g, h]$ is in H. ■

Definition 14. *Let G be a group. The* lower central series *of G is the series $(G_i)_{i \geq 1}$ that is obtained by defining recursively, for all $i \in \mathbb{Z}_{\geq 1}$, the subgroups $G_1 = G$ and $G_{i+1} = [G, G_i]$. One calls G_2 the* commutator subgroup *of G.*

Unless otherwise specified, we will stick to the notation from Definition 14 to refer to the lower central series of a group (see also the List of Symbols). We remark that, in Chapter 13, we will define the lower central series of a profinite group G, by taking the closures of the elements of the lower central series of G as an abstract group. In the case of finite groups, the two notions coincide.

A group G is said to be *nilpotent* if there exists $i \in \mathbb{Z}_{\geq 0}$ for which $G_{i+1} = 1$ and, in the latter case, one calls $\mathrm{cl}(G) = \min\{i \in \mathbb{Z}_{\geq 0} : G_{i+1} = 1\}$ the (*nilpotency*) *class* of G. The class of a nilpotent group is, in other words, the number of elements of the lower central series that are distinct from $\{1\}$. Another way of deciding whether a group is nilpotent is by looking at its upper central series.

Definition 15. *Let G be a group. The* upper central series *of G is the series $(Z_i)_{i \geq 0}$ that is obtained by defining recursively, for all $i \in \mathbb{Z}_{\geq 0}$, the subgroups $Z_0 = 1$ and $Z_{i+1}/Z_i = \mathrm{Z}(G/Z_i)$.*

It is a general result (see for example Chapter 4 in [Isa08]) that a group is nilpotent if and only if its upper central series stabilizes at the group itself. In other words, if G is a finite group and $(Z_i)_{i \geq 0}$ is its upper central series, then G is nilpotent if and only if there exists $r \in \mathbb{Z}_{\geq 0}$ such that $Z_r = G$. Moreover, one can show (see for example in [Isa08, §1D]) that if the group G is nilpotent, then its class is equal to $\min\{r \in \mathbb{Z}_{\geq 0} : Z_r = G\}$.

Lemma 16. *Let G be a finite group. Then G is nilpotent if and only if G is equal to the direct product of its Sylow p-subgroups.*

Proof. This is a weaker version of Hauptsatz 2.3 from [Hup67, Ch. III]. ■

Definition 17. *Let G be a group and let m, n be integers with $m \leq n$. Let moreover $\{x_i\}_{i=m}^{n}$ be a subset of G. Then*

$$\prod_{i=m}^{n} x_i = x_m x_{m+1} \ldots x_{n-1} x_n.$$

Lemma 18 (Multiplication formulas)**.** *Let G be a group and let x, y, z, t be elements of G. Let moreover n be a non-negative integer. Then the following hold.*

1. $[x, yz] = [x, y]y[x, z]y^{-1}$.
2. $[xt, y] = x[t, y]x^{-1}[x, y]$.
3. $[x^n, y][x, y]^{-n} = \prod_{s=1}^{n-1}[x, [x^{n-s}, y]]$.
4. $[x, y]^{-n}[x, y^n] = \prod_{r=1}^{n-1}[[y^r, x], y]$.

Proof. Easy exercise. ■

Lemma 19 (Three-subgroups Lemma)**.** *Let G be a group and let X, Y, Z, and N be subgroups of G such that N is normal. Assume moreover that both $[X, [Y, Z]]$ and $[Y, [Z, X]]$ are contained in N. Then $[Z, [X, Y]]$ is contained in N.*

Proof. See for example [Isa08, Corollary 4.10]. ■

Lemma 20. *Let G be a group and let $(G_i)_{i\geq 1}$ be the lower central series of G. Then, for all $h, k \in \mathbb{Z}_{\geq 1}$, one has $[G_h, G_k] \subseteq G_{h+k}$.*

Proof. We work by induction on h. If $h = 1$, we are done by definition of the lower central series. Let us now assume that $h > 1$ and, for all $k \in \mathbb{Z}_{>0}$, that $[G_{h-1}, G_k] \subseteq G_{h+k-1}$. It follows that $[G, [G_{h-1}, G_k]] \subseteq [G, G_{h+k-1}] \subseteq G_{h+k}$ and $[G_{h-1}, [G_k, G]] \subseteq [G_{h-1}, G_{k+1}] \subseteq G_{h+k}$. By Lemma 19, also $[G_h, G_k] = [[G, G_{h-1}], G_k]$ is contained in G_{h+k}. ■

Let H, K, and L be groups. Let moreover $\phi : H \times K \to L$. The map ϕ is *bilinear* if, for all $h \in H$, the map ${}_h\phi : K \to L$, defined by $x \mapsto \phi(h, x)$, is a homomorphism and, for all $k \in K$, the map $\phi_k : H \to L$, defined by $x \mapsto \phi(x, k)$, is also a homomorphisms. If ϕ is bilinear, then the *left kernel* and the *right kernel* of ϕ, are defined as

$$\ker^{\text{left}} \phi = \bigcap_{h\in H} \ker {}_h\phi, \quad \text{and} \quad \ker^{\text{right}} \phi = \bigcap_{k\in K} \ker \phi_k.$$

Assume $H = K$. Then ϕ is *alternating* if it is bilinear and, for all $x \in H$, one has $\phi(x, x) = 1$.

Definition 21. *Let H, K, and L be groups. Let moreover $\phi : H \times K \to L$. Then ϕ is* non-degenerate *if it is bilinear and both maps $H \to \operatorname{Hom}(K, L)$, defined by $h \mapsto {}_h\phi$, and $K \to \operatorname{Hom}(H, L)$, defined by $k \mapsto \phi_k$, are injective.*

Lemma 22. *Let G be a group and let H, L be subgroups of G. Let moreover $\phi : H \times L \to G$ be defined by $\phi(x, y) = [x, y]$. Then ϕ is bilinear if and only if $[H, L]$ is contained in the centre of the subgroup generated by H and L.*

Proof. This follows directly from the multiplication formulas from Lemma 18. ■

Lemma 23. *Let G be a group. Then for every $h, k \in \mathbb{Z}_{\geq 1}$ the commutator map induces a bilinear map $G_h/G_{h+1} \times G_k/G_{k+1} \to G_{h+k}/G_{h+k+1}$.*

Proof. The integers h and k being positive, it follows from Lemma 20 that both $[G_h, G_{h+k}]$ and $[G_k, G_{h+k}]$ are subgroups of G_{h+k+1}. Then G_{h+k}/G_{h+k+1} is contained in the centre of $\langle G_h, G_k \rangle / G_{h+k+1}$ and, by Lemma 22, the commutator map $G_h \times G_k \to G_{h+k}/G_{h+k+1}$ is bilinear. Again by Lemma 20, both subgroups $[G_h, G_{k+1}]$ and $[G_{h+1}, G_k]$ are contained in G_{h+k+1}. The commutator map induces hence a bilinear map $G_h/G_{h+1} \times G_k/G_{k+1} \to G_{h+k}/G_{h+k+1}$. ■

Lemma 24. *Let G be a group. Then for every $i \in \mathbb{Z}_{\geq 1}$ the commutator map induces a bilinear map $G/G_2 \times G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ whose image generates G_{i+1}/G_{i+2}.*

Proof. The commutator map induces a bilinear map $\gamma : G/G_2 \times G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ by Lemma 23. The image of γ generates G_{i+1}/G_{i+2} by definition of the lower central series of a group. ■

In Lemma 25 and throughout the whole manuscript, we write $\otimes$ instead of $\otimes_{\mathbb{Z}}$ (in concordance with the List of Symbols).

Lemma 25. *Let G be a group and let $(G_i)_{i \geq 1}$ be its lower central series. Then for every $i \in \mathbb{Z}_{\geq 1}$ the commutator map induces a surjective homomorphism of groups $G/G_2 \otimes G_i/G_{i+1} \to G_{i+1}/G_{i+2}$.*

Proof. This follows from Lemma 24 and the universal property of tensor products. ■

Lemma 26. *Let G be a group of class at most 2. Then the commutator map induces a non-degenerate alternating map $G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \to G_2$ whose image generates G_2.*

Proof. By Lemma 24, the commutator map induces a bilinear map $\gamma : G/G_2 \times G/G_2 \to G_2$ whose image generates G_2. Moreover, γ is alternating because each element of G commutes with itself. The class of G being at most 2, the subgroup G_2 is central and $\operatorname{Z}(G)/G_2$ is equal to both the right and the left kernel of γ. Then γ factors as a non-degenerate map $G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \to G_2$. ■

Lemma 27. *Let G be a group and assume that $G/\operatorname{Z}(G)$ is cyclic. Then G is abelian.*

Proof. Since the quotient $G/\operatorname{Z}(G)$ is cyclic, the commutator subgroup of G is contained in $\operatorname{Z}(G)$. In particular, G has class at most 2, and therefore, thanks to Lemma 26, the commutator map induces a non-degenerate alternating map $\gamma : G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \to G_2$ whose image generates G_2. The image of γ is trivial, because $G/\operatorname{Z}(G)$ is cyclic, and so $G = \operatorname{Z}(G)$. ■

Lemma 28. *Let G be a group and let N be a normal subgroup of G. Assume that G/N is cyclic. Then $G_2 = [G, N]$.*

Proof. Since N is normal, the subgroup $[G, N]$ is normal in G. We denote by $\overline{G} = G/[G, N]$ and we use the bar notation for the subgroups of $\overline{G}$. By definition of $\overline{G}$, the subgroup $\overline{N}$ is contained in $\operatorname{Z}(\overline{G})$, and so $\overline{G}/\operatorname{Z}(\overline{G})$ is cyclic. It follows from Lemma 27 that $\overline{G}$ is abelian, and therefore $G_2 = [G, N]$. ■

1.3 About p-groups

Let p be a prime number. A finite group G is a *p-group* if the order of G is a power of p. The trivial group is a p-group for each prime p. Moreover, as a direct consequence of Lemma 16, every finite p-group is nilpotent.

Lemma 29. *Let p be a prime number and let G be a finite p-group. Let N be a normal subgroup of G such that $N \cap \operatorname{Z}(G) = \{1\}$. Then $N = \{1\}$.*

Proof. This is Satz 7.2(a) from [Hup67, Ch. III]. ■

Lemma 30. *Let p be a prime number and let G be a finite p-group of class c. Let moreover N be a subgroup of G. Assume that, for all $i \in \{1, \ldots, c\}$, if H is a quotient of G of class i, then $\operatorname{Z}(H) = H_i$. Then N is normal if and only if there exists $i \in \mathbb{Z}_{>0}$ such that $G_{i+1} \subseteq N \subseteq G_i$.*

Proof. ($\Leftarrow$) Assume that $G_{i+1} \subseteq N \subseteq G_i$. Then the quotient N/G_{i+1} is contained in $\operatorname{Z}(G/G_{i+1})$, and so N is normal modulo G_{i+1}. In particular, N is normal in G. ($\Rightarrow$) If $N = \{1\}$, the result is clear, because G is nilpotent. We assume N is a non-trivial normal subgroup of G and we let $i \in \mathbb{Z}_{>0}$ be the minimum index such that $G_{i+1} \subseteq N$ and $G_{i+1} \neq N$. We claim that N is contained in G_i. First assume that G_i is contained in N. By the minimality of i, the subgroup G_i is equal to N, so we are done with this case. We assume now that G_i is not contained in N. Then the group $\overline{G} = G/(N \cap G_i)$ has class i and, by assumption, the center of $\overline{G}$ is equal to $\overline{G_i}$. On the other hand, $\overline{N}$ is a normal subgroup of $\overline{G}$ that has trivial intersection with $\overline{G_i}$. Lemma 29 yields $\overline{N} = \{1\}$, and thus $N \subseteq G_i$. ■

Lemma 31. *Let p be a prime number and let G be a finite p-group. Assume that G/G_2 is cyclic. Then G is abelian.*

Proof. This is a weaker version of Hilfssatz 7.1(b) from [Hup67, Ch. III.7]. ■

Definition 32. *Let G be a group. Then, for all $n \in \mathbb{Z}$, define*

$$G^n = \langle x^n \ : \ x \in G \rangle \quad \textit{and} \quad \mu_n(G) = \langle x \in G \ : \ x^n = 1 \rangle.$$

Let p be a prime number. The *Frattini subgroup* $\Phi(G)$ of a finite p-group G is the unique normal subgroup of G minimal with the property that $G/\Phi(G)$ is elementary abelian: in other words $\Phi(G) = G^p[G, G]$.

Lemma 33. *Let p be a prima number and let G be a finite p-group. Let H be a subgroup of G such that $G = H\Phi(G)$. Then $H = G$.*

Proof. This is a weaker reformulation of Satz 3.2(a) from [Hup67, Ch. III]. ■

Lemma 34. *Let p be a prime number and let G be a finite p-group. Then the map $\phi : \mathrm{Aut}(G) \to \mathrm{Aut}(G/\Phi(G))$ given by $\alpha \mapsto (x\Phi(G) \mapsto \alpha(x)\Phi(G))$ is a well-defined homomorphism. Moreover, the kernel of ϕ is a p-group.*

Proof. This is a reformulation of Satz 3.18 from [Hup67, Ch. III]. ■

Lemma 35. *Let p be a prime number and let H be a finite p-group. Let moreover K and N be normal subgroups of H such that $K \subseteq N$ and $K \neq N$. Then there exists a normal subgroup M of H such that $K \subseteq M \subseteq N$ and $|N : M| = p$.*

Proof. See [Isa08, Lemma 1.23]. ■

Lemma 36. *Let p be a prime number and let G be a finite p-group. Assume that $|G : G_2| = p^2$. Then one of the following holds.*

1. *The group G is abelian.*

2. *The group G_2 is equal to $\Phi(G)$.*

Proof. Assume that G is not abelian. It follows from Lemma 31 that G/G_2 has exponent p and so G^p is contained in G_2. In particular, we have that $G_2 = G_2G^p = \Phi(G)$. ■

Definition 37. *Let G be a group and let p be a prime number. The p-*central series *of G is the series $(P_i(G))_{i\geq 1}$ that is obtained by defining recursively, for all $i \in \mathbb{Z}_{\geq 1}$, the subgroups $P_1(G) = G$ and $P_{i+1}(G) = [G, P_i(G)]P_i(G)^p$.*

We remark that, if p is a prime number and G is a finite p-group, then saying that the lower central series of G coincides with its p-central series is equivalent to saying that all quotients of consecutive elements of the lower central series have exponent dividing p.

1.4 Extraspecial p-groups

In Section 1.4 we explore the world of extraspecial p-groups, a class of groups that have been widely studied and whose structure is very well-understood (see for example [Hup67, Ch. III.13]). Given a group G, we recall that $(G_i)_{i\geq 1}$ denotes its lower central series (see Section 1.2).

Definition 38. *Let p be a prime number and let G be a finite p-group. Then G is* extraspecial *if G_2 is central and $\mathrm{Z}(G)$ is cyclic of order p.*

Lemma 39. *Let p be a prime number and let G be a finite extraspecial p-group. If G is non-abelian, then $\mathrm{Z}(G)$ and G_2 are equal and they both have order p.*

Proof. Straightforward. ■

Lemma 40. *Let p be a prime number and let G be a finite p-group. Assume that G has class at most 2 and that the exponent of G_2 divides p. Then $\Phi(G)$ is contained in $\mathrm{Z}(G)$.*

Proof. By Lemma 26, the map $G/\mathrm{Z}(G) \times G/\mathrm{Z}(G) \to G_2$ that is induced by the commutator map is bilinear. Let now $g, x \in G$. Then $[g^p, x] = [g, x]^p = [g, x^p]$ and $[g, x]^p = 1$, since the exponent of G_2 divides p. It follows that $G/\mathrm{Z}(G)$ is annihilated by p and thus $\Phi(G) \subseteq \mathrm{Z}(G)$. ■

Lemma 41. *Let p be a prime number and let G be an extraspecial p-group. Then there exists $n \in \mathbb{Z}_{\geq 0}$ such that $|G| = p^{2n+1}$.*

Proof. This is a reformulation of Satz 13.7(c) from [Hup67, Ch. III]. ■

Lemma 42. *Let p be a prime number and let X, Y, Z be finite-dimensional vector spaces over $\mathbb{F}_p$ such that $\dim_{\mathbb{F}_p} Z = 1$. Let moreover $\theta : X \times Y \to Z$ be a non-degenerate map. Call $G = G(Z, Y, X, \theta)$ the set $Z \times Y \times X$ together with the multiplication defined by $(z, y, x)(z', y', x') = (z + z' + \theta(x, y'), y + y', x + x')$. Then the following hold.*

1. *One has that G is an extraspecial p-group and, if p is odd, then G has exponent p.*

2. *The centre of G is $Z \times \{0\} \times \{0\}$.*

3. *The commutator map $G \times G \to G$ is given by*

$$((z, y, x), (z', y', x')) \mapsto [(z, y, x), (z', y', x')] = (\theta(x, y') - \theta(x', y), 0, 0).$$

Proof. Straightforward. ■

Lemma 43. *Let p be a prime number and let G be an extraspecial p-group of exponent p. Then there exist finite-dimensional vector spaces X, Y, Z over $\mathbb{F}_p$, with Z of dimension 1, and a non-degenerate map $\theta : X \times Y \to Z$ such that $G \cong G(Z, Y, X, \theta)$.*

Proof. If G is abelian, we take $X = Y = 0$, $Z = G$, and θ to be the zero map. Since every group of exponent 2 is abelian, we are done when $p = 2$. Assume now that p is odd and that G has class 2. In this case $\mathrm{Z}(G) = G_2$ and $V = G/\,\mathrm{Z}(G)$ is a finite-dimensional vector space over $\mathbb{F}_p$, as a consequence of Lemma 40. Write $Z = \mathrm{Z}(G)$ and let $\pi : G \to V$ denote the canonical projection. By Lemma 26, the commutator map on G induces a non-degenerate map $\phi : V \times V \to Z$. Let now X be a maximal isotropic subspace of V. By Lemma 12 there exists an isotropic subspace Y of V such that $V = X \oplus Y$. It follows that the map $\phi_{|X\times Y} : X \times Y \to Z$ is non-degenerate. Now, we have that $0 = \phi(X \times X) = [\pi^{-1}(X), \pi^{-1}(X)]$, and so $\pi^{-1}(X)$ is abelian of exponent p. As a result, the sequence $0 \to Z \to \pi^{-1}(X) \to X \to 0$ of $\mathbb{F}_p$-modules is split and there is a homomorphism $s : X \to \pi^{-1}(X)$ such that $\pi \circ s = \mathrm{id}_X$. The same argument applies to Y and there exists therefore a homomorphism $t : Y \to \pi^{-1}(Y)$ such that $\pi \circ t = \mathrm{id}_Y$. To conclude, we denote $\theta = \phi_{|X\times Y}$ and we define $\psi : G(Z, Y, X, \theta) \to G$ by $(z, y, x) \mapsto zt(y)s(x)$. It is not difficult at this point to check that ψ is an isomorphism. ■

Proposition 44. *Let p be a prime number. Let moreover X, Y, Z, A, B, C be finite-dimensional vector spaces over $\mathbb{F}_p$ with $\dim Z = \dim C = 1$. Let $\theta : X \times Y \to Z$ and $\psi : A \times B \to C$ be non-degenerate maps. Let f, g, h respectively belong to $\mathrm{Hom}(X, A), \mathrm{Hom}(Y, B), \mathrm{Hom}(Z, C)$ and assume that the following diagram is commutative.*

$$\begin{tikzcd}
X \times Y \arrow[r, "\theta"] \arrow[d, shift right=2, "f"'] \arrow[d, shift left=2, "g"] & Z \arrow[d, "h"] \\
A \times B \arrow[r, "\psi"] & C
\end{tikzcd}$$

Then $(h, g, f) : G(Z, Y, X, \theta) \to G(C, B, A, \psi)$ is a homomorphism of groups and, if f, g, h are isomorphisms, then (h, g, f) is an isomorphism.

Proof. Straightforward. ■

Lemma 45. *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 46. *Let p be a prime number and let G be an extraspecial p-group. Let Δ denote the subgroup of $\mathrm{Aut}(G)$ consisting of those automorphisms of G that induce the identity on G/G_2. Then $\Delta = \mathrm{Inn}(G)$.*

Proof. If G is abelian, then $\mathrm{Inn}(G)$ is trivial and we are done. Assume now that G is non-abelian. Then, by Lemma 39, the subgroups $\mathrm{Z}(G)$ and G_2 are equal and they both have order p. It follows from Lemma 26 that the commutator map induces a non-degenerate map $G/G_2 \times G/G_2 \to G_2$ and so the homomorphism $G/G_2 \to \mathrm{Hom}(G/G_2, G_2)$, defined by $t \mapsto (x \mapsto [t, x])$, is injective. Thanks to Lemma 40, the quotient G/G_2 is elementary abelian and thus $G/G_2 \to \mathrm{Hom}(G/G_2, G_2)$ is an isomorphism. Now, by Lemma 60, each element δ of Δ restricts to the identity on G_2 and so we derive from Lemma 45 that, for each element $\delta \in \Delta$, there exists $t \in G$ such that, for all $x \in G$, one has $\delta(x) = [t, x]x = txt^{-1}$. In particular, Δ is contained in $\mathrm{Inn}(G)$. The inclusion $\mathrm{Inn}(G) \subseteq \Delta$ is clear and so the proof is complete. ■

1.5 Regular p-groups

Most of the results from this section are taken from [Hup67], an excellent reference for getting acquainted with regular p-groups. We recall here briefly the *Hall-Petrescu formula* and we refer to Appendix *A* from [DdSMS91] for more detail. We also refer to Definition 17 for a clear interpretation of the Hall-Petrescu formula.

Lemma 47 (Hall-Petrescu formula)**.** *Let G be a group and let $(G_i)_{i\geq 1}$ denote its lower central series. Let moreover x and y be elements of G. Then, for all $n \in \mathbb{Z}_{>0}$, there exists $(c_k)_{k=2}^n \in \prod_{k=2}^n G_k$ such that*

$$(xy)^n = x^n y^n \prod_{k=2}^{n} c_k^{\binom{n}{k}}.$$

Proof. See [DdSMS91, Appendix A]. ■

Corollary 48. *Let p be a prime number and let G be a group. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for all $x, y \in G$, one has $(xy)^p \equiv x^p y^p \bmod G_2^p G_p$.*

Proof. This follows directly from Lemma 47. ■

Definition 49. *Let p be a prime number. A finite p-group G is* regular *if, for all $x, y \in G$, there exists $\gamma \in [\langle x, y\rangle, \langle x, y\rangle]^p$ such that $(xy)^p = x^p y^p \gamma$.*

Lemma 50. *Let p be a prime number and let G be a finite p-group of nilpotency class at most $p-1$. Then G is regular.*

Proof. The class of each subgroup of G is at most that of G. The result now follows directly from Corollary 48. ■

Let p be a prime number and let G be a p-group. We will denote by ρ the map $G \to G$ that is defined by $x \mapsto x^p$. We remark that the map ρ is in general not a homomorphism and that $G^{p^k} = \langle \rho^k(G) \rangle$, for any integer k. We stick to the notation from the List of Symbols.

Lemma 51. *Let p be a prime number and let G be a finite p-group. Assume that G is regular and that G_2 has exponent dividing p. Then ρ is an endomorphism of G.*

Proof. This follows directly from the definition of regularity. ■

Lemma 52. *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 Satz 10.5 and Satz 10.7(a) from [Hup67], Chapter 3. ■

We remark that p-groups satisfying conditions 1–3 from Lemma 52 are often referred to as *power abelian.*

Lemma 53. *Let p be a prime number and let G be a finite p-group. If $|G : G^p| < p^p$, then G is regular.*

Proof. The lemma is a simplified version of Satz 10.13 from [Hup67], Chapter 3. ■

Lemma 54. *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 $[\rho^r(M), \rho^s(N)] = \rho^{r+s}([M, N])$.*

Proof. See [Hup67, Satz 10.8(a) from Ch. 3]. ■

Lemma 55. *Assume G is 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 3. ■

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 68, 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 thesis, 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. To conclude, we remark that we have here adopted the additive notation for the abelian group G, but this will sadly not be the case through the whole thesis. 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 77.

Definition 56. *Let A and G be groups. An* action of A on G *is a homomorphism $A \to \mathrm{Aut}(G)$.*

Definition 57. *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 58. *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 59. *Let A be a group acting on two sets T and Z. A map $\phi : T \to Z$ is said to* respect the action of A *if, for all $t \in T$, $a \in A$, one has $\phi(at) = a\phi(t)$.*

Definition 60. *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 61. *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. Let $(x, y) \in X \times Y$ and $a \in A$. Then one has

$$a\phi(x, y) = \phi(ax, ay) = \phi(\chi(a)x, \psi(a)y) = \chi(a)\psi(a)\phi(x, y) = (\chi\psi)(a)\phi(x, y).$$

Since χ and ψ are homomorphisms, the action of A on $\phi(X \times Y)$ is through $\chi\psi$. ■

Lemma 62. *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.*

The elements of the lower central series of a group are characteristic subgroups and, for each $i \in \mathbb{Z}_{\geq 1}$, the quotient G_i/G_{i+1} is abelian. Lemma 62 is thus well-stated.

Proof. We will 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. By Lemma 24 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, by Lemma 61, the group A acts on G_i/G_{i+1} through $\chi\chi^{i-1} = \chi^i$. ■

Lemma 63. *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 $a \in A$. If ϕ is surjective, then, for each $h \in H$ there exists $g \in G$ such that $\phi(g) = h$. If, moreover, the action of A is respected by ϕ, then $ah = a\phi(g) = \phi(ag) = \phi(\chi(a)g) = \chi(a)\phi(g) = \chi(a)h$. ■

Lemma 64. *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 $\omega : \mathbb{F}_p^* \to \mathbb{Z}_p^*$.

The last is a classical result, which can be found for example in [Coh07, §4.3]. The homomorphism $\omega : \mathbb{F}_p^* \to \mathbb{Z}_p^*$ is called the *Teichmüller character* at p and its image is contained in the torsion subgroup of $\mathbb{Z}_p^*$. (For a reminder of the notation, see the List of Symbols.) Moreover, if p is odd, then $\omega(\mathbb{F}_p^*)$ is in fact equal to the torsion subgroup of $\mathbb{Z}_p^*$; for more information see for example Section 4.3 from [Coh07].

We remark that, if V is a vector space over $\mathbb{F}_p$, then, for each $v \in V$ and for each $a \in \mathbb{F}_p^*$, one has $av = \omega(a)v$. It follows that the natural action of $\mathbb{F}_p^*$ on a vector space over $\mathbb{F}_p$ is through the Teichmüller character.

Lemma 65. *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 $\lambda(a) \neq \mu(a)$. As a consequence of Lemma 64, 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 66. *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 65. 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 $x = 0$. As the choice of x was arbitrary, we get $G = \{0\}$. ■

Definition 67. *Let G be a group and let N be a normal subgroup of G. A subgroup H of G is a* complement of N in G *if $N \cap H = \{1\}$ and $NH = G$.*

Theorem 68. *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 68. 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 $I_\mu = \ker \sigma_\mu$.

Lemma 69. *One has $R = I_\lambda + I_\mu$.*

Proof. We will construct an invertible element in $I_\lambda + I_\mu$. Let $a \in A$ be as in Lemma 65. The element $\lambda(a) - \mu(a) = -(a - \lambda(a)) + (a - \mu(a))$ belongs to $I_\lambda + I_\mu$, because $a - \lambda(a) \in I_\lambda$ and $a - \mu(a) \in I_\mu$, and $\lambda(a) - \mu(a)$ is invertible because of the choice of a. ■

Lemma 70. *The subgroup $\iota(N)$ has an A-stable complement.*

Proof. Let $(e, f) \in I_\lambda \times I_\mu$ be such that $e + f = 1$ in R; the pair (e, f) exists thanks to Lemma 69. 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, the cardinalities of $e(G)$ and $\iota(N)$ being respectively $|G : N|$ and $|N|$, it follows that $G = e(G) \oplus \iota(N)$. The subgroup $e(G)$ is thus a complement of $\iota(N)$ in G. Furthermore, 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 A-stable. ■

Lemma 71. *There exists a unique A-stable complement of $\iota(N)$.*

Proof. The subgroup $\iota(N)$ has an A-stable complement in G, by Lemma 70; assume it has two. 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 63, 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 66 that $r = 0$, as claimed. In particular, $f = f'$, and so $\iota(N)$ has a unique A-stable complement in G. ■

In view of Lemma 71, Theorem 68 is proven.

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

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

We will keep the notation we just introduced until the end of Section 2.2. We remind the reader about the List of Symbols, at the beginning of this thesis.

Lemma 72. *One has $G^+ \cap G^- = \{1\}$.*

Proof. Let $a \in G^+ \cap G^-$. Then we have $a = \alpha(a) = a^{-1}$, so $a^2 = 1$. The order of G being odd, it follows that $a = 1$. ■

Proposition 73. *The set G^+ is a group. Moreover, G^+ acts by conjugation on the set G^-.*

Proof. The subset G^+ is a group, because α is a homomorphism. Let now g be in G^+ and a in G^-. Then we have that

$$\alpha(gag^{-1}) = \alpha(g)\alpha(a)\alpha(g)^{-1} = ga^{-1}g^{-1} = (gag^{-1})^{-1},$$

and so gag^{-1} belongs to G^-. ■

Lemma 74. *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 $b \in G^-$. Since the order of G is odd, there exists a unique a in G such that $a^2 = b$. The element a belongs to $\langle b \rangle$, ando so $\alpha(a) = a^{-1}$. As a consequence, we have that $a\alpha(a)^{-1} = a^2 = b$. We have proven that ϕ is a bijection, from which it follows that $|G|/|G^+| = |G^-|$. ■

Lemma 75. *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 $ty^{-1} = z^{-1}x$. By Lemma 73, the set G^+ is a subgroup of G, so $z^{-1}x \in G^+$. As a consequence, we get that $ty^{-1} = \alpha(ty^{-1}) = t^{-1}y$. It follows that $t^2 = y^2$ so, the order of G being odd, the elements t and y coincide. Consequently, $(x, y) = (z, t)$ and the map is injective. Now by Lemma 74, the cardinalities of $G^+ \times G^-$ and G are the same and the given multiplication is also surjective. ■

Corollary 76. *Assume G is abelian. Then $G = G^+ \oplus G^-$.*

Proof. The sets G^+ and G^- are both subgroups of G, because G is abelian, and $G^+ \cap G^- = \{1\}$, by Lemma 72. It follows from Lemma 75 that $G = G^+ \oplus G^-$. ■

Lemma 77. *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. From the assumptions it follows that, for each $x \in G$, the element $\alpha(x)x$ belongs to N. Since the order of G is odd, if $x \in G^+$, then x is actually an element of N. It follows that G^+ is contained in N, but N is contained in G^- by assumption. As a consequence of Lemma 72, the subgroup G^+ is trivial so, as a consequence of Lemma 75, the group G is equal to G^-. Let now x and y be elements of G. Then we have that

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

and therefore $[x, y] = 1$. The choice of x and y being arbitrary, the group G is abelian. ■

Lemma 78. *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 $G = G^+$.*

Proof. Let $x \in G$. Then $\alpha(x)x^{-1}$ is an element of N. If x belongs to G^-, then x^{-2} belongs to N so, the order of G being odd, x itself is an element of N. It follows that G^- is a subset of N. The group N is however contained in G^+ and, as a consequence of Lemma 72, one gets $G^- = \{1\}$. It follows from Lemma 75 that $G = G^+$. ■

Lemma 79. *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. Since f and g are homomorphisms respecting the action of A, it suffices to prove the surjectivity of g'. Let $\gamma \in \Gamma^+$. Then there exists $x \in G$ such that $g(x) = \gamma$ and, by Lemma 75, there exists $(a, b) \in G^+ \times G^-$ such that $x = ab$. Now, $(g(a), g(b)) \in \Gamma^+ \times \Gamma^-$, because g respects the action of A, and $\gamma = g(x) = g(ab) = g(a)g(b)$. It follows that $g(b) = g(a)^{-1}\gamma$, and so $g(b) \in \Gamma^+ \cap \Gamma^-$. Thanks to Lemma 72, we get that $g(b) = 1$, so γ is equal to $g(a)$. ■

Lemma 80. *Let p be an odd prime number and assume that G is a finite p-group. Let $(G_i)_{i\geq 1}$ denote the lower central series of G and assume that the automorphism of G/G_2 that is induced by α equals the inversion map $x \mapsto x^{-1}$. 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 positive integers. Then the following hold.*

1. *Let $j \in \mathbb{Z}_{\geq 1}$. Then $H^+ \cap G_j \neq H^+ \cap G_{j+1}$ if and only if $H \cap G_j \neq H \cap G_{j+1}$ and $j \in \mathcal{E}$.*
2. *One has $|H^+| = \prod_{j\in\mathcal{E}} |H \cap G_j : H \cap G_{j+1}|$.*
3. *One has $|H^-| = \prod_{j\in\mathcal{O}} |H \cap G_j : H \cap G_{j+1}|$.*

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. We first prove (1) and (2) together. If $j \in \mathbb{Z}_{\geq 1}$, we note that $(H \cap G_j)^+ = H^+ \cap G_j$, so Lemma 79 yields

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

From Lemma 62 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, Lemma 72 yields that the cardinality of $(G_j/G_{j+1})^+$ is equal to 1. Since, for all $j \in \mathbb{Z}_{\geq 1}$, the groups V_j and $(H \cap G_j)G_{j+1}/G_{j+1}$ are isomorphic, it follows that, for each odd j, the cardinality of V_j^+ is equal to 1. Moreover, 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

$$|H^+| = \prod_{j\geq 1} |V_j^+| = \prod_{j\in\mathcal{E}} |V_j^+| = \prod_{j\in\mathcal{E}} |V_j|.$$

This proves (1) and (2). We now prove (3). By Lemma 74, the cardinality of $|H^-|$ is equal to $|H|/|H^+|$. Since $|H| = \prod_{j\geq 1} |V_j|$, it follows from (2) that

$$|H^-| = \frac{\prod_{j\geq 1} |V_j|}{\prod_{j\in\mathcal{E}} |V_j|} = \prod_{j\in\mathcal{O}} |V_j|.$$

■

Lemma 81. *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 $G^+ \operatorname{N}_G(H)$.*

Proof. Let $I = \operatorname{N}_G(H)$; then I is A-stable, because H is. We first prove that (1) implies (2). Assume that the subgroup gHg^{-1} is A-stable, so $\alpha(gHg^{-1}) = gHg^{-1}$. In particular, the element $g^{-1}\alpha(g)$ belongs to I, and thus $\alpha(gI) = \alpha(g)I = gI$. Since the cardinality of I is odd and A has order 2, 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; we prove (1). Since g belongs to $G^+ \operatorname{N}_G(H)$, there exists $(\gamma, n) \in G^+ \times \operatorname{N}_G(H)$ 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 (see Section 1.2). 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 $\operatorname{dpt}_G(x)$. Let now H be a subgroup of G and let j be a positive integer. The *j-th width of H in G* is

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

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 $p^{\operatorname{wt}_H^G(j)}$. An index j is a *jump of H in G* if $\operatorname{wt}_H^G(j) \neq 0$ and, whenever it will be clear that j is a jump of H in G, we will refer to $\operatorname{wt}_H^G(j)$ as the *width of j in G*. If $G = H$, we denote the *j-th width of G* by $\operatorname{wt}_G(j)$ instead of $\operatorname{wt}_G^G(j)$ and, in several results, we will lighten the notation even further by writing $w_j = \operatorname{wt}_G(j)$. The *width of G* is defined as $\operatorname{wt}(G) = \max_{i\geq 1} \operatorname{wt}_G(i)$; for a generalization to general pro-p-groups, see [KLGP97].

Lemma 82. *Let p be a prime number and let j be a positive integer. Let moreover G be a finite p-group and let H be a subgroup of G. Then j is a jump of H in G if and only if H contains an element of depth j in G.*

Proof. Straightforward. ■

Lemma 83. *Let p be a prime number. Let moreover G be a finite p-group and let H be a subgroup of G. Then, for all $\alpha \in \operatorname{Aut}(G)$, the groups H and $\alpha(H)$ have the same jumps in G.*

Proof. Let α be an automorpshism of G and let j be a positive integer. By Lemma 82, the integer j is a jump of H if and only if there exists $x \in H$ such that $\mathrm{dpt}_G(x) = j$. As the elements of the lower central series are characteristic in G, we have that $\mathrm{dpt}_G(\alpha(x)) = \mathrm{dpt}_G(x)$, and thus we are done. ■

Lemma 84. *Let p be a prime number and let G be a finite p-group. Let moreover H be a subgroup of G and call $\mathcal{J}$ the collection of all jumps of H in G. Then $|H| = \prod_{j\in\mathcal{J}} p^{\mathrm{wt}_H^G(j)}$.*

Proof. It follows directly from the definitions of jumps. ■

In the next proposition, we use the notation introduced in Section 2.2.

Lemma 85. *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 automorphism of G/G_2 that is induced by α equals the inversion map $x \mapsto x^{-1}$. 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. Assume that the induced action of A on G/G_2 is through χ. 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. Apply the new dictionary to Lemma 80. ■

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 $\mathrm{Aut}(G)$.

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

Theorem 86. *Let p be a prime number and let G be a finite p-group. Then $\mathrm{Int}(G)$ is isomorphic to $S \rtimes C$, 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. Most of the notation used appears in the List of Symbols, at the beginning of this thesis.

Proposition 87. *Let G be a group. Then $\mathrm{Inn}(G) \subseteq \mathrm{Int}(G) \subseteq \mathrm{Aut}(G)$ and $\mathrm{Int}(G)$ is normal in $\mathrm{Aut}(G)$.*

Proof. Straightforward application of the definitions. ■

We recall that, if A is a group acting on a set X, a subset Y of X is A-stable if the action of A on X restricts to an action of A on Y (see Section 2.1).

Lemma 88. *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* $\alpha \mapsto (xN \mapsto \alpha(x)N)$.

3. *Assume N is contained in* $\mathrm{Z}(G)$*. Then the image of the homomorphism* $\mathrm{Int}(G) \to \mathrm{Aut}(N)$*, sending α to $\alpha_{|N}$, is contained in* $\mathrm{Int}(N)$.

Proof. (1) Intense automorphisms send every subgroup to a conjugate and therefore each normal subgroup to itself. (2) The map is well-defined as a consequence of (1) and it is a homomorphism by construction. (3) This follows from the fact that conjugation in G restricts to the trivial map on each subgroup of $\mathrm{Z}(G)$. ■

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

Lemma 89. *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 $\alpha(v) = \mu(\alpha, v)v$. We will show that $\mu(\alpha, v)$ is independent of the choice of v. To this end, let $\alpha \in \mathrm{Int}(V)$ and let v and w be elements of $V \setminus \{0\}$. If v and w are linearly dependent, then $\mu(\alpha, v) = \mu(\alpha, w)$. We assume that v and w are linearly independent. From the linearity of α, it follows that $\mu(\alpha, v+w)(v+w) = \mu(\alpha, v)v + \mu(\alpha, w)w$. The vectors v and w are linearly independent, so $\mu(\alpha, v) = \mu(\alpha, v+w) = \mu(\alpha, w)$, as required. We fix $v \in V \setminus \{0\}$ and define $\mu : \mathrm{Int}(V) \to \mathbb{F}_p^*$ by $\alpha \mapsto \mu(\alpha, v)$. The map μ is well-defined and it 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 $\omega(\mathbb{F}_p^*)$ by construction. The uniqueness of λ follows from Lemma 66. ■

We recall that, an action of a group C on a group B is a homomorphism $C \to \mathrm{Aut}(B)$ (see Section 2.1).

Definition 90. *Let C be a finite group acting on a finite group B. Assume moreover that both B and C act on a set X. The actions are said to be* compatible *if for all $x \in X$, $b \in B$, and $c \in C$, one has $c(bx) = (cb)(cx)$.*

Lemma 91 (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 92 (An equivalent condition)**.** *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.*

Proof. (2) ⇒ (1) By assumption there exists an element $b \in N$ such that $bHb^{-1} = \alpha(bHb^{-1}) = \alpha(b)\alpha(H)\alpha(b)^{-1}$. Define $a = \alpha(b)^{-1}b$. (1) ⇒ (2) 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 91, there exists an element of X that is fixed by α. ∎

Lemma 93. *Let G be a finite group and let α be an automorphism of G of order coprime to $|G|$. Then $\alpha \in \mathrm{Int}(G)$ if and only if each subgroup of G has an $\langle\alpha\rangle$-stable conjugate.*

Proof. Take $N = G$ in Lemma 92. ∎

Lemma 94. *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 93, 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

Let p be a prime number and let G be a finite p-group. We recall that $\Phi(G) = [G,G]G^p$ and so $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$ (see Section 1.3). In Section 3.2 we build the foundation for our theory and we give the dictionary that we will use throughout the whole thesis. We will also prove the following result.

Proposition 95. *Let G be a finite 2-group. Then $\mathrm{Int}(G)$ is a finite 2-group.*

Definition 96. *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 composition of the following.*

- *The homomorphism $\mathrm{Int}(G) \to \mathrm{Int}(G/\Phi(G))$ from Proposition 88(2).*
- *The homomorphism $\lambda : \mathrm{Int}(G/\Phi(G)) \to \mathbb{Z}_p^*$ from Proposition 89.*

Lemma 97. *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 $\mathrm{Int}(G) = \ker \chi_G = \{1\}$ and $\{1\}$ is a Sylow p-subgroup of $\mathrm{Int}(G)$. Assume now G is non-trivial and set $V = G/\Phi(G)$. By Lemma 89, the map $\lambda : V \to \mathrm{Int}(V)$ is injective and so, with the notation of Lemma 34, the subgroup $\ker \chi_G$ is equal to $\mathrm{Int}(G) \cap \ker \phi$. As a consequence of Lemma 34, the kernel of χ_G is a normal Sylow p-subgroup of $\mathrm{Int}(G)$. Since $\mathrm{Int}(G)$ acts on the collection of its Sylow p-subgroup in a transitive manner, $\mathrm{Int}(G)$ has a unique Sylow p-subgroup, namely $\ker \chi_G$. ■

Definition 98. *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 the value $|\mathrm{Int}(G) : \ker \chi_G|$ and it is denoted by $\mathrm{int}(G)$.*

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.

Lemma 99. *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 $\mathrm{int}(G)$ divides $p-1$ and $\ker \chi_G$ has a cyclic complement in $\mathrm{Int}(G)$ of order $\mathrm{int}(G)$.*

Proof. The image of χ_G is a subgroup of $\omega(\mathbb{F}_p^*)$, which has order $p-1$. It follows that $\mathrm{int}(G)$ divides $p-1$. Now, by Proposition 97, the kernel of χ_G is the unique Sylow p-subgroup of G and it is therefore normal. The group $\ker \chi_G$ has a complement C in $\mathrm{Int}(G)$, by the Schur-Zassenhaus theorem, and C is cyclic because it is isomorphic to a subgroup of $\mathbb{F}_p^*$. ■

Proposition 95 now follows from Lemmas 97 and 99.

The major goal of this thesis if classifying all pairs (p, G) where p is a prime number and G is a finite p-group with $\mathrm{int}(G) > 1$. Starting from the next chapter, 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

The main result of Section 3.3 is the following.

Proposition 100. *Let p be a prime number and let G be a finite non-trivial abelian p-group. Then $\mathrm{int}(G) = p - 1$.*

Lemma 101. *Let p be a prime number and let G be a finite p-group. Let N be a normal subgroup of G. If $N \neq G$, then $\mathrm{int}(G)$ divides $\mathrm{int}(G/N)$.*

Proof. Assume $N \neq G$; then G is non-trivial. Let $\phi : \mathrm{Int}(G) \to \mathrm{Int}(G/N)$ be as in Lemma 88(2). The subgroup $N\Phi(G)$ is different from G, thanks to Lemma 33, and therefore $\Phi(G)N/N \neq G/N$. The groups $(G/N)/\Phi(G/N)$ and $G/(\Phi(G)N)$ being isomorphic (and non-trivial!), it follows that $\chi_G = \chi_{G/N} \circ \phi$. The image of χ_G is a subgroup of 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 102. *Let p be a prime number and let G be a finite abelian p-group. Let α be intense 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 $\mathrm{Int}(G) = \ker\chi_G \rtimes \Omega$, 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 100 is a special case of Lemma 102. Moreover, Theorem 86 is proven by combining Lemmas 97, 99, and Proposition 100.

Corollary 103. *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. Let $\zeta : \mathrm{Int}(G) \to \mathrm{Int}(\mathrm{Z}(G))$ be the map from Lemma 88(3) and define $\sigma = \chi_{\mathrm{Z}(G)_{|\langle\zeta(\alpha)\rangle}} \circ \zeta_{|\langle\alpha\rangle}$. Lemma 97 yields that $\langle\alpha\rangle$ acts on $\mathrm{Z}(G)$ through σ. ■

Lemma 104. *Let p be a prime number and let G be a finite p-group. Let α be intense of order dividing* $\mathrm{int}(G)$ *and write $\chi = \chi_{G_{|\langle\alpha\rangle}}$. 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 $\langle\alpha\rangle$ on G_i/G_{i+1} is through χ^i.*

Proof. Denote $A = \langle\alpha\rangle$. As a consequence of Proposition 88(2), the action of A on G induces an action of A on G/G_2. By Proposition 102, the action of A on G/G_2 is through χ. We now apply Lemma 62. ■

Chapter 4

Intensity of groups of class 2

The main goal of this thesis, 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. We remind the reader that a finite p-group is always nilpotent and that its (nilpotency) class is defined to be the number of non-trivial successive quotients of the lower central series (see Section 1.2). 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 105. *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 and let G denote a finite p-group of nilpotency class 2 (see Section 1.2). 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 and p is odd (see Sections 3.2 and 3.3). We will keep this notation until the end of this section, together with the one from the List of Symbols.

Lemma 106. *Assume G_2 has exponent p. Then $\Phi(G)$ is central and A acts on G_2 is through χ^2.*

Proof. The Frattini subgroup of G is central by Lemma 40 and A acts on G_2 through χ^2 by Lemma 104. ∎

Lemma 107. *The homomorphisms $\chi, \chi^2 : A \to \mathbb{Z}_p^*$ are distinct.*

Proof. Assume $\chi = \chi^2$. Then $\chi(\alpha) = \chi(\alpha)^2$ and $\chi(\alpha) = 1$. It follows that the intensity of G is equal to 1. Contradiction. ∎

Lemma 108. *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 106, the group A acts on G_2 through χ^2. By Corollary 103, the group A acts on $\mathrm{Z}(G)$ through a character and, as a consequence of Lemma 66, the action of A on the centre is through χ^2. On the other hand, by Lemma 104, 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 66 yields $\mathrm{Z}(G) = G_2$. By Lemma 106 the subgroup $\Phi(G)$ is central, and thus $G_2 = \Phi(G) = \mathrm{Z}(G)$. ∎

Lemma 109. *Assume G_2 has order p. Then G is an extraspecial group of exponent p.*

Proof. Thanks to Lemma 108 we are only left with showing that G has exponent p. Assume by contradiction there exists $g \in G$ of order p^2 and write $H = \langle g \rangle$. Then H^p has order p. Now, H^p is contained in $\Phi(G)$ and, as a consequence of Lemma 108, the Frattini subgroup of G has itself order p. It follows that $H^p = \Phi(G)$ and, in particular, H contains $\Phi(G)$. The group G_2 is equal to $\Phi(G)$, by Lemma 108, so the group H is normal. By Lemma 88(1), the subgroup H is A-stable. As a consequence of Lemma 104, the actions of A on H/G_2 and G_2 are respectively through χ and χ^2 and, by Lemma 107, the characters χ and χ^2 are distinct. From Theorem 68 it follows that the groups H and $(H/G_2) \oplus G_2$ are isomorphic. Contradiction. ∎

Lemma 110. *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 and we start by assuming $i = 1$. Let M be a normal subgroup of Q that is contained in Q_2 with index p; the group M exists by Lemma 35. Thanks to the isomorphism theorems, the groups Q/Q_2 and $(Q/M)/(Q_2/M)$ are isomorphic. 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 101. From Lemma 109, 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, as a consequence of Lemma 25, the exponent of Q_i/Q_{i+1} divides p. ■

Corollary 111. *Let Q be a finite p-group of nilpotency class* 2*. If* $\mathrm{int}(Q) > 1$*, then* $\mathrm{Z}(Q) = Q_2$*.*

Proof. By Lemma 110, the commutator subgroup of Q has exponent p. To conclude, apply Lemma 108. ■

4.2 More general setting

Throughout this whole section (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. It follows from the work done in Sections 3.2 and 3.3 that G is not trivial and p is odd. Let α be intense of order $\mathrm{int}(G)$ and write $A = \langle\alpha\rangle$ and $\chi = \chi_{G|A}$. We denote by V and Z respectively G/G_2 and G_2 and by π the canonical projection $G \to V$. From Lemma 110 it follows that both V and Z are vector spaces over $\mathbb{F}_p$. By Corollary 111, the non-trivial subgroup Z is equal to $\mathrm{Z}(G)$ and, as a consequence of Lemma 26, the map $\phi : V \times V \to Z$ that is induced by the commutator map is alternating.

Lemma 112. *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.*

Proof. The subgroup H is contained in the centre Z and is therefore a normal subgroup of G. It follows from Lemma 101 that $\mathrm{int}(G/H) > 1$. As a consequence of Lemma 109, the group G/H is extraspecial, and so, thanks to Lemma 26, the map $\phi_H : V \times V \to Z/H = [G/H, G/H]$ is non-degenerate. ■

Corollary 113. *There exists $n \in \mathbb{Z}_{>0}$ such that* $\dim V = 2n$*.*

Proof. Let H be a linear subspace of Z of codimension 1 and let ϕ_H be as in Lemma 112. Then ϕ_H is non-degenerate, and so, by Lemma 10, the dimension of V is even. The dimension is positive, because G has class 2. ■

Lemma 114. *Let G be a group, let N be a central subgroup, and let H be a complement of N in G. Let moreover $\mathcal{C}_N$ be the collection of complements of N in G 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.*

Proof. Straightforward. ■

We recall that, as defined in Section 1.1, an isotropic subspace of V is a linear subspace T of V such that $\phi(T \times T) = 0$.

Lemma 115. *Let T be a linear subspace of V. Then T is isotropic if and only if $\pi^{-1}(T)$ is abelian.*

Proof. The subspace T is isotropic if and only if $\phi(T \times T) = 0$, which happens if and only if $[\pi^{-1}(T), \pi^{-1}(T)] = 1$. ■

In the next lemma, we use the same notation as in Section 1.1. The map ϕ_T is given in Definition 6.

Lemma 116. *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. The subgroup $\pi^{-1}(T)$ is abelian, by Lemma 115, and it contains Z. It follows that $\pi^{-1}(T)$ is normal, and so, by Proposition 88(1), it is A-stable. By Lemma 104, the actions of A on $\pi^{-1}(T)/Z$ and on Z are respectively through χ and χ^2, which are distinct by Lemma 107. By Theorem 68 the subgroup Z has a unique A-stable complement H in $\pi^{-1}(T)$, which is isomorphic to T via π. We now show that ϕ_T is surjective. For this purpose, let $f \in \mathrm{Hom}(T, Z)$ 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 114, 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 93 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 we get $h = t$. We have proven that f is the map $t \mapsto [g, t]$. It follows from Definition 6 that ϕ_T is surjective. ■

Corollary 117. *Let T be an isotropic subspace of V. Then T is maximal isotropic if and only if the map $\phi_T : V/T \to \mathrm{Hom}(T, Z)$, defined by $v + T \mapsto (t \mapsto \phi(v, t))$, is a bijection.*

Proof. The map ϕ_T is surjective by Lemma 116 and it is injective by Lemma 7. ■

Lemma 118. *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. From Corollary 117, it follows 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 116. 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 dimension of $\ker \psi$ is positive and, as a consequence of Lemma 4, there are 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. ■

Corollary 119. *The group G is extraspecial of exponent p.*

Proof. The commutator subgroup of G is non-trivial. If G_2 has order p, then G is extraspecial of exponent p, by Lemma 109. We claim that the order of G_2 is in fact p. Assume by contradiction that G_2 has order larger than p. Then, by Lemma 35, there exists a normal subgroup M of G that is contained in G_2 with index p^2. The group G/M has class 2 and, by Lemma 101, its intensity is greater than 1. This is a contradiction to Lemma 118, with G_2/M in the role of Z. ■

We remark that Corollary 119 gives (1) ⇒ (2) in Theorem 105. 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 (see Section 1.4) is particularly suitable for explicit construction of intense automorphisms of order coprime to p. In this section, we conclude the proof of Theorem 105.

Lemma 120. *Let p be a prime number and let G be a non-abelian extraspecial group of exponent p. Let moreover H be a subgroup of G that trivially intersects G_2. Then $|G : \mathrm{N}_G(H)| = |\mathrm{Hom}(H, G_2)|$.*

Proof. The group G being non-abelian, Lemma 39 yields that $\mathrm{Z}(G) = G_2$ and G_2 has order p. Since $H \cap G_2$ is trivial, we have $\mathrm{N}_G(H) = \mathrm{C}_G(H)$ and H is abelian. By Lemma 22, the commutator map $G \times G \to G_2$ is bilinear, and moreover, 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 $G/\operatorname{C}_G(H)$ and H are $\mathbb{F}_p$-vector spaces and G_2 has order p. It follows from Lemma 2 that $|G : \operatorname{N}_G(H)| = |G : \operatorname{C}_G(H)| = |H| = |\operatorname{Hom}(H, G_2)|$. ■

Lemma 121. *Let p be a prime number and let G be a non-abelian 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. As G is non-abelian, Lemma 39 yields that $G_2 = \operatorname{Z}(G)$ and G_2 has order p. It follows that 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, also 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 114, the number of complements of G_2 in T equals the cardinality of $\operatorname{Hom}(H, G_2)$, which is equal to $|G : \operatorname{N}_G(H)|$ by Lemma 120. It follows that the number of complements of G_2 in T is equal to the number of conjugates of H in G. As all conjugates of H are themselves complements of G_2 in T, we get that every complement of G_2 in T is conjugate to H in G. In particular, H and $\alpha(H)$ are conjugate in G. The choice of H being arbitrary, it follows that $\alpha \in \operatorname{Int}(G)$. ■

Lemma 122. *Let p be a prime number and let G be a non-abelian 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. By Proposition 43, we can write G in the form $G(Z, Y, X, \theta)$, where X, Y, and Z are vector spaces over $\mathbb{F}_p$ and $\theta : X \times Y \to Z$ is bilinear. 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. For each $m \in \mathbb{F}_p^*$, the following diagram is commutative because θ is bilinear.

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

By Proposition 44, 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 $A = \{a_m \mid m \in \mathbb{F}_p^*\}$ is a subgroup of $\operatorname{Aut}(G)$ that is isomorphic to $\mathbb{F}_p^*$. Thanks to Lemma 121, the subgroup A is contained in $\operatorname{Int}(G)$ and therefore $\operatorname{int}(G) = p - 1$. ■

We remark that Lemma 122 is the same as (2) ⇒ (3) in Theorem 105. Since the implication (3) ⇒ (1) is clear and (1) ⇒ (2) is given by Corollary 119, Theorem 105 is finally proven.

Proposition 123. *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 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 101 and Theorem 105; we assume that $i > 1$. As a consequence of Lemma 20, the quotient G_i/G_{i+2} is abelian. By Lemma 104, 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 68 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 110. ■

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 124. *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 $\mathrm{wt}_G(j) = \log_p |G_j : G_{j+1}|$. For more detail, see Section 2.3.

Theorem 125. *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 126. *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 126, we will work under the following assumptions until the end of Section 5.1. Let p be 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 127. *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. The subgroup G_3 is contained in $\mathrm{Z}(G)$ because G has class 3. By Lemma 101 the intensity of G/G_3 is greater than 1, and thus, by Theorem 105, 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, the subgroup $\mathrm{Z}(G)$ is different from G_2, and so $\mathrm{Z}(G) = G_3$. ∎

Lemma 128. *Assume 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. (1) The group G_4 is trivial and, as a consequence of Lemma 20, the subgroup G_2 is abelian. The exponent of G_2 is equal to p, by Proposition 123. This proves (1). We now prove (2). To lighten the notation, let $C = \mathrm{C}_G(G_2)$. The subgroup G_2 is central in C, by definition of C, and, as a consequence of Lemma 26, 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 they are A-stable. Thanks to Lemma 104, the group A acts on C/G_2 through χ, and, by Lemma 61, it acts on $[C, C]$ through χ^2. By Lemma 104, 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 Lemma 66 yields $[C, C] \cap G_3 = \{1\}$. By Lemma 127(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 from Lemma 29 that $[C, C] = \{1\}$. ∎

Lemma 129. *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. The group G_3 having order p, it follows from Lemma 29 that G_3 is central, and so G has class 3. To lighten the notation, let $C = \mathrm{C}_G(G_2)$. Let moreover $V = G/G_2$, $Z = G_2/G_3$, and $T = C/G_2$. The groups V, Z, and T are vector spaces over $\mathbb{F}_p$, as a consequence of Lemma 110. We prove (1). By Lemma 24, the commutator map induces a bilinear map $\psi : V \times Z \to G_3$ whose left kernel is T. The centre of G is equal to G_3, by Lemma 127(3), so the right kernel of ψ is trivial. The map $\psi_C : V/T \times Z \to G_3$ that is induced from ψ is thus non-degenerate. The dimension of Z is equal to 1, by Lemma 127(2), and Lemma 2 yields $\dim V/T = 1$. This proves (1). We prove (2) and (3) together. Let $\phi : V \times V \to Z$ be the bilinear map from Lemma 24. The map ϕ is induced from the commutator map and, by Lemma 128(2), the group C is abelian. It follows that T is isotropic. As a consequence of (1) the space T has codimension 1 in V and T is maximal isotropic, because ϕ is not the zero map. From Corollary 117, it follows that $1 = \dim(V/T) = \dim \mathrm{Hom}(T, Z) = \dim T$ and so $\dim V = 2$. To conclude, we compute $|G : G_2| = p^{\dim V} = p^2$ and $|C| = |C : G_2||G_2 : G_3||G_3| = p^{\dim T} p^{\dim Z} p = p^3$. ■

Lemma 130. *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 128(2). We will show that C has exponent p. By Lemma 128(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 104, and, by Lemma 63, it acts on C^p also through χ. It follows from Lemma 127(1) that $C^p \subseteq G_3$. The action of A on G_3 is through χ^3, by Lemma 128(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 66, the group C has exponent p. ■

Lemma 131. *Assume that $\chi^2 \neq 1$ and that G_3 has order p. Then $\mathrm{C}_G(G_2)$ is a vector space over $\mathbb{F}_p$ and there exist unique A-stable subspaces C_1 and C_2 of $\mathrm{C}_G(G_2)$, of dimension 1, such that $\mathrm{C}_G(G_2) = C_1 \oplus C_2 \oplus G_3$.*

Proof. To lighten the notation, let $C = \mathrm{C}_G(G_2)$. Since G_3 has order p, it follows from Lemma 29 that G_3 is central so G has class 3. As a consequence of Lemmas 129(3) and 130, the group C is a vector space over $\mathbb{F}_p$ of dimension 3. The group C is A-stable, by Lemma 128(2), and, by Lemma 104, the action of A on C/G_2,

G_2/G_3, and G_3 is respectively through χ, χ^2, and χ^3. The three characters are pairwise distinct because $\chi^2 \neq 1$. We first apply Theorem 68 to C/G_3. Then there exists 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 68 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 127(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 132. *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 now C_1 and C_2 be as in Lemma 131 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 129(1), the index of C in G is equal to p and the size of each orbit of X under G is 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 94 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 126. The prime p is odd as a consequence of Proposition 95. Since G has class at least 3, the group G_3 is non-trivial, so, by Lemma 35, there exists a normal subgroup M of G that is contained in G_3 with index p. By Lemma 101, the group G/M has intensity greater than 1 and, as a consequence of Lemma 132, the intensity of G/M is equal to 2. From Lemma 101 it follows that $1 < \mathrm{int}(G) \leq \mathrm{int}(G/M) = 2$. Moreover, Lemma 129(2) yields

$$|G : G_2| = |G/M : [G/M, G/M]| = p^2.$$

We remark that Proposition 126 gives (1) ⇔ (2) and (1) ⇒ (3) in Theorem 124 and Theorem 125(1). We give the full proof of Theorem 124 in Section 5.4 and the full proof of Theorem 125 in Section 5.2.

Proposition 133. *Let p be a prime number and let G be a finite p-group. Then the following are equivalent.*

1. *One has* $\mathrm{int}(G) > 1$.
2. *The prime p is odd and* $\mathrm{int}(G)$ *is even.*

Proof. The implication (2) ⇒ (1) is clear. Assume now (1). Then G is non-trivial and p is odd, by Proposition 95. Moreover, if G has class at least 3, then

Proposition 126 yields $\operatorname{int}(G) = 2$. On the other hand, if G has class at most 2, then we know from Theorems 86 and 105 that $\operatorname{int}(G) = p - 1$, which is even because p is odd. ■

Proposition 134. *Let p be a prime number and let G be a finite p-group of class at least 3. Let α be an intense automorphism of G of order $\operatorname{int}(G)$ and assume that $\operatorname{int}(G) > 1$. Then 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 126, the intensity of G is 2 and p is odd. In particular, $\chi(\alpha)$ has order 2 in $\omega(\mathbb{F}_p^*)$, so $\chi(\alpha) = -1$. Lemma 104 draws the conclusion. ■

5.2 Groups of class 3

This section is devoted to understanding the structure of p-groups G of class 3 with the property that $|G : G_2| = p^2$. We will see in the next section that all these groups have intensity 2. We also give the proof of Theorem 125.

Lemma 135. *Let p be a prime number and let G be a finite p-group of class 3. Assume that $|G : G_2| = p^2$. Then the following hold.*

1. *One has $|G_2 : G_3| = p$.*
2. *One has $|G_3| \in \{p, p^2\}$.*
3. *The subgroup G_3 is elementary abelian.*

Proof. The group G is non-abelian and, as a consequence of Lemma 36, the group G/G_2 is a vector space over $\mathbb{F}_p$ of dimension 2. By Lemma 25, the commutator map induces a surjective homomorphism $G/G_2 \otimes G/G_2 \to G_2/G_3$ which factors as a surjective homomorphism $\bigwedge^2(G/G_2) \to G_2/G_3$ by the universal property of wedge products. The space $\bigwedge^2(G/G_2)$ has dimension 1 and so $|G_2 : G_3| = p$. Again applying Lemma 25, we derive that G_3 is isomorphic to a quotient of $G/G_2 \otimes G_2/G_3$. In particular, one has

$$1 < |G_3| \leq |G/G_2 \otimes G_2/G_3| = p^2$$

and G_3 is elementary abelian. ■

Thanks to Lemma 135, we can finally give the proof of Theorem 125. Indeed, if p is a prime number and G is a finite p-group of class at least 3 with $\operatorname{int}(G) > 1$, then Proposition 126 yields $\operatorname{int}(G) = 2$ and $w_1 = 2$. We now apply Lemma 135, with G/G_4 in place of G, to get $w_2 = 1$ and $w_3 \in \{1, 2\}$. The proof of Theorem 125 is now complete.

Lemma 136. *Let p be an prime number and let G be a finite p-group of class* 3. *Assume that $|G : G_2| = p^2$. Then the following hold.*

1. *One has $G_2 \subseteq \mathrm{C}_G(G_2)$.*

2. *The commutator map induces an isomorphism $G/\mathrm{C}_G(G_2) \otimes G_2/G_3 \to G_3$.*

3. *One has $|G : \mathrm{C}_G(G_2)| = |G_3|$.*

Proof. (1) As a consequence of Lemma 20, the group $[G_2, G_2]$ is contained in $G_4 = \{1\}$ and G_2 centralizes itself. This proves (1). We now prove (2) and (3) together. The subgroup G_3 is central, because the class of G is 3, so, by Lemma 22, the commutator map $\gamma : G \times G_2 \to G_3$ is bilinear. The right kernel of γ is equal to $G_2 \cap \mathrm{Z}(G)$, which is equal to G_3 as a consequence of Lemma 135(1). The left kernel of γ coincides with $\mathrm{C}_G(G_2)$ and, in particular, γ induces a non-degenerate map $\gamma_1 : G/\mathrm{C}_G(G_2) \times G_2/G_3 \to G_3$ whose image generates G_3. Thanks to (1) the quotient $G/\mathrm{C}_G(G_2)$ is abelian and, thanks to Lemma 36, it has exponent p. By the universal property of tensor products, γ_1 induces a surjective homomorphism $G/\mathrm{C}_G(G_2) \otimes G_2/G_3 \to G_3$, which is also an isomorphism since the index $|G_2 : G_3|$ is equal to p. Moreover, we have $|G : \mathrm{C}_G(G_2)| = |G_3|$. ■

Lemma 137. *Let p be a prime number and let G be a finite p-group of class* 3. *Assume that $|G : G_2| = p^2$. Then the following hold.*

1. *One has $|G_3| = p$ if and only if $|\mathrm{C}_G(G_2) : G_2| = p$.*

2. *One has $|G_3| = p^2$ if and only if $\mathrm{C}_G(G_2) = G_2$.*

Proof. By Lemma 136(3), we have $|G : \mathrm{C}_G(G_2)| = |G_3|$. By Lemma 136(1), the subgroup G_2 is contained in $\mathrm{C}_G(G_2)$, so (1) and (2) follow from the fact that $|G : G_2| = p^2$. ■

Lemma 138. *Let p be a prime number and let G be a finite p-group of class* 3. *Assume that $|G : G_2| = p^2$. Then $\mathrm{C}_G(G_2)$ is abelian.*

Proof. Write $C = \mathrm{C}_G(G_2)$. As a consequence of Lemma 137, the group C/G_2 is cyclic. It follows from Lemma 28 that $[C, C] = [C, G_2] = \{1\}$. ■

Lemma 139. *Let p be an odd prime number and let G be a finite p-group of class* 3. *Assume that $|G : G_2| = p^2$. Then G/G_3 is extraspecial of exponent p.*

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 $\mathrm{Z}(\overline{G})$. By Lemma 135(1), the order of $\overline{G_2}$ is equal to p and, as a consequence of Lemma 27, 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 $C \neq G$, because G_2

is not central, and D is a group, thanks to Corollary 48. Let now $x \in G \setminus C$. As a consequence of Lemma 36, the element x^p belongs to G_2. Moreover, by Lemma 136(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. It follows that $\overline{G} = \overline{D}$ and so $\overline{G}$ has exponent p. ∎

Lemma 140. *Let p be an odd prime number and let G be a finite p-group of class 3. Assume that $|G : G_2| = p^2$. Then $G_3 = \mathrm{Z}(G)$.*

Proof. The subgroup G_3 is contained in $\mathrm{Z}(G)$, since G has class 3 and, as a consequence of Lemma 139, the centre of G/G_3 is equal to G_2/G_3. It follows that $\mathrm{Z}(G)/G_3 \subseteq G_2/G_3$ and $\mathrm{Z}(G) \subseteq G_2$. Moreover, the group $\mathrm{Z}(G)$ does not contain G_2, because G has class 3. The group G_2/G_3 having order p, one gets $G_3 = \mathrm{Z}(G)$. ∎

Lemma 141. *Let p be an odd prime number and let G be a finite p-group of class 3. Assume that $|G : G_2| = p^2$. Then G_2 is elementary abelian.*

Proof. The group G_2 is abelian as a consequence of Lemma 136(1). 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, because G_3 is central. 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 from Lemma 138 that $\mathrm{C}_{\overline{G}}(\overline{G_2})$ is abelian and, from Lemma 137(1), that it contains $\overline{G_2}$ with index p. Write $\overline{C} = \mathrm{C}_{\overline{G}}(\overline{G_2})$. As a consequence of Lemma 139, 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 139, so G_2/G_3 is equal to $\mathrm{Z}(G/G_3)$. As a consequence of Lemma 135(1), the quotient G_2/G_3 has order p, so Lemma 29 yields $\overline{G_2} \subseteq \mu_p(\overline{C})$. 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, by Lemma 135(2-3), and G_2^p is contained in $N \cap M = \{1\}$, by the previous arguments. The exponent of G_2 is thus p. ∎

5.3 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. For more detail see Section 1.2. The main result of this section is the following.

Proposition 142. *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* $\operatorname{int}(G) = 2$.

The following assumptions will be valid until the end of Section 5.3. 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 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. We will prove that α is intense.

Lemma 143. *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 139, 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 121 and Lemma 93, there exists $g \in G$ such that $\alpha(gHg^{-1})/G_3 = (gHg^{-1})/G_3$ and, 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 $\operatorname{wt}_H^G(j) = \log_p |H \cap G_j : H \cap G_{j+1}|$. For more information about jumps and width see Section 2.3.

Lemma 144. *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 $\operatorname{wt}_H^G(1) = 1$.*

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

Proof. (1) Assume that 1 is a jump of H in G. By Lemma 36, the Frattini subgroup of G is equal to G_2. The subgroup H does not contain G_3 and thus $H \neq G$. By Lemma 33, we have $H\Phi(G) \neq G$ so $H\Phi(G)/\Phi(G) = HG_2/G_2$ has order p. Since HG_2/G_2 is isomorphic to $(H \cap G_1)/(H \cap G_2)$, this proves (1). We now prove (2). Assume that 2 is a jump of H in G. Then by Lemma 82 there exists an element $x \in (H \cap G_2) \setminus G_3$. Fix x. As a consequence of Lemma 135(1), the group G_2 is equal to $\langle x, G_3 \rangle$. The group 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. In particular, H centralizes G_2. ■

Lemma 145. *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 140, the groups G_3 and $\mathrm{Z}(G)$ are equal, so the group $T = H \oplus G_3$ is abelian. By Lemma 143, 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 63 that the induced action of A on gTg^{-1}/G_3 is through χ. Moreover, by Lemma 62, the group A acts on G_3 through $\chi^3 = \chi$. From Lemma 77, 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 146. *Let H be a subgroup of G such that $G_2 = H \oplus G_3$. Then H has an A-stable conjugate in G.*

Proof. By Lemma 135(1), the index $|G_2 : G_3|$ is equal to p, so H has order p. By Lemma 62, the induced action of A on G_2/G_3 and G_3 is respectively through χ^2 and $\chi^3 = \chi$. By assumption, the characters χ and χ^2 are distinct. Moreover, by Lemma 136(1), the group G_2 is abelian and so, by Theorem 68, 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 140, thus $\mathrm{C}_G(H) = \mathrm{C}_G(G_2)$. Moreover, we have that $H \cap [H,G] \subseteq H \cap G_3 = \{1\}$, so $\mathrm{C}_G(H) = \mathrm{N}_G(H)$. Let X be the collection of complements of G_3 in G_2. Then K and all conjugates of H in G are in X. By Lemma 136(3), we have $|G : \mathrm{C}_G(G_2)| = |G_3|$. By Lemma 135(3), the subgroup G_3 is elementary abelian and, by Lemma 114, the cardinality of X is equal to the cardinality of $\mathrm{Hom}(H, G_3)$, which coincides with $|G_3|$ because H has order p. It follows that $|X| = |G : \mathrm{C}_G(G_2)| = |G : \mathrm{N}_G(H)|$ and, every conjugate of H being in X, every complement of G_3 in G_2 is conjugate to H. In particular, K and H are conjugate in G. ■

Lemma 147. *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 144(2), the subgroup H has trivial intersection with G_2. We now apply Lemma 145. ■

Lemma 148. *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. Let us call $T = H \oplus G_3$. If $T = G_2$, then H has an A-stable conjugate by Lemma 146. 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 conclude applying Lemma 145. ■

We denote $G^+ = \{x \in G : \alpha(x) = x\}$ and $G^- = \{x \in G : \alpha(x) = x^{-1}\}$, in concordance with the notation from Section 2.2. In the context of Section 5.3, we will use this notation in Lemmas 149 and 150.

Lemma 149. *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. (1) The subgroup $\mathrm{C}_G(G_2)$ is abelian, by Lemma 138, and therefore H is abelian. Moreover, as a consequence of Lemma 139, the subgroup H^p is contained in $H \cap G_3 = \{1\}$, so H is elementary abelian. This proves (1). We now prove (2). The subgroup G^+ is contained in G_2, thanks to Lemma 85, and G_2 centralizes C, by definition of C. It follows that $G^+ \,\mathrm{N}_G(H) \subseteq G_2 \,\mathrm{N}_G(H) = \mathrm{N}_G(H)$. Since $\mathrm{N}_G(H)$ is contained in $G^+ \,\mathrm{N}_G(H)$, the proof is complete. ■

Lemma 150. *Let H be a subgroup of G such that $\mathrm{C}_G(G_2) = H \oplus G_3$. Then H has a conjugate that is A-stable.*

Proof. To lighten the notation, write $C = \mathrm{C}_G(G_2)$. If $C = G_2$, then we are done by Lemma 146. Assume now that $C \neq G_2$. As a consequence of Lemma 137(1), the group 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 140, and, as a consequence of Lemma 29, 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 149(1), the subgroup H is elementary abelian, and, G_3 being central of order p, it follows that C is naturally an $\mathbb{F}_p$-vector space. Combining Lemmas 135(1) and 137(1), we get that $\dim C = 3$. Write $C^+ = \{x \in C : \alpha(x) = x\}$ and $C^- = \{x \in C : \alpha(x) = x^{-1}\}$. Then $C = C^+ \oplus C^-$, thanks to Corollary 76 and, as a consequence of Lemma 85, one has $|C^-| = p^2$ and $|C^+| = p$. Moreover, C being abelian, both C^+ and C^- are linear subspaces of C. It is not difficult to show at this point 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 81 and 149(2), ensures that no two elements of X^+ are conjugate in G. It follows from Lemma 94 that

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

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

Lemma 151. *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 148. Assume now that H is contained in $\mathrm{C}_G(G_2)$ and that H has order p^2. The group $\mathrm{C}_G(G_2)$ is abelian, by Lemma 138, and thus, as a consequence of Lemmas 135(1) and 137, one has $\mathrm{C}_G(G_2) = H \oplus G_3$. The group H has an A-stable conjugate by Lemma 150. We conclude by Lemma 147, in case H is not contained in $\mathrm{C}_G(G_2)$. ■

Lemma 152. *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 143 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. As a consequence of Lemma 135(2), the cardinality of G_3 is p^2, so $H \cap G_3$ has order p. 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 151, the subgroup $\overline{H}$ has an A-stable conjugate, and therefore so does H. ■

Lemma 153. *The automorphism α is intense and* $\mathrm{int}(G) = 2$.

Proof. We will show that $\alpha \in \mathrm{Int}(G)$. Thanks to Lemma 93, 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 151, otherwise apply Lemma 152. ■

Thanks to Lemma 153, Proposition 142 is proven.

5.4 Constructing intense automorphisms

The aim of Section 5.4 is giving the proof of Theorem 124. We will prove the following essential result.

Proposition 154. *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 154, 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 5.4. 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

$$L = F_3F^p \text{ and } E = [F, L]F_2^p.$$

The notation we just introduced will be valid until the end of Section 5.4. We will introduce some extra notation between Lemma 158 and Lemma 159. We refer to the diagram given at the end of the present section for a visualization of the proof of Proposition 154.

Lemma 155. *One has $\theta^{-1}(G_2) = F_2$.*

Proof. Since θ is a surjective homomorphism, one has $\theta(F_2) = \theta([F, F]F^p) = G_2G^p = \Phi(G)$ and so, as a consequence of Lemma 36, we get $\theta(F_2) = G_2$. In other words, $F_2 \subseteq \theta^{-1}(G_2)$. The group F being 2-generated, we have that $|F : F_2| = p^2$, and so $F_2 = \theta^{-1}(G_2)$. ■

Lemma 156. *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, the index $|F_2 : L|$ is at most p.*

Proof. We write $\overline{F} = F/L$ and we will use the bar notation for the subgroups of $\overline{F}$. The subgroup $[F, [F, F]]$ is contained in F_3 and $[\overline{F}, \overline{F}]$ is central. Moreover, $\overline{F}$ being annihilated by p, the subgroup $\overline{F_2}$ coincides with $[\overline{F}, \overline{F}]$. As a consequence of Lemma 22, the commutator map induces a bilinear map $\phi : \overline{F}/\overline{F_2} \times \overline{F}/\overline{F_2} \to \overline{F_2}$ whose image generates $\overline{F_2} = [\overline{F}, \overline{F}]$. The map ϕ is alternating because every element of a group commutes with itself. By the universal property of the exterior square, ϕ factors as a surjective homomorphism $\bigwedge^2(\overline{F}/\overline{F_2}) \to \overline{F_2}$. As a consequence of Lemma 36, the quotient $\overline{F}/\overline{F_2}$ is a 2-dimensional vector space over $\mathbb{F}_p$ and $\bigwedge^2(\overline{F}/\overline{F_2})$ has dimension 1. It follows that $\overline{F_2}$ has order at most p. ■

Lemma 157. *One has $\theta^{-1}(G_3) = L$ and $|F_2 : L| = p$.*

Proof. As a consequence of Lemma 139, the group G_3 contains G^p, from which it follows that $\theta(L) = G_3$. In particular, the subgroup L is contained in $\theta^{-1}(G_3)$. As a consequence of Lemma 155, the subgroup $\theta^{-1}(G_3)$ is contained in F_2 and $\theta^{-1}(G_3) \neq F_2$, because $G_3 \neq G_2$. In particular, F_2 is different from L. By Lemma 156, the index $|F_2 : L|$ is at most p, and so we get that $|F_2 : L| = p$ and $\theta^{-1}(G_3) = L$. ■

Lemma 158. *One has $E \subseteq \ker\theta \cap F_3$.*

Proof. The group E is contained in $[F, F_2]F_2^p = F_3$, by definition of the p-central series of F. As a consequence of Lemma 139, the image of L under θ is equal to G_3 and, as a consequence of Lemma 141, the subgroup F_2^p is contained in the kernel of θ. It follows that $\theta(E) = \theta([F, L]F_2^p) = [G, G_3] = G_4 = \{1\}$. ■

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 5.4.

Lemma 159. *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, every element of F is inverted by β modulo F_2; in other words, the action of B on F/F_2 is through σ. By Lemma 156, 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, by Lemma 61, the action of B on F_2/L is through σ^2. ■

Lemma 160. *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, since $[F, [F, F]]$ is contained in F_3, the group $\overline{F}$ has class at most 2. Moreover, we have that $[F, F]^p \subseteq F_2^p \subseteq F_3$, so $[\overline{F}, \overline{F}]$ is annihilated by p. It follows from Lemma 48 that 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 63, the induced action of B on $\overline{L}$ is through σ. ■

Lemma 161. *The induced action of B on F_3/E is through σ.*

Proof. The group F_2/L is cyclic, thanks to Lemma 157, so Lemma 28 yields $[F_2, F_2] = [F_2, L]$. It follows that $[F_2, F_2]$ is contained in E. The group $[F, F_3]$ is also contained in E and, as a consequence of Lemma 22, the commutator map induces a bilinear map $\phi : F/F_2 \times F_2/L \to F_3/E$. By definition of F_3, the image of ϕ generates F_3/E. By Lemma 159, the induced actions of B on F/F_2 and F_2/L are respectively through σ and σ^2 and, by Lemma 61, the action of B on F_3/E is through $\sigma^3 = \sigma$. ■

Lemma 162. *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 160 and 161, the induced actions of B on L/F_3 and F_3/E are both through σ. It follows from Lemma 77 that the action of B on L/E is through σ. As a consequence of Lemmas 157 and 158, 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. ■

Lemma 163. *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 162, 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 142 yields that α is intense. ■

We remark that Proposition 154 follows directly from Lemma 163. Moreover, we are also finally ready to give the proof of Theorem 124. Proposition 126 gives (1) ⇔ (2) and (1) ⇒ (3). On the other hand, the implication (3) ⇒ (2) is given by the combination of Lemma 163 and Proposition 142. The proof of Theorem 124 is finally complete.

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

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 the class of G is the number of indices i for which $G_i \neq 1$. Recall moreover that, 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 164. *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 165. *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 166. *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 $H^- = H \cap G^-$.

Lemma 167. *Let H be an A-stable subgroup of G. If H is cyclic, then $H \subseteq G^+$ or $H \subseteq G^-$.*

Proof. Assume that H is cyclic. As a consequence of Corollary 76, the subgroup H decomposes as $H = H^+ \oplus H^-$. Then H is cyclic if and only if one of H^+ and H^- is trivial. This concludes the proof. ■

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 168. *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 93 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 $H = \langle gxg^{-1} \rangle$. By Lemma 167, the subgroup H is contained either in G^+ or in G^-. By Lemma 104, 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. If d is even, then $\chi^d = 1$ and H is contained in G^+. Otherwise, H is contained in G^-. ■

We recall that, if H is a subgroup of G, then a jump of H in G is a positive integer j such that $H \cap G_j \neq H \cap G_{j+1}$.

Lemma 169. *All jumps of a cyclic subgroup of G have the same parity.*

Proof. Let H be a cyclic subgroup of G. The automorphism α being intense, it follows from Lemma 93 that there exists $g \in G$ such that gHg^{-1} is A-stable. By Lemma 167, the subgroup gHg^{-1} is contained in G^+ or in G^-. We conclude by applying Lemma 168. ■

Lemma 170. *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 104, the group A acts on G_c through χ^c. From the combination of Corollary 103 with Lemma 66, 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 $\mathrm{Z}(G)$ is a subset of G^-. ■

Lemma 171. *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 101, 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 104, 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 170(1). Lemma 66 yields $\mathrm{Z}(H) = H_i$. ■

We remark that, to prove Proposition 166, it now suffices to combine Lemma 171 with Lemma 30.

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 125(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 172. *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 173. *Assume that p is odd. Then $\mathrm{Z}(G) = G_4$.*

Proof. The class of G being 4, the subgroup G_4 is contained in $\mathrm{Z}(G)$. Now, the group $\mathrm{Z}(G)/G_4$ is contained in $\mathrm{Z}(G/G_4)$ and, as a consequence of Lemma 140, the centre of G/G_4 is equal to G_3/G_4. It follows that $G_4 \subseteq \mathrm{Z}(G) \subseteq G_3$. The groups $\mathrm{Z}(G)$ and G_3 are distinct, because the class of G is 4, so, the index $|G_3 : G_4|$ being p, we get that $G_4 = \mathrm{Z}(G)$. ■

Lemma 174. *The subgroup G_2 is abelian.*

Proof. The group G_2/G_3 is cyclic, because $w_2 = 1$, so $[G_2, G_2] = [G_2, G_3]$, by Lemma 28. It follows from Lemma 20 that $[G_2, G_2] \subseteq G_5 = \{1\}$, and thus G_2 is abelian. ■

Lemma 175. *Assume that p is odd. Then the following hold.*

1. *The subgroup $[\mathrm{C}_G(G_3), G_2]$ is contained in G_4.*

2. *One has $|\,\mathrm{C}_G(G_3) : G_2| = p$.*

Proof. To lighten the notation, write $C = \mathrm{C}_G(G_3)$. We first prove (1). The group $[G_2, [G, C]]$ is contained in $[G_2, G_2]$ so it follows from Lemma 174 that $[G_2, [G, C]] = \{1\}$. Moreover, $[C, [G_2, G]] = [C, G_3] = \{1\}$, by definition of C. Thanks to Lemma 19, the subgroup $[G, [C, G_2]]$ is trivial, and thus $[C, G_2]$ is contained in $\mathrm{Z}(G)$. The centre of G is equal to G_4, by Lemma 173, and (1) is proven. We prove (2). Let D be the unique subgroup of G containing G_4 such that $D/G_4 = \mathrm{C}_{G/G_4}(G_2/G_4)$. Then one has $[[G, D], G_2] \subseteq [G_2, G_2] = \{1\}$ and $[[D, G_2], G] \subseteq [G_4, G] = \{1\}$. Lemma 19 yields that $[D, G_3] = [D, [G, G_2]] = \{1\}$ and therefore D is contained in C. It follows from Lemma 137(1) that

$$p \leq |C : G_2| \leq |G : G_2| = p^2.$$

The group G_3 is not central, and so $|C : G_2| = p$. ■

Lemma 176. *If $\mathrm{int}(G) > 1$, then $\mathrm{C}_G(G_3)$ is abelian.*

Proof. Assume that $\mathrm{int}(G) > 1$. As a consequence of Proposition 95, the prime p is odd. Let α be an intense automorphism of G of order 2 and write $A = \langle \alpha \rangle$ and $\chi = \chi_{G|A}$. To lighten the notation, write $C = \mathrm{C}_G(G_3)$. By Lemma 175(2), the index of G_2 in C is p, so it follows from Lemma 28 that $[C, C] = [C, G_2]$. Moreover, $[C, G_2]$ is contained in G_4, by Lemma 175(1), and $G_4 = \mathrm{Z}(G)$ by Lemma 173. By Lemma 22, the commutator map $C \times G_2 \to G_4$ is bilinear and, as a consequence of Lemma 174, it factors as $\phi : C/G_2 \times G_2/G_3 \to G_4$. By Lemma 104, 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 61, the group A acts on $[C, G_2]$ through $\chi^3 = \chi$. By Lemma 104, the group A acts on G_4 through $\chi^4 = 1$. Since $\chi \neq 1$, it follows from Lemma 66 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 177. *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 176. From Corollary 76, it follows that $C = C^+ \oplus C^-$. The cardinalities of C^+ and C^- are both equal to p^2, as a consequence of Lemma 85. ■

Lemma 178. *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 is A-stable and $C = C^+ \oplus C^-$, by Lemma 177. Moreover, both C^+ and C^- have cardinality p^2. The subgroup C^p is characteristic in G, so C^p is A-stable. The group G has class 4 and, as a consequence of Lemma 170(2), the subgroup $\mathrm{Z}(G)$ is contained in G^+. We first prove the implication from right to left. Assume that C^- is cyclic. Then C^p is a non-trivial subgroup of the p-group G. From Lemma 29, it follows that C^p has non-trivial intersection with the centre of G and, in particular, $C^p \cap G^+ \neq \{1\}$. The group C^+ is cyclic, because it has order p^2 and exponent different from p. To prove the implication from left to right, assume that C^+ is cyclic. As a consequence of Lemma 85, 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 it means that C is equal to the union of two of its proper subgroups, namely $C \cap G_2$ with $\mu_p(C)$, which is impossible. It follows that there exists $x \in C$ of order p^2, with $\mathrm{dpt}_G(x) = 1$. Fix such x. By Lemma 168, 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 179. *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 176, and therefore $\mathrm{C}_G(G_3)$ normalizes H. It follows that $|G : \mathrm{N}_G(H)|$ is at most $|G : \mathrm{C}_G(G_3)|$. By Lemma 175(2) the index $|G : \mathrm{C}_G(G_3)|$ is equal to p, and thus H has at most p conjugates in G. ■

Lemma 180. *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 178, both C^+ and C^- are elementary abelian. From Lemma 177 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

$$|X| = \frac{p^4-1}{p-1} = p^3+p^2+p+1.$$

Let moreover $X^+ = \{H \in X : \alpha(H) = H\}$. As a consequence of Lemma 167, the set X^+ consists of the 1-dimensional subspaces of C that are contained in $C^+ \cup C^-$. Then $|X^+| = 2(p+1)$. By Lemma 179, each element of X^+ has at most p conjugates in G, so it follows from Lemma 94 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 181. *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 176, and $C = C^+ \oplus C^-$, by Lemma 177. Moreover, C^+ and C^- have both cardinality p^2. By Lemma 180, the subgroup C^+ is cyclic so, by Lemma 178, 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. It follows from Lemma 167 that $X^+ = \{C^+, C^-\}$ and the cardinality of X^+ is thus 2. On the other hand, the cardinality of X is equal to

$$|X| = \frac{p^4-p^2}{p^2-p} = p(p+1).$$

By Lemma 179, each element of X^+ has at most p conjugates, so it follows from Lemma 94 that

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

Contradiction. ■

We conclude Section 6.2 by giving the proof of Proposition 172. Let Q be a finite p-group of class at least 4 with $\mathrm{int}(Q) > 1$. The class of Q being 4, the subgroup Q_4 is non-trivial and, by Lemma 35, there exists a normal subgroup M of Q that is contained in Q_4 with index p. Fix M and denote $\overline{Q} = Q/M$. Thanks to Lemma 101, the intensity of $\overline{Q}$ is greater than 1, so it follows from Theorem 125(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 181 yields $f = 2$ and the proof of Proposition 172 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 182. *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 Proposition 182. Until the end of Section 6.3 we work thus under the assumptions of Proposition 182. As a consequence of Proposition 95, the prime p is odd.

Lemma 183. *One has $\mathrm{wt}_G(1)\,\mathrm{wt}_G(2) = 2$.*

Proof. This follows directly from Theorem 125(2). ■

Lemma 184. *Let $\phi : G/G_2 \to \mathrm{Hom}(G_{c-1}/G_c, G_c)$ be the function defined by $xG_2 \mapsto (aG_c \mapsto [x, a])$. Then ϕ is a homomorphism.*

Proof. The map ϕ is induced from the surjective homomorphism from Lemma 25 and ϕ is thus itself a homomorphism of groups. ■

Lemma 185. *The group G_{c-1} is abelian.*

Proof. By Lemma 20, the group $[G_{c-1}, G_{c-1}]$ is contained in G_{2c-2}, which is itself contained in G_{c+1} because $c \geq 3$. Since $G_{c+1} = \{1\}$, the group G_{c-1} is abelian. ■

Lemma 186. *Let α be an intense automorphism of G of order $\mathrm{int}(G)$ and write $A = \langle \alpha \rangle$. Then G_c has a unique A-stable complement in G_{c-1}.*

Proof. Denote by χ the restriction of the intense character of G to A (see Section 3.2). The group G_{c-1} is abelian, by Lemma 185, and, by Lemma 104, the group A acts on G_{c-1}/G_c and G_c respectively through χ^{c-1} and χ^c. The characters χ^{c-1} and χ^c are distinct, because $\chi \neq 1$, so, by Theorem 68, the subgroup G_c has a unique A-stable complement in G_{c-1}. ■

Lemma 187. *The homomorphism ϕ from Lemma 184 is surjective.*

Proof. Let α be an intense automorphism of G of order $\mathrm{int}(G)$ and write $A = \langle \alpha \rangle$. By Lemma 185, the group G_{c-1} is abelian and, by Lemma 186, there exists a unique A-stable complement M of G_c in G_{c-1}. Now 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 93 that all complements of G_c in G_{c-1} are conjugate to M in G. On the other hand, by Lemma 114, 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 $x \in G$. In other words, we have proven surjectivity of ϕ. ■

Lemma 188. *One has* $\mathrm{wt}_G(c-1)\,\mathrm{wt}_G(c) \leq 2$.

Proof. The groups G_{c-1}/G_c and G_c are $\mathbb{F}_p$-vector spaces, as a consequence of Lemma 110. It follows that the dimension of $\mathrm{Hom}(G_{c-1}/G_c, G_c)$ is equal to $\mathrm{wt}_G(c-1)\,\mathrm{wt}_G(c)$. Thanks to Lemma 187, the product $\mathrm{wt}_G(c-1)\,\mathrm{wt}_G(c)$ is at most $\mathrm{wt}_G(1)$, which is equal to 2, by Theorem 125(2). We get thus that $\mathrm{wt}_G(c-1)\,\mathrm{wt}_G(c) \leq 2$. ■

The proof of Proposition 182 is now an easy exercise, which we spell out here. If $i = 1$, then we are done by Lemma 183. Assume that $i > 1$. For all indices $j \leq i$, the quotient G/G_{j+1} has class j so, without loss of generality, we assume that $c = i + 1$. We conclude by applying Lemma 188.

We remark that Theorem 165 is the same as Proposition 182. Moreover, Theorem 164 is given by the combination of Propositions 172 and 182.

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. $G^n = \langle x^n : x \in G \rangle$ (see List of Symbols). One of the most important results we achieve in Chapter 7 is the following.

Theorem 189. *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 189 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 Groups of class 4

In Section 7.1 we start the preparation for the proof of Theorem 189, which will be given in Section 7.3. This very section will thus just consist of structural lemmas, which will be later of use.

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).

Lemma 190. *Assume that $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$ and $\mathrm{Z}(G) = G_4$. Then the commutator map induces a non-degenerate map $G/G_2 \times G_3/G_4 \to G_4$.*

Proof. The commutator map induces a bilinear map $\gamma : G/G_2 \times G_3/G_4 \to G_4$ whose image generates G_4, by Lemma 24. The subgroup G_4 has dimension 1 as an $\mathbb{F}_p$-vector space, while $w_1 = w_3 = 2$. The quotient G/G_2 has exponent p, thanks to Lemma 36, and the exponent of G_3/G_4 is equal to p, as a consequence of Lemma 25 (the property of being elementary abelian is preserved by surjective homomorphisms and tensor products). Moreover, the centre of G being G_4, the right kernel of γ is trivial. It follows from Lemma 2 that the left kernel of γ has also dimension 0, so γ is non-degenerate. ■

Lemma 191. *Assume that* $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. *Let* C *be a maximal subgroup of* G. *Then* C *contains* G_2 *and* $|G : C| = |C : G_2| = p$.

Proof. The subgroup C being maximal, it has index p in G and it contains the Frattini subgroup of G. Since G_2 is contained in $\Phi(G)$ and $|G : C| = p$, we get $|C : G_2| = p$. ■

Lemma 192. *Assume that* $\operatorname{int}(G) > 1$. *Then* $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$ *and* G *has order* p^6. *Moreover, one has* $\mathrm{Z}(G) = G_4$.

Proof. The quadruple (w_1, w_2, w_3, w_4) is equal to $(2, 1, 2, 1)$ by Theorem 164 and the order of G is equal to p^6, as a consequence of Lemma 84. The centre of G is equal to G_4 thanks to Lemma 171. ■

Lemma 193. *Let* C *be a maximal subgroup of* G *and assume that* $\operatorname{int}(G) > 1$. *Then* $G_4 \subseteq \mathrm{Z}(C) \subseteq G_3$ *and* $|G_3 : \mathrm{Z}(C)| = |\,\mathrm{Z}(C) : G_4| = p$.

Proof. We assume that $\operatorname{int}(G) > 1$. By Lemma 192, the subgroups G_4 and $\mathrm{Z}(G)$ are the same and $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. Moreover, by Lemma 190, the commutator map induces a non-degenerate map $G/G_2 \times G_3/G_4 \to G_4$. It follows from Lemma 2 that $G_3 \cap \mathrm{Z}(C)$ has index p in G_3. Now the subgroup $\mathrm{Z}(C)$ is normal in G, because it is characteristic in the normal subgroup C, and therefore Proposition 166 yields $\mathrm{Z}(C) \subseteq G_3$. We get that $|G_3 : \mathrm{Z}(C)| = |\,\mathrm{Z}(C) : G_4| = p$. ■

Lemma 194. *Let* M *be a normal subgroup of* G *that contains* G_4 *with index* p. *If* $\operatorname{int}(G) > 1$, *then* $\mathrm{C}_G(M)$ *is a maximal subgroup of* G.

Proof. We assume that $\operatorname{int}(G) > 1$. Then, by Lemma 192, we have that $\mathrm{Z}(G) = G_4$ and $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. Let now M be a normal subgroup of G that contains G_4 with index p. As a consequence of Proposition 166, the subgroup M is contained in G_3. The commutator map from Lemma 190 being non-degenerate, it follows from Lemma 2 that $\mathrm{C}_G(M)$ is maximal in G. ■

Lemma 195. *Assume that* $\operatorname{int}(G) > 1$. *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* $N \mapsto \mathrm{Z}(N)$. *Then* f *is a bijection with inverse* $f^{-1} : M \mapsto \mathrm{C}_G(M)$.

Proof. The map f is well-defined, as a consequence of Lemma 193. Also the map $g : \mathcal{N} \to \mathcal{M}$, sending M to $\mathrm{C}_G(M)$, is well-defined thanks to Lemma 194. It is now easy to show that f and g are inverses to each other. ■

7.2 Class 4 and p-th powers

The goal of this section is to prove some technical lemmas regarding the p-th powering on finite p-groups of intensity greater than 1. We will use such lemmas in Section 7.3, where Theorem 189 is proven.

Through the whole of Section 7.2, the following assumptions will be valid. 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. Let $\rho : G \to G$ be defined by $x \mapsto x^p$; this is the first time we introduce this notation, which can be also found in the List of Symbols. For each $i \in \{1, 2, 3, 4\}$, we will write $w_i = \mathrm{wt}_G(i)$ for the i-th width of G (see Section 2.3). Assume that $\mathrm{int}(G) > 1$. It follows from Proposition 95 that G is non-trivial and p is odd.

Lemma 196. *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 123. In particular, $\rho(G_2)$ is contained in G_4. By Lemma 192, the subgroup $\mathrm{Z}(G)$ is equal to G_4 and $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. 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, thanks to Lemma 28, the subgroups C_2 and $[C, G_2]$ are equal. It follows that $C_3 = [C, C_2]$ 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 Lemma 48, 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 the element $\rho(y)$ belongs to G_4 and the choices of x and y were arbitrary, the map $\overline{\rho}$ is well-defined. ■

Lemma 197. *Let C be a maximal subgroup of G and assume that $\rho(C \setminus G_2) \cap G_4$ is not empty. Then $\rho(C) \subseteq G_4$.*

Proof. By Lemma 196, the map ρ induces a function $\overline{\rho} : G/G_2 \to G_3/G_4$, which then becomes a homomorphism whenever we restrict it to a cyclic subgroup of G/G_2. Since $\rho^{-1}(G_4) \cap (C \setminus G_2)$ is non-empty, it generates C modulo G_2, and thus $\overline{\rho}(C/G_2) \subseteq G_4$. It follows that $\rho(C) \subseteq G_4$. ■

Lemma 198. *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 α be an intense automorphism of G of order 2 and set $A = \langle\alpha\rangle$. 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 93). As a consequence of Proposition 134, the automorphism α induces scalar multiplication by -1 on $H/(H \cap G_2)$, so, thanks to Lemma 63, 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 134 that α coincides with the identity map on H^p. Lemma 66 yields $H^p = \{1\}$, and, the choiche of H being arbitrary, we get $\rho(C \setminus G_2) = \{1\}$. ■

7.3 Class 4 and intensity

The unique purpose of Section 7.3 is to give the proof of the following proposition.

Proposition 199. *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 $G^p = G_3$.*

Until the end of Section 7.3, the following assumptions will hold. Let p be a prime number and let G be a finite p-group of class 4. Let $\rho : G \to G$ be defined by $x \mapsto x^p$ (see also the List of Symbols). Assume that $\mathrm{int}(G) > 1$. It follows that p is odd and the group G is non-trivial (see Section 3.2). Let α denote an intense automorphism of G of order 2 and write $A = \langle \alpha \rangle$. Set $G^+ = \{g \in G \ : \ \alpha(g) = g\}$ and $G^- = \{g \in G \ : \ \alpha(g) = g^{-1}\}$. For each maximal subgroup C of G, define moreover 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 200. *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 group $\mathrm{Z}(C)$ is normal in G, because $\mathrm{Z}(C)$ is characteristic in the normal subgroup C, and, by Lemma 193, the group G_3 contains $\mathrm{Z}(C)$. From Proposition 123, it follows that $\mathrm{Z}(C)$ has exponent p, and thus $y^p = 1$. The element x^p is 1, by Lemma 198, and so $H^p = \{1\}$. To conclude, assume that $x^a y^b \in H \cap G_4$. Then $x^a = (x^a y^b) y^{-b}$ belongs to $H \cap G_3$, so $a \equiv 0 \bmod p$. From the fact that $\langle y \rangle \cap G_4 = \{1\}$, we conclude that $H \cap G_4 = \{1\}$. ■

Lemma 201. *Let C be a maximal subgroup of G and assume that $\rho(C \setminus G_2) \cap G_4$ is not empty. If $H \in Y_C^+$, then $H \subseteq G^-$.*

Proof. Let $H = \langle x \rangle \oplus \langle y \rangle$ be an element of Y_C^+, where $x \in C \setminus G_2$ and $y \in \mathrm{Z}(C) \setminus G_4$. By Lemma 200, the group H has exponent p and so the order of H is p^2. The element x has depth 1 and the depth of y is 3, as a consequence of Lemma 193. It follows from Lemma 85 that

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

All inequalities are in fact equalities and $H \cap G^- = H$. ∎

Lemma 202. *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. Write $C^- = C \cap G^-$ and $\mathrm{Z}(C)^- = \mathrm{Z}(C) \cap G^-$. Thanks to Lemma 201 we are reduced to count the subgroups of the form $\langle x \rangle \oplus \langle y \rangle$, with $x \in C^- \setminus G_2$ and $y \in \mathrm{Z}(C)^- \setminus G_4$. By Lemma 193, the subgroup $\mathrm{Z}(C)$ contains G_4. By Lemma 192, the quadruple $(\mathrm{wt}_G(1), \mathrm{wt}_G(2), \mathrm{wt}_G(3), \mathrm{wt}_G(4))$ is equal to $(2,1,2,1)$ so, as a consequence of Lemma 85, the cardinalities of $C^- \setminus G_2$ and $\mathrm{Z}(C)^- \setminus G_4$ are respectively $p^3 - p^2$ and $p - 1$. Fix now a basis (x, y) for a subgroup H, where $x \in C^- \setminus G_2$ and $y \in \mathrm{Z}(C)^- \setminus G_4$. Thanks to Lemma 200, the set 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 thus $|B| = p(p-1)^2$. The cardinality of Y_C^+ is

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

∎

Lemma 203. *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. We want to count the subgroups of the form $\langle x \rangle \oplus \langle y \rangle$, with $x \in C \setminus G_2$ and $y \in \mathrm{Z}(C) \setminus G_4$. The quadruples $(\mathrm{wt}_G(1), \mathrm{wt}_G(2), \mathrm{wt}_G(3), \mathrm{wt}_G(4))$ and $(2,1,2,1)$ are the same, by Lemma 192, and so $|C| - |G_2| = p^5 - p^4$. Moreover, thanks to Lemma 193, the set $\mathrm{Z}(C) \setminus G_4$ has cardinality $p^2 - p$. Fix now (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 200, the set 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 $p(p-1)^2$. It follows 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 204. *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 one has $\mathrm{N}_G(H) = HG_4$ and $|G : \mathrm{N}_G(H)| \leq p^3$.*

Proof. Let H be an arbitrary element of Y_C^+. By Lemma 192, the subgroup G_4 is central of order p so, as a consequence of Lemma 200, the cardinality of HG_4 is at least p^3. Moreover, by Lemma 192, the cardinality of G is equal to p^6. The subgroup HG_4 is contained in the normalizer of H and, in particular, $|G : \mathrm{N}_G(H)| \leq |G : HG_4| \leq p^3$. 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 it follows from Lemma 94 that

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

By Lemma 202, the cardinality of Y_C^+ is equal to p, so we get a contradiction to Lemma 203. ■

Lemma 205. *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. Thanks to Lemma 204, the normalizer of each element H of Y_C^+ is equal to HG_4. It follows from the definition of Y_C that, given any $H \in Y_C^+$, the A-stable subgroup $\mathrm{N}_G(H)$ does not contain G_2. As a consequence of Lemma 85, the subgroup G^+ is not contained in $\mathrm{N}_G(H)$. From the combination of Lemmas 81 and 94, we get that $|Y_C| < \sum_{H \in Y_C^+} |G : \mathrm{N}_G(H)|$. By Lemma 204, the normalizer of each element of Y_C^+ has index at most p^3 in G, so, together with Lemmas 202 and 203, we obtain $p^4 = |Y_C| < |Y_C^+|\, p^3 = p^4$. Contradiction. ■

Lemma 206. *Let $\overline{\rho}$ be as in Lemma 196. 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 205, 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 Lemma 166 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 190, 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 195, the quotient G_3/G_4 is equal to $\bigcup_{N \in \mathcal{M}} \mathrm{Z}(N)/G_4 = \bigcup_{N \in \mathcal{M}} \overline{\rho}(N/G_2)$ and so $\overline{\rho}$ is surjective. By Lemma 192, 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 189 is the same as Proposition 199, which we now prove. Let Q be a finite p-group of class at least 4. Assume that $\mathrm{int}(G) > 1$. As a consequence of Lemma 101, the group Q/Q_5 has intensity greater than 1, so Lemma 206 yields $Q_3 = Q^pQ_5$. The subgroup Q^p being normal in Q, it follows from Lemma 166 that $Q^p = Q_3$. The proof of Proposition 199 is now complete.

7.4 Groups of class 5

In analogy with Sections 7.1 and 7.3, this section serves as foundations for the results in Section 7.5.

Until the end of Section 7.4, the following assumptions will hold. Let p be a prime number and let G be a finite p-group. Let $\rho : G \to G$ denote the p-the powering on G, i.e. the map $x \mapsto x^p$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G and, for each positive integer i, write $w_i = \mathrm{wt}_G(i)$. Assume that $|G_5| = p$, so G has class 5. Furthermore, assume that $\mathrm{int}(G) > 1$, so p is odd. Let α be an intense automorphism of G of order 2 and write $A = \langle \alpha \rangle$.

Lemma 207. *One has $(w_1, w_2, w_3, w_4, w_5) = (2, 1, 2, 1, 1)$ and the order of G is p^7. Moreover, one has $\mathrm{Z}(G) = G_5$.*

Proof. As a consequence of Lemma 101, the intensity of G/G_5 is greater than 1. The group G/G_5 has class 4, so from Lemma 192 it follows that $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$ and that the order of G/G_5 is p^6. Since G_5 has order p, the order of G is equal to p^7. The centre of G is equal to G_5 by Lemma 171. ■

Lemma 208. *The subgroup G_3 is abelian and $G_2 \subseteq \mathrm{C}_G(G_4)$.*

Proof. The group G_6 being trivial, both claims follow from Lemma 20. ■

Lemma 209. *One has $|G_3 : \mathrm{C}_{G_3}(G_2)| \leq p$.*

Proof. To lighten the notation, let $C = \mathrm{C}_{G_3}(G_2)$. By Lemma 23, the commutator map induces a bilinear map $\gamma : G_2/G_3 \times G_3/G_4 \to G_5$ whose right kernel is equal to C/G_4. It follows that γ induces an injective homomorphism $G_3/C \to \mathrm{Hom}(G_2/G_3, G_5)$. By Lemma 207, both w_2 and w_5 are equal to 1, so $\mathrm{Hom}(G_2/G_3, G_5)$ has order p. In particular, we get $|G_3 : C| \leq p$. ■

Lemma 210. *The restriction of ρ to G_2 is an endomorphism of G_2.*

Proof. Thanks to Lemma 207, the group G_2/G_3 is cyclic and so $[G_2, G_2] = [G_2, G_3]$. From Lemma 20, it follows that $[G_2, G_2]$ is contained in G_5, which is equal to the centre of G by Lemma 207. In particular, the class of G_2 is at most 2 and, p being odd, Lemma 50 yields that G_2 is regular. Now the commutator subgroup of G_2 is contained in G_5, whose order is p, so, by Lemma 51, the restriction of ρ to G_2 is an endomorphism of G_2. ■

7.5 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 (see List of Symbols). In this section, we prove the following result.

Proposition 211. *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 7.5. 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 $w_5 = 1$. Then the class of G is 5. Assume moreover that $\mathrm{int}(G) > 1$, so, thanks to Proposition 95, the prime p is odd. 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 are exactly 2 and 4 and denote $X^+ = \{H \in X : \alpha(H) = H\}$. In this section, the List of Symbols will be fully respected.

Lemma 212. *The elements of X have order p^2.*

Proof. Let H be an element of X. As a consequence of Lemma 207, both widths $\mathrm{wt}_H^G(2)$ and $\mathrm{wt}_H^G(4)$ are equal to 1. Now apply Lemma 84. ■

Lemma 213. *Assume that G_2 has exponent p. Let H be a subgroup of G. Then $H \in X$ if and only if there exist $x \in G_2\backslash G_3$ and $y \in G_4\backslash G_5$ 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 82. We prove the converse. The subgroup H has order p^2, by Lemma 212, and H cannot be cyclic, because it is contained in G_2. The jumps of H in G being 2 and 4, it follows from Lemma 82 that there exist elements x and y in H of depths respectively 2 and 4 in G. As a consequence of Lemma 208, the subgroup H decomposes as $H = \langle x\rangle \oplus \langle y\rangle$. ■

Lemma 214. *Assume that G_2 has exponent p. Then $|X| = p^4$.*

Proof. Thanks to Lemma 213, 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 $p(p-1)^2$. From Lemma 207 it follows that the cardinalities of $G_2 \setminus G_3$ and $G_4 \setminus G_5$ are respectively $p^5 - p^4$ and $p^2 - p$. We conclude by computing

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

■

Lemma 215. *One has $X^+ = \{G^+\}$.*

Proof. From Lemmas 85 and 207, it follows that G^+ has order p^2. Let now H be an element of X^+. It follows from Lemma 85 that $H \cap G^+$ has cardinality p^2 and, thanks to Lemma 212, the subgroups H and G^+ are the same. In particular, the only element of X^+ is G^+. ■

Lemma 216. *The exponent of G_2 is different from p.*

Proof. We work by contradiction, assuming that the exponent of G_2 is p. To lighten the notation, write $C = \mathrm{C}_{G_3}(G_2)$ and $N = CG^+$. The group C is characteristic in G, so N is a subgroup of G. Moreover, G^+ is contained in G_2, thanks to Lemma 85, so N is a subgroup of $\mathrm{N}_G(G^+)$. By Lemma 209, the group C is contained in G_3 with index at most p and, by Lemma 207, the quadruple (w_2, w_3, w_4, w_5) is equal to $(1, 2, 1, 1)$. It follows from Lemma 84 that the order of N is at least p^4. The order of G is p^7, by Lemma 207, and thus $|G : N| \leq p^3$. By Lemma 215, the set X^+ has only one element, namely G^+, so Lemma 94 yields

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

Contradiction to Lemma 214. ■

Lemma 217. *One has $\rho(G_2) = G_4$.*

Proof. As a consequence of Lemma 210, the set $\rho(G_2)$ is a characteristic subgroup of G and, by Lemma 216, it is non-trivial. By Lemma 207, the centre of G is equal to G_5 so, as a consequence of Lemma 29, the intersection $G_5 \cap \rho(G_2)$ is non-trivial. The order of G_5 being p, the subgroup $\rho(G_2)$ contains G_5. Thanks to Proposition 123, the quotient G_2/G_4 is elementary abelian and so $G_5 \subseteq \rho(G_2) \subseteq G_4$. By Lemma 207, the dimension of G_4/G_5 is 1 and therefore there are 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 169, 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 211. To this end, let Q be a finite p-group of class at least 5 with $\mathrm{int}(Q) > 1$. Then the group Q/Q_6 has class 5 and, as a consequence of Lemma 101, the intensity of Q/Q_6 is greater than 1. By Lemma 217, the subgroups $(Q_2/Q_6)^p$ and Q_4/Q_6 are equal, and so $Q_2^p Q_6 = Q_4$. The subgroup Q_2^p being normal in G, it follows from Lemma 166 that $Q_2^p = Q_4$. This concludes the proof of Proposition 211.

We remark that Proposition 211 can be easily derived, when p is greater than 3, from Theorem 189. 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 218. 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 218. *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 218 is that of saying that, if G satisfies the assumptions of Theorem 218 and we writw $w_i = \mathrm{wt}_G(i)$, then

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

The restriction to primes greater than 3 in Theorem 218 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 125(2) and 164 that Theorem 218 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 219. We refer to Section 1.5, for an overview of regular p-groups.

Proposition 219. *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 219 at the end of Section 8.1.

Lemma 220. *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, the group G is regular by Lemma 50. We assume that G has class at least 4. It follows from Lemma 101 that $\mathrm{int}(G/G_5)$ is larger than 1, and so, thanks to Lemma 192, the index $|G : G_3|$ is equal to p^3. From Theorem 189, we get that $G^p = G_3$, and therefore $|G : G^p| < p^p$. The group G is regular, by Lemma 53, so, thanks to Lemma 52, the subgroup G^p coincides with $\rho(G)$. The proof is now complete. ■

We would like to stress that, for $p > 3$, Proposition 220(2) is a stronger version of Theorem 189. 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 221. *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 by Lemma 50. Assume by contradiction that G is regular of class at least 3. As a consequence of Theorem 125(2), the group G is 2-generated, and so, by Lemma 55, the subgroup G_2 is cyclic. Proposition 123 yields that $G_3 = \{1\}$. Contradiction. ■

We now give the proof of Proposition 219. 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 95 that p is odd. The implication (2) $\Rightarrow$ (1) is given by Lemma 221. We prove (1) $\Rightarrow$ (2). Assume that G is not regular. Then Lemma 220 yields $p = 3$. Moreover, the class of G is larger than 2, as a consequence of Lemma 50. The proof of Proposition 219 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 222. *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 $\mathrm{rk}(G) = 3$.*

We recall that, if G is a group and n is a positive integer, then the subgroup $\mu_n(G)$ is defined to be $\langle x \in G : x^n = 1 \rangle$.

Lemma 223. *Let p be a prime number and let G be a non-trivial finite p-group. Then* $\mathrm{rk}(G) \leq \log_p |\mu_p(G)|$.

Proof. This is is Corollary 2 from [Laf73]. ■

Lemma 224. *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* $\mathrm{rk}(G) \leq 3$.

Proof. Assume that $\mathrm{int}(G) > 1$. By Theorem 189, the subgroup G^p is equal to G_3 so, by Lemma 52(3), the order of $\mu_p(G)$ is equal to $|G : G^p| = |G : G_3|$. As a consequence of Theorem 164, the index $|G : G_3|$ is equal to p^3, and thus Lemma 223 yields $\mathrm{rk}(G) \leq \log_p |G : G_3| = 3$. ■

We can now finally prove Proposition 222. In order to do this, let p be a prime number and let G be a finite p-group of class at least 4, with $\mathrm{int}(G) > 1$. Thanks to Lemma 224, it 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 101, it has intensity greater than 1. As a consequence of Theorem 164, the index $|G_2 : G_4|$ is equal to p^3 and, thanks to Proposition 123, 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 222 is now proven.

We would like to remark that, if $p = 3$, then Proposition 222 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 225, which is the same as Theorem 218.

Proposition 225. *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 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 95, the prime p is odd and G is non-trivial. Let α be an intense automorphism of G of order 2 and write $A = \langle \alpha \rangle$.

Lemma 226. *Let $i \in \mathbb{Z}_{\geq 1}$ be such that $w_i w_{i+1} = 1$. Then $i > 1$.*

Proof. The subgroup G_{i+1} being non-trivial, Lemma 31 yields $i > 1$. ■

Lemma 227. *Assume that $w_2 w_3 = 1$. Then $c = 3$.*

Proof. The widths w_2 and w_3 are both equal to 1, so Theorem 164 yields $c = 3$. ■

Lemma 228. *Let $i \in \mathbb{Z}_{\geq 1}$ be such that $w_i w_{i+1} = 1$. If $c > 3$, then $i \geq 4$.*

Proof. Assume that the class of G is at least 4. Then, by Lemma 101, the group G/G_5 has intensity greater than 1. Theorem 164 yields $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$ and therefore $i \geq 4$. ■

Lemma 229. *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 Lemma 228 yields $i - 1 > 1$. The width w_{i-1} is at most 2, as a consequence of Theorem 165, and thus, 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 165 and the minimality of i, whenever $j < i$, the product $w_j w_{j+1}$ is equal to 2. Moreover, by Theorem 125(2), we have that $w_1 = 2$, so i is even. ■

Lemma 230. *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 101. The group $[G_{i-1}, G_{i-1}]$ is contained in G_{2i-2}, by Lemma 20, and, by Lemma 228, 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 $[\overline{G}_{i-1}, \overline{G}_{i-1}]^p = \{1\}$. As a consequence of Corollary 48, the p-power map is an endomorphism of $\overline{G}_{i-1}$. Now, thanks to Proposition 123, the subgroup $\overline{G}_{i-1}^p$ is contained in $\overline{G}_{i+1}$ and, from Lemmas 52(3) and 229, 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 166, the subgroup $\overline{G}_i$ is contained in $\mu_p(\overline{G}_{i-1})$. Hence the p-power map factors thus as a homomorphism $\overline{G}_{i-1}/\overline{G}_i \to \overline{G}_{i+1}$. By Lemma 229, the index i is even, and so, by Proposition 134, 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 63 that α restricts to the inversion map on $\overline{G}_{i-1}^p$. Moreover, again by Proposition 134, the action of A on $\overline{G}_{i+2}$ is trivial. It follows from Lemma 66 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 171. Lemma 29 yields $\overline{G}_{i-1}^p = \{1\}$. ■

We conclude Section 8.3 with the proof of Proposition 225. By Lemma 226, the integer i is larger than 1. If $i = 2$, then Lemma 227 yields $c = 3 = i + 1$. 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. By Lemma 35, there exists a normal subgroup N of G that is contained in G_{i+2} with index p. We fix N and denote the quotient G/N by $\overline{G}$. Lemma 101 yields $\mathrm{int}(\overline{G}) > 1$. By Lemma 229, the width $\mathrm{wt}_{\overline{G}}(i-1) = w_{i-1}$ is equal to 2 so, by Lemma 84, the order of $\overline{G}_{i-1}$ is equal to p^5. By Lemma 228, the index i is at least 4, and thus, as a consequence of Lemma 20, 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 Lemma 28 gives $[M, M] = [M, \overline{G}_i] = \{1\}$. Moreover, the order of M is equal to p^4 and M has exponent p, because of Lemma 230. In particular, M is a 4-dimensional vector space over $\mathbb{F}_p$. Contradiction to proposition 222.

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 231. *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 231, which is given in Section 9.7. An essential contribution to it is given by the theory of "κ-groups" we develop.

Definition 232. *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 206(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 125, 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 results from Section 1.5, 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 206 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 237. 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 233. *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 233 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 234. *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 233 and 234 provide us with sufficient information on the structure of κ-groups to be able to go into the proof of Theorem 231. 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 5.4 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 $\mathrm{MC}(3)$. Since $\mathrm{MC}(3)$ has an elementary abelian commutator subgroup, Proposition 211 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 239.

Lemma 235. *Let G be a group of order 81 and class 3. Then the exponent of G is different from 3.*

Proof. The class of G is 3 so, thanks to Lemma 31, the quotient G/G_2 is non-cyclic. The order of G being 81, it follows that $(\mathrm{wt}_G(1), \mathrm{wt}_G(2), \mathrm{wt}_G(3)) = (2, 1, 1)$. Let now $C = \mathrm{C}_G(G_2)$. Then, by Lemma 137(1), the subgroup C contains G_2 with index 3 and, by Lemma 140, the centre of G is equal to G_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. As a consequence of Lemma 138, the subgroup 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 $aca^{-1} = cd^k$. The element d^k is not equal to the identity element, because a and c do not centralize each other. 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 236. *Let G be a finite 3-group of class 3 such that $|G : G_2| = 9$. Then $G_3 = G^3$.*

Proof. The class of G is equal to 3 and so G_3 is central in G. By Lemma 135(1), the index $|G_2 : G_3|$ is equal to 3 and, by Lemma 135(2), the order of G_3 is either 3 or 9. As a consequence of Lemma 139, moreover, the subgroup G^3 is contained in G_3. Assume by contradiction that $G_3 \neq G^3$. Then, by Lemma 35, there exists a normal subgroup M of G such that $G^3 \subseteq M \subseteq G_3$ and $|G_3 : M| = 3$. Fix such M. Then the quotient G/M has class 3 and order 81. Moreover, the exponent of G/M is equal to 3. Contradiction to Lemma 235. ∎

Lemma 237. *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. The class of G is at most 3, so the subgroup G_3 is central. Fix x and y in

G. Then we have

$$\begin{aligned}(xy)^3 &= xyxyxy \\ &= xyx[y,x]xy^2 \\ &= xyx[[y,x],x]x[y,x]y^2 \\ &= xyxx[y,x]y^2[[y,x],x] \\ &= x[y,x]xyx[y,x]y^2[[y,x],x] \\ &= x[[y,x],x]x[y,x]yx[y,x]y^2[[y,x],x] \\ &= x^2[y,x]yx[y,x]y^2[[y,x],x]^2 \\ &= x^2[y,x]^2xy[y,x]y^2[[y,x],x]^2 \\ &= x^2[y,x]^2[xy,[y,x]][y,x]xy^3[[y,x],x]^2 \\ &= x^2[y,x]^3xy^3[[y,x],x]^2[xy,[y,x]].\end{aligned}$$

The commutator subgroup of G being annihilated by 3, the element $[y,x]^3$ is trivial. Moreover, thanks to Lemma 24, the commutator map induces a bilinear map $G/G_2 \times G_2/G_3 \to G_3$. It follows that

$$\begin{aligned}(xy)^3 &= x^3y^3[[y,x],x]^2[xy,[y,x]] \\ &= x^3y^3[[y,x],x^2][[y,x],(xy)^{-1}] \\ &= x^3y^3[[y,x],x^2y^{-1}x^{-1}] \\ &= x^3y^3[[y,x],xy^{-1}] \\ &= x^3y^3[xy^{-1},[x,y]].\end{aligned}$$

The proof is now complete. ■

Lemma 238. *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 236, the image of the cubing map is contained in G_3 and, by Lemma 141, 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 237, 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 232, the real requirement for a 3-group G satisfying $|G:G_2| = 9$ to be a κ-group is that the map from Lemma 238 is a bijection. The reason why we are interested in κ-groups is given by the following lemma.

Lemma 239. *Let G be a finite 3-group of class 4 and denote by $(G_i)_{i\geq 1}$ the lower central series of G. Assume that $\mathrm{int}(G) > 1$. Then G is a κ-group.*

Proof. Take $p = 3$ in Lemma 206(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 $(G_i)_{i\geq 1}$ denote the lower central series of G and, for each $i \in \mathbb{Z}_{\geq 1}$, denote $w_i = \mathrm{wt}_G(i)$. 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 238.

Lemma 240. *The group G_2 is abelian.*

Proof. The quotient G_2/G_3 being cyclic, it follows from Lemma 28 that $[G_2, G_2] = [G_2, G_3]$, so, thanks to Lemma 20, we get $[G_2, G_3] \subseteq G_5$. The class of G is 4, so $G_5 = \{1\}$ and G_2 is abelian. ∎

Lemma 241. *The commutator map $G \times G_2 \to G_3$ induces an isomorphism $G/G_2 \otimes G_2/G_3 \to G_3/G_4$.*

Proof. By Lemma 25, the commutator map induces a surjective homomorphism $G/G_2 \otimes G_2/G_3 \to G_3/G_4$. The induced map is bijective because $|G/G_2 \otimes G_2/G_3| = 3^{w_1 w_2} = 9 = 3^{w_3} = |G_3 : G_4|$. ∎

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 242. *Let C be a maximal subgroup of G. Then $G_4 C^3 \subseteq \mathrm{Z}(C)$.*

Proof. The subgroup G_4 is central in G, because the class of G is 4, so G_4 is contained in $\mathrm{Z}(C)$. By Lemma 25, 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 $G_4 C^3/G_4$ being equal to $\kappa(C/G_2)$, it follows that $G_4 C^3$ is contained in the centre of C. ∎

Lemma 243. *There exists at most one maximal subgroup C of G such that $G_3 \subseteq \mathrm{Z}(C)$.*

Proof. Let C and D be maximal subgroups of G such that G_3 is contained in $\mathrm{Z}(C) \cap \mathrm{Z}(D)$. Then CD centralizes G_3 and, the class of G being equal to 4, the subgroup CD is different from G. It follows that $C = D$. ∎

Lemma 244. *Assume that G is a κ-group. Then $\mathrm{Z}(G) = G_4$.*

Proof. We first claim that $G_4 \subseteq \mathrm{Z}(G) \subsetneq G_3$. The subgroup G_4 is contained in $\mathrm{Z}(G)$ and, as a consequence of Lemma 140, one has $\mathrm{Z}(G)/G_4 \subseteq \mathrm{Z}(G/G_4) = G_3/G_4$. Since the class of G is 4, the inclusion $\mathrm{Z}(G) \subseteq G_3$ is not an equality so the claim is proven. Now, by Lemma 36, the subgroup 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. Thanks to Lemma 243, there exist two distinct maximal subgroups C and D of G such that both $\mathrm{Z}(C)$ and $\mathrm{Z}(D)$ do not contain G_3. Fix such C and D. Since κ is a bijection and $w_3 = 2$, Lemma 242 yields $\mathrm{Z}(C) \cap G_3 = C^3G_4$ and $\mathrm{Z}(D) \cap G_3 = D^3G_4$. Now, the subgroup $\mathrm{Z}(G)$ contains G_4 and is contained in $\mathrm{Z}(C) \cap \mathrm{Z}(D) \cap G_3 = C^3G_4 \cap D^3G_4$. The map κ being a bijection, the subgroup $C^3G_4 \cap D^3G_4$ is equal to G_4 and therefore $\mathrm{Z}(G) = G_4$. ■

Lemma 245. *Let C be a maximal subgroup of G. Assume moreover that G is a κ-group and that G_2 has exponent* 3*. Then $[C,C] \cap \mathrm{Z}(C) = G_4$.*

Proof. The quotient C/G_2 is cyclic of order 3 so, by Lemma 28, the subgroups $[C,C]$ and $[C,G_2]$ are equal. It follows that $[C,C]$ is contained in G_3 and, from Lemma 241, 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, the subgroup $[C,C]$ is characteristic in the normal subgroup C and therefore it is itself normal in G; Lemma 29 yields $[C,C] \cap \mathrm{Z}(G) \neq 1$. By Lemma 244, the centre of G is equal to G_4 and thus $[C,C]$ 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 therefore 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 $[C,C]$. We get that $[C,C]$ is contained in $\mathrm{Z}(C)$ and so, as a consequence of Lemmas 50 and 51, the cubing map is an endomorphism of C. By assumption, the exponent of G_2 is 3, and so it follows that

$$|C^3| = |C : \mu_3(C)| \leq |C : G_2| = 3.$$

Since C^3 contains G_4, we get that $C^3 = G_4$. Contradiction. ■

Lemma 246. *Assume that G is a κ-group. Then G_3 has exponent* 3*.*

Proof. The subgroup G_2 is abelian, by Lemma 240, and G_2^3 is contained in G_4, as a consequence of Lemma 238. 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 140. Contradiction to Lemma 29. ∎

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 231, 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 $M_i = (1 + \mathfrak{m}^i) \cap G$. 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 231.

Lemma 247. *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 248. *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

$$\begin{aligned} c = ab\overline{a}\overline{b} &\equiv (1 - \epsilon + \mathrm{i})(1 - \epsilon + \mathrm{j})(1 - \epsilon - \mathrm{i})(1 - \epsilon - \mathrm{j}) \\ &\equiv (1 + \epsilon + \mathrm{i} + \mathrm{j} + \mathrm{k})(1 + \epsilon - \mathrm{i} - \mathrm{j} + \mathrm{k}) \\ &\equiv 1 - \mathrm{k} \bmod G_3. \end{aligned}$$

Thanks to Lemma 24, 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 232, 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 249. *The group* $\mathrm{MC}(3)$ *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 247, the group G has class 4 and, by Lemma 248(1), one has $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. Let $\kappa : G/G_2 \to G_3/G_4$ be as in Lemma 238; we want to show that κ is a bijection. Let a and b be as in Lemma 248(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 $w_2 = 1$, it follows from Lemma 241 that 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 237 that

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

We have proven that κ is surjective so, the widths w_1 and w_3 being the same, it follows that κ is a bijection. ∎

Lemma 250. *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* $\mathrm{MC}(3)$. *Moreover, α 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 248(1), the order of G/G_2 is 9. It follows from Lemma 36(2) that G/G_2 is elementary abelian. We define $a = 1 - \epsilon + \mathrm{i}$ and $b = 1 - \epsilon + \mathrm{j}$. Then a and b span G modulo G_2 and

$$\alpha(a) = \bar{a} = a^{-1} \;\text{ and }\; \alpha(b) = \bar{b} = b^{-1}.$$

The quotient G/G_2 being commutative, the map $G/G_2 \to G/G_2$ that is induced by α is equal to the inversion map $x \mapsto x^{-1}$. ∎

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 $3.\mathrm{J}_3$ of the simple Janko-3 group J_3. If S is a Sylow 3-subgroup of $3.\mathrm{J}_3$ and N denotes the normalizer of S in $3.\mathrm{J}_3$, 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

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

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 251. *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 251, 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 252. *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

$$\begin{aligned}(x+y)^5 = \sum_{k=0}^{5} \binom{5}{k} x^k y^{5-k} &= x^5 - xy^4 + x^2y^3 + x^3y^2 - x^4y + y^5 \\ &= x^5 + y^5 + (x-y)(xy^3 - x^3y)\end{aligned}$$

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

Lemma 253. *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 252, the map σ_V is well-defined. ■

Lemma 254. *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 homomorphism $\mathrm{Aut}(V) \to \mathrm{Sym}(\mathbb{P}V)$ factors as an injective homomorphism $\mathrm{Aut}(V)/\mathbb{F}_3^* \to \mathrm{Sym}(\mathbb{P}V)$, which is in fact also surjective, because $|\,\mathrm{Aut}(V) : \mathbb{F}_3^*| = 48/2 = 24 = |\,\mathrm{S}_4\,| = |\,\mathrm{Sym}(\mathbb{P}V)|$. ■

Lemma 255. *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 254 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 256. *Write $V = \mathbb{F}_3[i]$, with $i^2 = -1$. Then the map $\bigwedge^2 V \to \mathbb{F}_3 i$ that is 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. ■

Lemma 257. *Write $V = \mathbb{F}_3[i]$, with $i^2 = -1$. Then the map $\mu : V \otimes \mathbb{F}_3 i \to V$ that is defined by $x \otimes y \mapsto xy$ is an isomorphism of vector spaces.*

Proof. The map $V \times \mathbb{F}_3 i \to V$ that is defined by $(x, y) \mapsto xy$ is a bilinear surjective map. By the universal property of tensor products, it factors as the surjective homomorphism $\mu : V \otimes \mathbb{F}_3 i \to V$. The dimensions of $V \otimes \mathbb{F}_3 i$ and V being the same, μ 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

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

and note that θ is an isomorphism of vector spaces, as a consequence of Lemma 256. Let μ be as in Lemma 257. We keep this notation until the end of Section 9.3.

Lemma 258. *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

$$\begin{aligned} l_V(\kappa)(x + y) &= \mu \circ \theta \circ \kappa(x + y) \\ &= \mu \circ \theta(\kappa(x) + \kappa(y) + (x - y) \otimes (x \wedge y)) \\ &= l_V(\kappa)(x) + l_V(\kappa)(y) + \mu \circ \theta((x - y) \otimes (x \wedge y)) \\ &= l_V(\kappa)(x) + l_V(\kappa)(y) + (x - y)(xy^3 - x^3 y). \end{aligned}$$

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 259. *Let l_V be as in Lemma 258. 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

$$\begin{aligned} l_V(\kappa)(x) &= \mu \circ \theta(ix \otimes ix \wedge x) \\ &= \mu(ix \otimes ((ix)x^3 - (ix)^3 x)) \\ &= ix((ix)x^3 - (ix)^3 x) \\ &= \lambda(x) \end{aligned}$$

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 260. *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 $\mathbb{F}_3x + \mathbb{F}_3ix = V = \mathbb{F}_3x + \mathbb{F}_3jx$ and therefore there exists $\omega_x \in \{\pm 1\}$ such that $ix \equiv \omega_x jx \bmod \mathbb{F}_3x$. 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, the elements 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 261. *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 $\mathrm{End}(V)$ being equal to the order of V^2, it follows that each element ψ of $\mathrm{End}(V)$ 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 262. *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 $\mathrm{End}(V)$, so, thanks to Lemma 252, we have $\lambda \in (x \mapsto x^5) + \mathrm{End}(V)$. It now follows from Lemma 261 that there exist $a, b \in V$ such that, for each $x \in V$, we have $\lambda(x) = x^5 + ax^3 + bx$. ■

Lemma 263. *Let m be a positive integer and let q be a prime power. Then*

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

Proof. This is Lemma 2.5.1 from [Coh07]. ■

Lemma 264. *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 262. 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 263 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 265. *The cardinality of* Λ *is at most* 3.

Proof. Let $\lambda \in \Lambda$ and let $b \in V$ be as in Lemma 264. The map λ is bijective and so, with x replaced by $\lambda(x)$, Lemma 263 gives

$$\begin{aligned} 0 = \sum_{x \in V} \lambda(x)^4 &= \sum_{x \in V} (x^5 + bx)^4 \\ &= \sum_{x \in V} (x^{10} - bx^6 + b^2x^2)^2 \\ &= \sum_{x \in V} (bx^{16} + b^3x^8) \\ &= -b(1 + b^2). \end{aligned}$$

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 251. The function $s_V : \mathcal{I}_V \to \mathcal{K}_V$ is injective by Lemma 260 and, by Lemma 255, 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 258, the set Λ has the same cardinality as $\mathcal{K}_V$ and thus, as a consequence of Lemma 265, 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 251 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 the present section, we consider κ-groups of class 3 and we prove the following main result.

Proposition 266. *Let* G *be a* κ*-group of class* 3. *Then* G *is isomorphic to* $\mathrm{MC}(3) \,/\, \mathrm{MC}(3)_4$.

As a consequence of Lemma 36(2), each κ-group is 2-generated. Our strategy, for proving Proposition 266, 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 5.4 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 $\mathbb{F}_3$, by construction, 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 267. *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. The map c_3 is well-defined, by definition of L, and $L/F_3 = (F^3F_3)/F_3$. As a consequence of Lemma 48, the map c_3 is a surjective homomorphism, which, F_2^3 being contained in F_3, factors as a surjective homomorphism $c_2 : F/F_2 \to L/F_3$. Since $V = F/F_2$ 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. The group A being abelian, we have that F_3 is contained in $\ker\psi$. Moreover, 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 has cardinality at least 9 and so $|L : F_3| = 9$. In addition, the map c_2 is an isomorphism of groups. ■

Lemma 268. *One has $|F_3 : E| \geq 9$.*

Proof. Thanks to Lemma 248, we have $|\operatorname{MC}(3) : \operatorname{MC}(3)_2| = 9$ and therefore, as a consequence of Lemma 36(2), the group MC(3) is 2-generated. We fix a surjective homomorphism $\phi : F \to \operatorname{MC}(3)$ and we denote by π the canonical projection $\pi : \operatorname{MC}(3) \to \operatorname{MC}(3) / \operatorname{MC}(3)_4$. The homomorphism $\pi \circ \phi : F \to \operatorname{MC}(3) / \operatorname{MC}(3)_4$ is surjective and so, from Lemma 157, we get $L = (\pi\circ\phi)^{-1}(\operatorname{MC}(3)_3 / \operatorname{MC}(3)_4)$. As a consequence, L is equal to $\phi^{-1}(\operatorname{MC}(3)_3)$ and thus $\phi(L) = \operatorname{MC}(3)_3$. Moreover, thanks to Lemma 141, we know that $\operatorname{MC}(3)_2^3$ is contained in $\operatorname{MC}(3)_4$ and therefore $\phi(F_2^3) \subseteq \operatorname{MC}(3)_4$. It follows that

$$\phi(F_3) = \phi([F, F_2])\phi(F_2^3) = [\operatorname{MC}(3), \operatorname{MC}(3)_2]\operatorname{MC}(3)_2^3 = \operatorname{MC}(3)_3$$

and also that

$$\phi(E) = \phi([F, L])\phi(F_2^3) = [\operatorname{MC}(3), \operatorname{MC}(3)_3]\operatorname{MC}(3)_2^3 = \operatorname{MC}(3)_4\,.$$

As a result, the index $|F_3 : E|$ is at least $|\operatorname{MC}(3)_3 : \operatorname{MC}(3)_4|$, which is, by Lemma 248(1), equal to 9. ■

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

Lemma 269. *The commutator map $F \times F_2 \to F_3$ induces an isomorphism of groups $\delta : F/F_2 \otimes F_2/L \to \overline{F_3}$. Moreover, $|F_3 : E| = 9$.*

Proof. The subgroup $\overline{F_3}$ is central in $\overline{F}$, by definition of E, and so, by Lemma 22, the commutator map $F \times F_2 \to \overline{F_3}$ is bilinear. Moreover, the quotient F_2/L is cyclic of order 3, thanks to Lemma 157, and so, by Lemma 28, the subgroup $[F_2, F_2]$ is equal to $[F_2, L]$. The commutator map factors thus as a surjective homomorphism $\delta : F/F_2 \otimes F_2/L \to \overline{F_3}$ and therefore $|F_3 : E| \leq |F/F_2 \otimes F_2/L| = 9$. Now, the group $\overline{F_3}$ has order at least 9, by Lemma 268, and therefore $|F_3 : E| = 9$ and δ is an isomorphism. ■

Lemma 270. *The group $\overline{L}$ is an $\mathbb{F}_3$-vector space of dimension 4.*

Proof. By the definition of E, the group $\overline{L}$ is central in $\overline{F}$ and so it is abelian. Moreover L^3 is contained in F_2^3, which is itself contained in E. It follows that $\overline{L}$ is naturally a vector space over $\mathbb{F}_3$. The dimension of $\overline{L}$ is equal to 4, thanks to the combination of Lemmas 267 and 269. ■

Lemma 271. *The commutator map $F \times F_2 \to F_3$ induces an isomorphism of groups $\gamma : V \otimes \bigwedge^2 V \to \overline{F_3}$.*

Proof. The subgroup F_2 is central modulo L so, thanks to Lemma 22, 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 157, the cardinality of F_2/L is equal to 3, which is the same as the cardinality of $\bigwedge^2 V$ and so, θ being non-trivial, it is an isomorphism of groups. We conclude by defining $\gamma = \delta \circ (1 \otimes \theta)$, where δ is as in Lemma 269. ■

Lemma 272. *Let γ be as in Lemma 271 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 subgroup $[F, [F, F]]$ is contained in L, which is central modulo E, so $\overline{F}$ has class at most 3. Moreover, $[F, F]^3$ is contained in F_2^3 and so $[\overline{F}, \overline{F}]$ has exponent at most 3. By Lemma 237, 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 the vector spaces V and $\overline{L}$, it follows from the definition of γ that, for each $x, y \in V$, one has $c(x + y) = c(x) + c(y) + \gamma((x - y) \otimes (x \wedge y))$. ■

Lemma 273. *Let $0 \to A \overset{\iota}{\to} B \overset{\sigma}{\to} C \to 0$ 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

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

$$s(u + v) - s(u) - s(v).$$

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 $f \circ s(u) = g(u)$. We prove now that f is a homomorphism. Let $x, y \in B$ and let $a, b \in A$ and $u, v \in C$ be such that $x = \iota(a) + s(u)$ and $y = \iota(b) + s(v)$. Keeping in mind that g belongs to $\mathcal{H}$, we compute

$$\begin{aligned} f(x+y) - f(x) - f(y) &= f(\iota(a) + s(u) + \iota(b) + s(v)) - f(\iota(a) + s(u)) + \\ &\quad - f(\iota(b) + s(v)) \\ &= f(\iota(a) + \iota(b) - g(u+v) + g(u) + g(v) + s(u+v)) + \\ &\quad - f(\iota(a) + s(u)) - f(\iota(b) + s(v)) \end{aligned}$$

and, since $g(C)$ is contained in A, we get

$$\begin{aligned} f(x+y) - f(x) - f(y) &= a + b - g(u+v) + g(u) + g(v) + g(u+v) + \\ &\quad - f(a + s(u)) - f(b + s(v)) \\ &= a + b + g(u) + g(v) - a - g(u) - b - g(v) \\ &= 0. \end{aligned}$$

We have proven that f is a homomorphism and so ν is surjective. ■

Proposition 274. *Let c be as in Lemma 272 and let γ be as in Lemma 271. Set $\mathcal{P} = \{\pi \in \mathrm{Hom}(\overline{L}, \overline{F_3}) : \pi_{|\bar{F}_3} = \mathrm{id}_{\bar{F}_3}, \pi \circ c$ 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 267. 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 273 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 273, 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 272, 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 272 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 251, 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 275. *There exists M in $\mathcal{N}_3$ such that the quotient F/M is isomorphic to* $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$. *Moreover, the set $\mathcal{N}_3$ is non-empty.*

Proof. The group MC(3) is a κ-group, by Lemma 249, and it has class 4, by Lemma 247. It follows that there exists M in $\mathcal{N}_3$ such that F/M is isomorphic to $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$ and, in particular, $\mathcal{N}_3$ is non-empty. ■

Lemma 276. *Let $\mathcal{P}$ be as in Proposition 274 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 $G = F/K_\pi$. Since $|F : F_2| = 9$, Lemma 36 yields that G_2 is equal to F_2/K_π. Moreover, it easily follows from the definition of $\mathcal{P}$ that $\overline{L}$ 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 269, the subgroup G_3 coincides with L/K_π. The class of G is equal to 3, because L is central modulo E. Now, the map $\pi \circ c$ being bijective, it follows that 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, we have that $|L : K_\pi| = |G_3| = |G : G_2| = |F : F_2| = 9$ and G is a κ-group. The choice of π being arbitrary, we have proven that 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 277. *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 251 and 274 and Lemma 276. 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 255, the set $\mathcal{I}_V$ has cardinality 3 and so $\mathcal{N}_3$ has cardinality 3. Again by Lemma 255, the action of $\mathrm{Aut}(V)$ on $\mathcal{I}_V$ is transitive and thus the action of $\mathrm{Aut}(F)$ on $\mathcal{I}_V$ is transitive. Since the map ψ is an isomorphism of $\mathrm{Aut}(F)$-sets, the action of $\mathrm{Aut}(F)$ on $\mathcal{N}_3$ is transitive. ■

We are finally ready to give the proof of Proposition 266. Let G be a κ-group of class 3. As a consequence of Proposition 275, there exist N and M normal subgroups of F such that F/N and F/M are respectively isomorphic to G and $\mathrm{MC}(3)\,/\,\mathrm{MC}(3)_4$. Fix such M and N. Then, thanks to Lemma 277, there exists an automorphism of F mapping M to N, which thus induces an isomorphism between G and $\mathrm{MC}(3) / \mathrm{MC}(3)_4$. The choice of G being arbitrary, the proof of Proposition 266 is complete.

We conclude the present section by giving the proof of Theorem 233. If G is a κ-group of class 3, then, by Proposition 266, the group G is isomorphic to $\mathrm{MC}(3) / \mathrm{MC}(3)_4$. On the other hand, the group $\mathrm{MC}(3)$ has class 4, by Lemma 247, and it is a κ-group, by Lemma 249. It follows that $\mathrm{MC}(3) / \mathrm{MC}(3)_4$ is a κ-group of class 3. This proves Theorem 233.

9.5 Extensions of κ-groups

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 239. The main purpose of the present section is that of proving the following proposition, which is the same as Theorem 234.

Proposition 278. *Let G be a κ-group such that G_4 has order 3. Then the subgroup G_2 is elementary abelian.*

Until the end of Section 9.5, we will work under the assumptions of Proposition 278. For each $i \in \mathbb{Z}_{\geq 1}$, we set $w_i = \mathrm{wt}_G(i)$. It follows from the assumptions, together with Lemma 135(1), that $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$. Moreover, the group G/G_4 being a κ-group of class 3, Proposition 266 yields that G/G_4 is isomorphic to $\mathrm{MC}(3) / \mathrm{MC}(3)_4$. It follows from Lemma 248(2) that there exist generators a, b of G satisfying $a^3 \equiv [b, [a, b]]^{-1} \bmod G_4$ and $b^3 \equiv [a, [a, b]] \bmod G_4$. Call $c = [a, b]$, $d = [a, c]$, and $e = [b, c]$. Let moreover $f = [a, d]$. Then we have $a^3 \equiv e^{-1} \bmod G_4$ and $b^3 \equiv d \bmod G_4$.

Lemma 279. *The elements d and e generate G_3 modulo G_4.*

Proof. The index $|G_2 : G_3|$ is equal to 3, so c generates G_2 modulo G_3. By Lemma 241, the commutator map induces an isomorphism $G/G_2 \otimes G_2/G_3 \to G_3/G_4$, and so d and e span G_3 modulo G_4. ∎

Lemma 280. *One has $G_4 = \langle f \rangle = \langle [b, e] \rangle$.*

Proof. By Lemma 244, the centre of G is equal to G_4 and, by Lemma 190, 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, thanks to Lemma 279, and, by the choice of a and b, 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 281. *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 $b^3 = df^s$.*

Proof. By assumption, the order of G_4 is 3 and, by Lemma 279, both elements f and $[b, e]$ generate G_4. There exists thus $u \in \{\pm 1\}$ such that $[b, e] = f^u$. Moreover, by the choice of a and b, we know that $a^3 \equiv e^{-1} \bmod G_4$ and $b^3 \equiv d \bmod G_4$. There exist hence integers r and s such that $a^3 = e^{-1} f^r$ and $b^3 = df^s$. To conclude, thanks to Lemma 141, 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 278. To this end, let u, t, r, s be as in Lemma 281. By Lemma 240, the subgroup G_2 is abelian and, by Lemma 246, the exponent of G_3 is equal to 3. It follows that

$$\begin{aligned} ab^3 &= cbab^2 \\ &= cbcbab \\ &= cbcbcba \\ &= cecbecb^2a \\ &= ec^2 f^u ebcb^2 a \\ &= f^u e^2 c^2 ecb^3 a \\ &= f^u e^3 c^3 b^3 a \\ &= f^u f^t b^3 a \\ &= f^{u+t} b^3 a \end{aligned}$$

from which we derive

$$fdaf^s = adf^s = ab^3 = f^{u+t} b^3 a = f^{u+t} df^s a.$$

The subgroup G_4 is central, thanks to Lemma 244, and so one gets

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

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

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

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 $c^3 = f^{-1}$ and we compute

$$\begin{aligned}
a^3 b &= a^2 cba \\
&= adcaba \\
&= fdac^2ba^2 \\
&= fd^2cacba^2 \\
&= fd^2cdcaba^2 \\
&= fd^3c^3ba^3 \\
&= ba^3.
\end{aligned}$$

We have shown that 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 242, 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 280. The proof of Proposition 278, and thus that of Theorem 234, is now complete.

Corollary 282. *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 249 and, thanks to Lemma 248(1), the subgroup $\mathrm{MC}(3)_4$ has order 3. It follows from Proposition 278 that $\mathrm{MC}(3)_2$ is elementary abelian. ■

Corollary 283. *Let Q be a finite 3-group of class 4 and let $(Q_i)_{i \geq 1}$ denote the lower central series of Q. If* $\mathrm{int}(Q) > 1$*, then Q_2 is elementary abelian.*

Proof. By Lemma 239, the group Q is a κ-group. Moreover, thanks to Theorem 164, the subgroup Q_4 has order 3. It follows from Proposition 278 that Q_2 is elementary abelian. ■

Corollary 284. *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 101, the intensity of Q/Q_5 is greater than 1, and so, as a consequence of Corollary 283, the subgroup Q_2^3 is contained in Q_5. However, because of Proposition 211, 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 239, which asserts that any finite 3-group of class 4 and intensity greater than 1 is a κ-group. Moreover, we know from Proposition 134, 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 285. *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 285 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

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

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 5.4 or to the diagram before Lemma 303. 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 5.4 and we will thus, in this section, often apply results achieved in Section 5.4. 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

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

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 286. *Let $N \in \mathcal{N}_3$. Then D_N is contained in E.*

Proof. As a consequence of Lemma 157, the subgroup L contains N. Again by Lemma 157, the index $|F_2 : L|$ is equal to 3 and so, thanks to Lemma 28, one has $[F_2, F_2] = [F_2, L]$. We get

$$[F, N]F_2^3[F_2, F_2] \subseteq [F, L]F_2^3[F_2, L] = [F, L]F_2^3 = E$$

and therefore D_N is contained in E. ■

Lemma 287. *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 $\phi([F, F_{k-1}]) \subseteq \phi([F, F_4]) \subseteq \phi([F, E]) = [\phi(F), \phi(E)]$ and so, as a consequence of Lemma 158, we get $\phi([F, F_{k-1}]) \subseteq [G, G_4] = \{1\}$. It follows from Lemma 36 that $\phi(F_k) = \phi(F_{k-1}^3) \subseteq \phi(F_2^3) \subseteq \Phi(G)^3 = G_2^3$ and so Proposition 278 yields $\phi(F_k) = \{1\}$. ■

Lemma 288. *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 85 yields that the map $G^- \to G/G_2$, defined by $g \mapsto gG_2$, is surjective. Thanks to Lemma 36, the subgroups G_2 and $\Phi(G)$ coincide and therefore there exist two elements x and y of G^- that generate G. ■

Proposition 289. *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 287. Let now x and y be as in Lemma 288 and let c and d be elements of F such that $\phi(c) = x$ and $\phi(d) = y$, which exist because ϕ is surjective. As a consequence of Lemma 155, 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 $b \mapsto d$; such ψ exists thanks to the universal property of free groups. 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 290. *Let M be an element of $\mathcal{N}_4$. Then $N = ME$ belongs to $\mathcal{N}_3$ and D_N is contained in 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 158, we get $\pi(N) \subseteq H_4$. 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 $M \neq N$. On the other hand, we 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 $\mathcal{N}_3$. We prove that $\pi(D_N)$ is trivial. The image of F_2 under π is equal to H_2, thanks to Lemma 155. Moreover, the subgroup H_4 is central in H, because H has class 4, and the commutator subgroup of H is elementary abelian, thanks to Proposition 278. We compute

$$\pi(D_N) = \pi([F,N])\pi(F_2^3)\pi([F_2,F_2]) = [H,H_4]H_2^3[H_2,H_2] = \{1\},$$

and so D_N is contained in M. We now prove that $\pi(N) = H_4$. We work by contradiction, assuming that $N \subseteq M$. Since $N = ME$, we get that E is contained in M. As a consequence, the group F/E has class at least 4. However, one has

$$[F,[F,[F,F]]] \subseteq [F,[F,F_2]] \subseteq [F,F_3] \subseteq [F,L] \subseteq E$$

and therefore F/E has class at most 3. Contradiction. ■

Lemma 291. *Let $N \in \mathcal{N}_3$. Denote moreover $H = \mathrm{MC}(3)$. 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, which exists thanks to the universal property of free groups. Set $K = \psi^{-1}(H_4)$. Then K belongs to $\mathcal{N}_3$, because H is a κ-group, and so, thanks to Lemma 277, 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 155 and 157. We conclude by showing that φ induces a surjective homomorphism

$E/D_N \to H_4$. Thanks to Lemma 290, 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

$$\varphi(E) = \varphi([F, L]F_2^3) = [H, H_3]H_2^3 = H_4H_2^3.$$

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 292. *Let $N \in \mathcal{N}_3$. Then the commutator map induces a non-degenerate 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 158, the subgroup E is contained in N and so $[F, E] \subseteq [F, N] \subseteq D_N$. In particular, $\overline{E}$ is central in $\overline{F}$ and so it follows from Lemma 22 that 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 now $H = \mathrm{MC}(3)$. Then, as a consequence of Lemmas 249 and 244, the centre of H is equal to H_4 and thus Lemma 190 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 291, the following diagram is commutative.

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

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 293. *Let V and W be 2-dimensional vector spaces over $\mathbb{F}_3$ and let $\eta : V \to W$ be a bijective map with the property 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. It follows that $(V \otimes V)/K$ has the same dimension as $(V \otimes V)/\Delta = \bigwedge^2 V$ and so $(V \otimes V)/K$ has dimension 1. Let now η be any map satisfying the hypotheses of Lemma 293. 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 254, 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 294. *Let $N \in \mathcal{N}_3$. Then $|E : D_N| = 3$.*

Proof. The quotient F/F_2 is a 2-dimensional vector space over $\mathbb{F}_3$, by definition of F_2, while L/E is a 4-dimensional vector space over $\mathbb{F}_3$, thanks to Lemma 270. Moreover, by Lemma 158, the subgroup N contains E and, as a consequence of Lemma 276, 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 292. Let moreover $c : F/F_2 \to L/E$ be the map from Lemma 272 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 276, 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 272, it is clear that c commutes with scalar multiplication by elements of $\mathbb{F}_3$. Define $K = \langle x \otimes c_N(x) : x \in F/F_2\rangle$. 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 293 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 $\mathbb{F}_3$. By Lemma 292, the quotient E/D_N is non-trivial and so γ is not the trivial map. It follows that $\ker\gamma$ has dimension 3 and thus E/D_N has cardinality 3. ■

The following lemmas pave the way to proving Proposition 300.

Lemma 295. *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 $H = F/L$. The group F being 2-generated, $|F : F_2| = 9$ and so, as a consequence of Lemma 157, the group H has order 27. Thanks to the definitions of F_2 and L, one easily sees that H is non-abelian of exponent 3 and that $H_2 = F_2/L$. Lemma 29 yields that H_2 is central in H. Applying Lemma 27, we get that $H_2 = \mathrm{Z}(H)$ and therefore H is extraspecial. 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 46, 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 $\mathrm{Inn}(H) \rtimes \langle\eta\rangle$ and ensures that there exists $\varphi_L \in \mathrm{Inn}(H)$ with the property that $\beta_L = \varphi_L\eta\varphi_L^{-1}$. ■

Lemma 296. *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 162, the element $\psi = \eta^{-1}\beta_E$ belongs to Δ and so, thanks to Lemma 45, 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 162, it induces the inversion map on L/E. For each $x \in F/F_2$, it follows that

$$(\eta h \eta^{-1})(x) = \eta(h(x^{-1})) = (h(x^{-1}))^{-1} = h(x).$$

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 $x \in F/E$, we compute

$$\begin{aligned}\psi(x)x^{-1} = h(x) &= (\eta h \eta^{-1})(x)\\ &= \eta(h(\eta^{-1}(x)))\\ &= \eta\big(\psi(\eta^{-1}(x))(\eta^{-1}(x))^{-1}\big)\\ &= (\eta\psi\eta^{-1})(x)x^{-1}\\ &= \psi^{-1}(x)x^{-1}\end{aligned}$$

and therefore $\psi(x)^2 = 1$. The group F/E being a 3-group, it follows that ψ coincides with the trivial map and therefore η and β_E are equal. ■

Lemma 297. *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 292, the commutator map induces an injective homomorphism $\varphi : L/N \to \mathrm{Hom}(F/F_2, E/D_N)$. Combining Lemmas 276 and 294, 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 45, 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 298. *Let N be an element of $\mathcal{N}_3$. Then $\beta(D_N) = D_N$.*

Proof. As a consequence of Lemma 162, the group N is $\langle\beta\rangle$-stable and therefore so is D_N. ■

Lemma 299. *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 $\overline{F}$. Thanks to Lemma 298, 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 292 and 61, the automorphism $\eta^{-1}\overline{\beta}$ belongs to Δ and thus, thanks to Lemma 297, we have $\eta^{-1}\overline{\beta} \in \mathrm{Inn}(\overline{F})$. Applying the Schur-Zassenhaus theorem to $\mathrm{Inn}(\overline{F}) \rtimes \langle\eta\rangle$, 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 300. *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 289, 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 290, 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 295 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 296 yields that in fact η_1 and β are the same modulo E. At last, let ψ_N be as in Lemma 299 and define $\eta_2 = \psi_N\eta_1\psi_N^{-1}$. As a consequence of Lemma 299, 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 301. *There exists $M \in \mathcal{N}_4$ such that F/M is isomorphic to* $\mathrm{MC}(3)$. *Moreover, $\mathcal{N}_4$ is non-empty.*

Proof. The group MC(3) is a κ-group, by Lemma 249, and $\mathrm{MC}(3)_4$ has cardinality 3, thanks to Lemma 248(1). By Lemma 247, the class of MC(3) is 4 and moreover, thanks to Lemma 250, the group MC(3) possesses an automorphism that induces the inversion map on the quotient $\mathrm{MC}(3) / \mathrm{MC}(3)_2$. By the universal property of free groups, there exists $M \in \mathcal{N}_4$ such that F/M is isomorphic to MC(3). In particular, $\mathcal{N}_4$ is non-empty. ■

Lemma 302. *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 300, there exists $\gamma \in \mathrm{Inn}(F)$ such that $\alpha\phi = \phi(\gamma\beta\gamma^{-1})$. It follows that

$$\{1\} = \alpha(\phi(M)) = \phi(\gamma\beta\gamma^{-1})(M) = \phi\beta(M)$$

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 $\beta(M) = M$. ■

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

Lemma 303. *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 162, 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 159, the group B acts on F/F_2 through σ and, by Lemma 162, 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 292 and 61 that β induces the identity map on $\overline{E}$ and so, thanks to Theorem 68, the subgroup $\overline{E}$ has a unique $\langle\overline{\beta}\rangle$-stable complement in $\overline{N}$, which coincides with $\overline{N}^-$. ■

Lemma 304. *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 290, 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 302 yields $\beta(M_1) = M_1$ and $\beta(M_2) = M_2$. It follows then from Lemma 303 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 305. *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 304. 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 303. 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 303, 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 294, 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 157 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

$$\pi([F, L]) = [\pi(F), \pi(L)] = [H, H_3\pi(N)] = [H, H_3] = H_4 = \{1\}$$

and therefore $[F, L]$ is contained in M. We get then

$$E = [F, L]F_2^3 \subseteq [F, L]F_2^3[F_2, F_2] \subseteq [F, L]D_N \subseteq M,$$

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. ■

Corollary 306. *The set $\mathcal{N}_4$ has 3 elements and the action of* $\mathrm{Aut}(F)$ *on $\mathcal{N}_4$ is transitive.*

Proof. Combine Proposition 277 and Lemma 305. ■

We are now ready to prove Proposition 285. By Lemma 301, there exists an element M of $\mathcal{N}_4$ with the property that F/M is isomorphic to MC(3). As a consequence of Corollary 306, the natural action of $\mathrm{Aut}(F)$ on $\mathcal{N}_4$ is transitive and therefore G and MC(3) are isomorphic. The proof of Proposition 285 is complete.

9.7 Intensity

In Section 9.5 we have proven Corollary 284, 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 231.

Proposition 307. *The group* MC(3) *has intensity* 2.

We will devote a big part of the present section to the proof of Proposition 307. 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 247, the group G has class 4 and order 729. Moreover, thanks to Lemmas 248(1) and 249, 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 250 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 308. *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, by Corollary 282, and in particular it normalizes each of its subgroups. As a consequence of Lemma 85(1), the subgroup G^+ is contained in G_2 and we conclude combining (1) with Lemma 81. ■

Lemma 309. *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 142, the automorphism α_4 is intense so, by Lemma 93, 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 310. *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, since $H \cap G_4 = \{1\}$, 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 $[C, C]$ and $[C, C] = [C, G_2]$, as a consequence of Lemma 28. Thanks to Lemma 20, the subgroup $[H, H]$ is contained in G_3. By Lemma 244, the centre of G is equal to G_4 and so, by Lemma 190, 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 282 and Lemma 245, the commutator subgroup of H is trivial. The group H being abelian, it follows, from the non-degeneracy of γ, that $\mathrm{wt}_H^G(3) \leq 1$ and, from Lemma 241, 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 84, 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 311. *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 310, the group H is cyclic. We define $T = H \oplus G_4$ so, by Lemma 309, 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 114, the elements of $\mathcal{C}$ are in bijection with the elements of $\mathrm{Hom}(H', G_4)$, which is naturally isomorphic to $\mathrm{Hom}(H'/\Phi(H'), G_4)$, because G_4 has order 3. The group H' is cyclic, so $\Phi(H') = (H')^3$ and, the group G being a κ-group, one gets $\Phi(H') = H' \cap G_2$. By Lemma 36, the quotient G/G_2 is elementary abelian and the restriction map $\mathrm{Hom}(G/G_2, G_4) \to \mathrm{Hom}(H'G_2/G_2, G_4)$ is thus surjective. Moreover, by Lemma 244, the subgroup G_4 coincides with $\mathrm{Z}(G)$ so, as a consequence of Lemma 190, 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 114 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 312. *Let H be a subgroup of G_3 such that $H \cap G_4 = \{1\}$. 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 282, and therefore so is $T = H \oplus G_4$. Let $g \in G$ be such that gTg^{-1} is A-stable, as in Lemma 309, 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, G_4 being characteristic, both H' and $\alpha(H')$ belong to $\mathcal{C}$. Thanks to Lemma 114, the elements of $\mathcal{C}$ are in bijection with the elements of $\mathrm{Hom}(H', G_4)$. By the isomorphism theorems, H' is isomorphic to $(H'G_4)/G_4$ and the restriction map induces a surjection $\mathrm{Hom}(G_3/G_4, G_4) \to \mathrm{Hom}(H', G_4)$. By Lemma 244, the subgroup G_4 coincides with $\mathrm{Z}(G)$ so, as a consequence of Lemma 190, 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 114 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. The groups H' and H being conjugate in G, it follows that H and $\alpha(H)$ are conjugate, too. ■

Lemma 313. *Let H be a subgroup of G such that $H \oplus G_4 = G_2$. 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 282, so the set X

is non-empty. Moreover, as a consequence of Lemma 114, 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 76, we can write $K = K^+ \oplus K^-$ and, as a consequence of Lemma 85, the subgroup K^- is equal to G_2^-. Again by Lemma 85, 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 308(1), the group G_2 normalizes K, but in fact $G_2 = \mathrm{N}_G(K)$, as a consequence of Lemma 190. It follows that the orbit of K in X has size $|G : G_2| = 9$ so, thanks to Lemma 308(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 314. *Let H be a subgroup of G such that $H \oplus G_3 = G_2$. 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 282, and so, from Lemma 114 it follows that 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 85, 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 we have that $|X^+| = 3$. Fix $K \in X^+$. Then, as a consequence of Lemma 241, 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 308(1), one has $\mathrm{N}_G(K) = G_2$. Lemma 308(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 315. *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 $D = \langle x, G_2 \rangle$. By Lemma 241, the element $[x, a]$ belongs to $G_3 \setminus G_4$ so, as a consequence of Lemmas 244 and 190, 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 282, and therefore, applying Lemma 18(2), one gets

$$\begin{aligned}[x,a]^{-1} &= [x^{-1}\gamma, a] \\ &= x^{-1}[\gamma, a]x[x^{-1}, a] \\ &= [x^{-1}, a] \\ &= x^{-1}axa^{-1} \\ &= x^{-1}[a,x]x \\ &= [x^{-1}, [a,x]][a,x] \\ &= [x^{-1}, [x,a]^{-1}][x,a]^{-1}.\end{aligned}$$

As a result, the element $[x^{-1}, [x,a]^{-1}]$ is trivial, and so $x \in C$. It follows that $C = D$, and thus $[x,a]$ belongs to $[C,C] \cap \mathrm{Z}(C)$. Lemma 245 yields $[x,a] \in G_4$. Contradiction. ∎

Lemma 316. *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.*

Proof. The group G_2 is elementary abelian, by Corollary 282, 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 76, the subgroup K decomposes as $K = K^+ \oplus K^-$ and, as a consequence of Lemma 85, there exists $a \in G_2^+$ such that $K = \langle a\rangle \oplus K^-$. Fix such a. Again thanks to Lemma 85, we get that $|X^+| = 12$. We want to count the conjugates of K. By Lemma 308(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 315 that $\mathrm{N}_G(K) = G_2$. As a consequence of Lemma 308(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 of the action of G/G_2 on X has a representative in X^+. The same holds for the orbit of H. ∎

Lemma 317. *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 309, 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 311. Assume that H is contained in G_2. If 2 is not a jump of H in G, then, by Lemma 312, the subgroups H and $\alpha(H)$ are conjugate in G. We suppose that 2 is a jump of H in G. By Corollary 282, 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

313, 314, and 316 guarantees that H has an A-stable conjugate in G. The choice of H being arbitrary, it follows from Lemma 93 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 125(1). ■

We remark that, thanks to Lemma 317, the proof of Proposition 307 is complete. Moreover, we are now also able to prove Theorem 231. The implication (2) $\Rightarrow$ (1) is clear and the implication (3) $\Rightarrow$ (2) is given by the combination of Proposition 307 and Lemma 247. We now prove (1) $\Rightarrow$ (2). To this end, let Q be a finite 3-group of class at least 4 with $\mathrm{int}(Q) > 1$. Because of Corollary 284, the class of Q is equal to 4 so, as a consequence of Theorem 164, the order of Q is equal to 729. The intensity of Q is equal to 2, thanks to Theorem 125(1). We have concluded the proof of (1) $\Rightarrow$ (2) and, to finish the proof of Theorem 231, we will next prove (2) $\Rightarrow$ (3). Let Q be a finite 3-group of class 4 and intensity 2. Then, by Lemma 239, the group Q is a κ-group and, as a consequence of Proposition 134, it possesses an automorphism of order 2 that induces the inversion map on Q/Q_2. By Theorem 164, the order of Q_4 is 3. Proposition 285 yields that Q is isomorphic to MC(3). The proof of Theorem 231 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 318. *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 164 and 189. ■

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 number 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.

Lemma 319. *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. *The class of G is at least 2.*

2. *One has $\mathrm{wt}_G(1) = 2$ and $\mathrm{wt}_G(2) = 1$.*

3. *The group G/G_3 is extraspecial of exponent p.*

Proof. The group G is non-abelian and thus $G_2 \neq G_3$. The index $|G : G_3|$ being equal to p^3, it follows from Lemma 31 that $\mathrm{wt}_G(1) = 2$ and $\mathrm{wt}_G(2) = 1$. We denote now $\overline{G} = G/G_3$ and use the bar notation for the subgroups of $\overline{G}$. Then $\overline{G_2}$ is contained in $\mathrm{Z}(\overline{G})$ and $\overline{G_2} = \mathrm{Z}(\overline{G})$, as a consequence of Lemma 27. The exponent of $\overline{G}$ is p, because G^p is contained in G_3. ■

Lemma 320. *Let $p > 3$ and let G be a p-obelisk. Then G is regular.*

Proof. This follows directly from Lemma 53. ■

Proposition 321. *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 321 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 321(1-2) was phrased in the following way: if G is a p-obelisk, then

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

Lemma 322. *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 $\mathrm{wt}_G(c) = 1$.*

Proof. For all $j \in \{1, \ldots, c-1\}$, denote $w_j = \mathrm{wt}_G(j)$. Thanks to Lemma 319, we have $w_1 = 2$ and $w_2 = 1$. As a consequence of Proposition 321, whenever $i < c-1$, the product $w_i w_{i+1}$ is equal to 2 and, for all indices $i, j \in \{1, \ldots, c-1\}$, one has $w_i = w_j$ if and only if i and j have the same parity. It follows from Proposition 321(1) that $\mathrm{wt}_G(c)$ can be 2 only if c is odd. ■

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

Lemma 323. *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 321, Blackburn also proves Lemma 323. 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].

Proposition 324. *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 319(3), the group G is extraspecial so $G_2 = \mathrm{Z}(G)$. Assume now that $c > 2$. The subgroup G_c is central, because G has class c, 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 321(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 322(1), there exists a positive integer k such that $c - 1 = 2k + 1$ so, from Lemma 323, we get $G_{c-1} = \rho^k(G)$ and $G_c = \rho^k(G_2)$. As a consequence of Proposition 321(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 by Lemma 24 and it factors as a surjective non-degenerate map $G/N \times G_{c-1}/\,\mathrm{Z}(G) \to G_c$. It follows from Lemma 2 that G/N is cyclic of order p so, by Lemma 28, one has $G_2 = [N, G]$. Lemma 54 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 325. *Let G be a group and let N be a normal subgroup of G. Let moreover H and K be subgroups of G such that $K \subseteq H$. Then one has $(H \cap N)K = (KN) \cap H$.*

Proof. Easy exercise. ■

Lemma 326. *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 $|H : H_2| \leq |G : G_2|$. Moreover, H being non-abelian, Lemma 31 yields $|H : H_2| \geq p^2$, and therefore, from Lemma 319(2), 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 319(2), 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 $|G_3 : M| = p$, as given by Lemma 35. Then $\overline{G} = G/M$ has class 3 and $\overline{N} \neq \{1\}$. But, by Lemma 140, the centre of $\overline{G}$ is equal to $\overline{G_3}$ so, $\overline{G_3}$ having order p, Lemma 29 yields $\overline{G_3} \subseteq \overline{N}$. In particular, G_3 is contained in MN. Thanks to Lemma 325, we get that $G_3 = (G_3 \cap N)M = M$, which gives a contradiction. It follows that $N \subseteq G_3$, as claimed, and thus we have $|H : H_3| = |G : G_3|$. It is moreover clear that $H^p = H_3$, and so we have proven that H is a p-obelisk. ∎

Lemma 327. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then the following hold.*

1. *If 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 H be a quotient of G and let i denote the class of H. Let moreover c denote the class of G and note that $i \leq c$. If $i = 0$ or $i = 1$, 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 326, it is a p-obelisk itself. To conclude, apply Proposition 324. For the proof of (2), we combine (1) with Lemma 30. ∎

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 denotes 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 328. *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 $k = 1$. As a consequence of Lemma 20, the group $[G_i, G_i]$ is contained in G_{2i} so, from Lemma 323, it follows 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 $G_{i+3} = \{1\}$. It follows from Lemma 20, that $(G_i)_p$ is contained in G_{ip}, and so, thanks to Corollary 48, 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 323. 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, the map 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). To prove (2) combine Proposition 321(3) with Lemma 23. ∎

Corollary 329. *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 of groups $\rho_i^m : G_i/G_{i+1} \to G_j/G_{j+1}$.

Proof. By Lemma 328(1), the map $\rho^m : G_i \to G_i$ induces a surjective homomorphism $\rho_i^m : G_i/G_{i+1} \to G_j/G_{j+1}$. Now, i and j having the same parity, it follows from Lemma 322 that $\mathrm{wt}_G(i) = \mathrm{wt}_G(j)$ and ρ_i^m is a bijection. ∎

Lemma 330. *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 328 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 322, 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 322(2). Assume without loss of generality that $h \leq k$. Then, by Lemma 323, 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 $\gamma_{h,k} \neq 1$, Lemma 20 yields that $G_{h+1} \subseteq C \subsetneq G_h$ and $G_{k+1} \subseteq D \subsetneq G_k$. 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, Lemma 2 yields that $|G_h : C| = |G_k : D|$. Now, by Lemma 320, the group G is regular, and therefore so is C. Thanks to Lemma 52(1), the set $\rho^{\frac{k-h}{2}}(C)$ is a subgroup of C and so, thanks to Lemma 54, 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 329 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. ■

Corollary 331. *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*

$$t\, G_{c-l+1} \quad \mapsto \quad (x\, G_{l+1} \mapsto [t, x])$$

is a surjective homomorphism of groups.

Proof. As a consequence of Lemma 323, 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 328 is thus a bilinear map of $\mathbb{F}_p$-vector spaces. Respecting the notation from Section 1.1, 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 ${}_v(\gamma_{c-l,l})$. 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 328(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 321 yields $w_{c-l} = w_l w_c$ and, if l is even, then $w_c = 2$. As a consequence of Lemma 330, 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. Then G is *framed* if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$.

Lemma 332. *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 $n \in \mathbb{Z}_{\geq 0}$. Then the following diagram is commutative.*

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

Proof. The maps from the above diagram are defined in Lemma 328. Assume without loss of generality that $G_{h+k+2n+1} = \{1\}$ so that G_{h+k+2n} is central. The diagram is clearly commutative for $n = 0$. We will prove the most delicate case, i.e. when $n = 1$, and leave the general case to the reader. Set $n = 1$. Let $(x, y) \in G_h \times G_k$. We will show, and that suffices, that $[x, y^p] = [x, y]^p$. Thanks to Lemma 18(4), one gets

$$[x, y]^{-p}[x, y^p] = \prod_{r=1}^{p-1} [[y^r, x], y].$$

Applying Lemma 20 twice, one gets that, for each index r, the element $[[y^r, x], y]$ belongs to G_{h+2k}, which is itself contained in the central subgroup G_{h+k+2}. Moreover, the group G_{h+k} being central modulo G_{h+k+1}, Lemma 22 yields $[y^r, x] \equiv [y, x]^r \bmod G_{h+k+1}$. Thanks to Lemma 23, the commutator map on G induces a bilinear map $G_{h+k}/G_{h+k+1} \times G_k/G_{k+1} \to G_{h+2k}$ and therefore we get $[[y^r, x], y] = [[y, x]^r, y] = [[y, x], y]^r$. It follows that

$$[x, y]^{-p}[x, y^p] = \prod_{r=1}^{p-1} [[y^r, x], y] = \prod_{r=1}^{p-1} [[y, x], y]^r = [[y, x], y]^{\binom{p}{2}}$$

and, the prime p being larger than 2, the number $\binom{p}{2}$ is a multiple of p. Since $[[y, x], y]$ belongs to G_{h+k+2}, it follows from Lemma 323 that $[x, y^p] = [x, y]^p$. This concludes the case $n = 1$. ■

Lemma 333. *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 $m \in \mathbb{Z}_{\geq 0}$. Then the following diagram is commutative.*

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

Proof. The maps in the diagram are as in Lemma 328 and they are well-defined. Assume without loss of generality that $G_{h+k+2m+1} = \{1\}$ and so G_{h+k+2m} is central. Let $(x, y) \in G_h \times G_k$. The diagram is clearly commutative if $m = 0$; we will prove commutativity when $m = 1$, the most difficult case, and we will leave the general case to the reader. Set $m = 1$. We will prove, and that suffices, that $[x^p, y] = [x, y]^p$. Applying Lemma 18(3) twice, we get

$$\begin{aligned}[x^p, y][x, y]^{-p} &= \prod_{s=1}^{p-1} [x, [x^{p-s}, y]] \\ &\prod_{s=1}^{p-1} \Big[x\,,\, \Big(\prod_{j=1}^{p-s-1} [x\,,\, [x^{p-s-j}, y]] \Big) [x, y]^{p-s} \Big].\end{aligned}$$

Thanks to Lemma 20, each element $[x, [x^{p-s-j}, y]]$ belongs to G_{k+2h} and, the group G_{h+k+3} being trivial, G_{k+2h} centralizes G_{h+k}. Again by Lemma 20, for each index s, the element $[x, y]^{p-s}$ belongs to G_{h+k} and applying Lemma 18(1) twice yields

$$\begin{aligned}[x^p, y][x, y]^{-p} &= \prod_{s=1}^{p-1} \Big[x\,,\, \prod_{j=1}^{p-s-1} [x, [x^{p-s-j}, y]]\Big] \prod_{s=1}^{p-1} [x, [x, y]^{p-s}] \\ &= \prod_{s=1}^{p-1} \Big[x\,,\, \prod_{j=1}^{p-s-1} [x, [x^{p-s-j}, y]]\Big] \prod_{s=1}^{p-1} [x, [x, y]]^{p-s}.\end{aligned}$$

Thanks to Lemma 23, given any two positive integers i and j, the commutator map induces a bilinear map $G_i/G_{i+1} \times G_j/G_{j+1} \to G_{i+j}/G_{i+j+1}$. By taking consecutively $(i, j) = (h, k)$ and $(i, j) = (h, h + k)$, we get respectively that $[x^{p-s-j}, y] \equiv [x, y]^{p-s-j} \bmod G_{h+k+1}$ and so

$$[x, [x^{p-s-j}, y]] \equiv [x, [x, y]^{p-s-j}] \equiv [x, [x, y]]^{p-s-j} \bmod G_{2h+k+1}.$$

By taking $(i, j) = (h, 2h + k)$, we derive that

$$\begin{aligned}[x^p, y][x, y]^{-p} &= \prod_{s=1}^{p-1} \Big[x\,,\, \prod_{j=1}^{p-s-1} [x, [x, y]]^{p-s-j}\Big] \prod_{s=1}^{p-1} [x, [x, y]]^{p-s} \\ &= \prod_{s=1}^{p-1} \Big[x, [x, [x, y]]^{\binom{p-s}{2}}\Big] \prod_{s=1}^{p-1} [x, [x, y]]^{p-s} \\ &= \prod_{s=1}^{p-1} [x, [x, [x, y]]]^{\binom{p-s}{2}} \prod_{s=1}^{p-1} [x, [x, y]]^{p-s} = [x, [x, [x, y]]]^{\binom{p}{3}} [x, [x, y]]^{\binom{p}{2}}.\end{aligned}$$

The prime p being larger than 3, both $\binom{p}{2}$ and $\binom{p}{3}$ are multiples of p. As both $[x, [x, y]]$ and $[x, [x, [x, y]]]$ belong to G_{h+k+1}, it follows from Lemma 323 that $[x^p, y] = [x, y]^p$. This concludes the proof for $m = 1$. ■

Proposition 334. *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.*

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

Proof. Combine Lemmas 332 and Lemma 333. ■

Lemma 335. *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 characteristic in the normal subgroup M; thus both M^p and $[M, M]$ are normal in G. By Lemma 319(2), the quotient G/G_2 has order p^2 and so $|G : M| = |M : G_2| = p$. It follows from Lemma 28 that $[M, M] = [M, G_2]$ and so, as a consequence of Corollary 329 and Lemma 330, 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 327(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 323, 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 336, it makes sense, for each positive integer i, to talk about subspaces of G_i/G_{i+1}.

Proposition 336. *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) $\Leftrightarrow$ (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 from Lemma 335 that $[M, G_2] = [M, M]$ and therefore (2) holds if and only if, given any maximal subgroup M of G, one has $\Phi(M)G_4 = G_3$. Lemma 327(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 328(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 328(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 334, 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. The importance of Section 10.4 will become clear in Chapter 13.

Proposition 337. *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, by definition of a p-obelisk, and it is in particular non-trivial. Let l denote the least jump of H in G. Then, as a consequence of Lemma 20, the subgroup $H_2 = [H, H]$ is contained in G_{2l}. Moreover, since H^p is equal to H_3, the subgroup H^p is contained in H_2. It follows from Corollary 329 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 319(2), the width $\mathrm{wt}_H^G(l)$ is equal to 1 and so Lemma 28 yields that $H_2 = [H, H \cap G_{l+1}]$. Thanks to Lemma 20, the subgroup 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 $\overline{G}$. By the isomorphism theorems, the groups $\overline{H}$ and $H/(H \cap G_4)$ are isomorphic and so, as a consequence of Lemma 326, 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 322 and 328(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 $G = HG_2$, from which we derive $G = H\Phi(G)$. Lemma 33 yields $H = G$. ■

Lemma 338. *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 328(1). ■

Lemma 339. *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 $J = \{l + 2k \ : \ k \in \mathbb{Z}_{\geq 0}, \ k \leq (c-l)/2\}$. Let x be an element of H such that $\mathrm{dpt}_G(x) = l$; the existence of x is guaranteed by Lemma 82. 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 329, 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 340. *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 428, the group $\overline{G}$ is abelian or it is a p-obelisk. If $\overline{G}$ is abelian, then $c = 2$ and so, by Lemma 339, 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 322, either $c-1$ is even or $\mathrm{wt}_{\overline{G}}(c-1) = 2$. It follows from Lemma 339 that $\overline{H}$ is cyclic and, the intersection $H \cap G_c$ being trivial, so is H. ∎

Lemma 341. *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 340, 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 322(3), the jump l is odd. The subgroup $[H, H]$ is contained in G_{2l}, thanks to Lemma 20, and therefore, $2l$ being even, Lemma 328(2) yields $2l > c$. In particular, one has $[H, H] = \{1\}$ so $\Phi(H) = H^p$. Moreover, as a consequence of Lemma 328(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 321 the width $\mathrm{wt}_H^G(l)$ is either 1 or 2 and the proof is thus complete. ∎

Lemma 342. *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, because G has class c, and so, by Lemma 114, all complements of G_c in $T = HG_c$ are of the form $\{f(h)h : h \in H\}$ as f varies in $\mathrm{Hom}(H, G_c)$. The subgroup G_c is elementary abelian, as a consequence of Lemma 323, and therefore $\mathrm{Hom}(H, G_c)$ is naturally isomorphic to $\mathrm{Hom}(H/\Phi(H), G_c) = \mathrm{Hom}(H/(H \cap G_{l+1}), G_c)$. By assumption, $c - l$ is odd so, thanks to Corollary 331, 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 323, 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. By the isomorphism theorems, HG_{l+1}/G_{l+1} and $H/(H \cap G_{l+1})$ are isomorphic and so every homomorphism $H \to G_c$ is of the form $x \mapsto [t, x]$, for some $t \in G_{c-l}$. For each complement K of G_c in T there exists thus $t \in G_{c-l}$ 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 343 and 344, which are proven in Section 11.4.

Theorem 343. *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 343 for higher nilpotency classes is proven in Chapter 12: the next theorem gives an essential contribution to its proof.

Theorem 344. *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 344. We will prove Theorem 344 by induction on the nilpotency class c of the group G and we will separate the cases according to the parity of c. Propositions 345, 358, and 369 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 from 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 358 and 369 we ask for the p-obelisk to be framed.

Proposition 345. *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 give the proof of Proposition 345 in Section 11.1.2, after some preparation.

11.1.1 Some lemmas

We will work under the hypotheses of Proposition 345 until the end of Section 11.1.1. The class c of G being even, Lemma 322(4) yields that G_c has order p. We denote moreover $A = \langle \alpha \rangle$ and we recall that a subgroup H of G is said to be A-stable if the action of A on G induces an action of A on H.

Lemma 346. *Let H be a subgroup of G containing G_c. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. The automorphism α_c is intense so, by Lemma 93, there exists $g \in G$ such that $(gHg^{-1})/G_c$ is $\langle \alpha_c \rangle$-stable. It follows from the definition of α_c that gHg^{-1} is A-stable. ■

Lemma 347. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. Then all jumps of H in G are odd.*

Proof. The subgroup H has trivial intersection with G_c and c is even. It follows from Corollary 329 that H cannot have even jumps in G. ■

Lemma 348. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. 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. We denote $\overline{G} = G/G_c$ and we use the bar notation for its subgroups. By Lemma 347, all jumps of H in G are odd and so all jumps of $\overline{T}$ in $\overline{G}$ are odd. The subgroup $\overline{T}$ is $\langle\alpha_c\rangle$-stable so, as a consequence of Lemma 85, each element of $\overline{T}$ is sent to its inverse by α_c. Every subgroup of $\overline{T}$ is thus $\langle\alpha_c\rangle$-stable and, in particular, so is $\overline{K}$. It follows from the definition of α_c that KG_c is A-stable. Moreover, every element of H is inverted, modulo G_c, by α and the restriction of α to G_c is the identity map, thanks to Lemma 62. ■

Lemma 349. *Let H be a non-trivial subgroup of G such that $H \cap G_c = \{1\}$. Let l denote 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, by Lemma 347, and H is abelian, by Lemma 341(1). The subgroup G_c being central, the group T is in fact equal to $H \oplus G_c$. Moreover, the subgroup G_c being characteristic, $T = \alpha(T) = \alpha(H) \oplus G_c$ and $\alpha(H)$ is a complement of G_c in T. By Lemma 341(2), the Frattini subgroup of H is equal to $H \cap G_{l+1}$ so it follows from Lemma 342 that there exists $t \in G_{c-l}$ such that $\alpha(H) = tHt^{-1}$. Thanks to Lemma 92, there exists $g \in G_{c-l}$ such that gHg^{-1} is A-stable. ■

Lemma 350. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. 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 $T = HG_c$. Thanks to Lemma 346, 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 349, there exists $b \in G$ such that $bH'b^{-1}$ is A-stable. To conclude, define $g = ba$. ■

Lemma 351. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. Then 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 351. We warn the reader that the following assumptions will be valid until the end of Section 11.1.1.

Let H be a subgroup of G such that $H \cap G_c = \{1\}$. Without loss of generality we assume that H is non-trivial and, in view of Lemma 350, that the jumps of H in G do not all have the same width. As a consequence of Proposition 321(1), each jump of H in G will have width 1 or 2. Let l and j denote respectively the least jump of width 1 and the least jump of width 2 of H in G. Write $T = HG_c$.

Lemma 352. *Let i and h be jumps of H. Assume that $\mathrm{wt}_H^G(i) = 1$ and that $\mathrm{wt}_H^G(h) = 2$. Then $i < h$.*

Proof. By Lemma 347, both i and h are odd so, the class c being even, Corollary 329 yields $i < h$. ■

Lemma 353. *The following hold.*

1. *One has $l < j$.*

2. *One has $j + l > c$.*

3. *The subgroup H is abelian.*

Proof. Part (1) follows directly from Lemma 352. We prove (2) and (3) together. As a consequence of Lemma 339, the group $H/(H \cap G_j)$ is cyclic and, thanks to Lemma 28, one gets $[H, H] = [H, H \cap G_j]$. The number $l + j$ being even, it follows from Lemma 347 that $l + j$ is not a jump of H in G. Lemma 330 yields $l + j > c$ and, as a result, $[H, H] \subseteq G_{c+1} = \{1\}$ so H is abelian. ■

Lemma 354. *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 subgroup H is abelian by Lemma 353(3) and, as a consequence of Lemma 352, the subgroup $H \cap G_j$ has only jumps of width 2. The smallest jump of H in G is l so, thanks to Lemma 82, 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 338, all jumps of L are odd and of width 1 in G. Now, l is smaller than j, by Lemma 353(1), and j is a jump of L in G as a consequence of Corollary 329. 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 329 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 by definition of j. Moreover, each jump $j \leq i < c$ of $J \oplus L$ is a jump of width 2 of H. Corollary 329 ensures that all odd integers $l \leq i < c$ are jumps of H in G, so Lemma 84 yields

$$|J \oplus L| = \prod_{i=l}^{c-1} p^{\dim_{J\oplus L}^{G}(i)} = \prod_{i=l}^{c-1} p^{\dim_{H}^{G}(i)} = |H|.$$

It follows that H and $J \oplus L$ coincide. ■

Lemma 355. *Let J and L be as in Lemma 354. 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 348, the group R is A-stable. The subgroup L is cyclic so, by Lemma 338, all its jumps in G are odd and of width 1. With L in the role of H, it follows from Lemma 349 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 is j and therefore $[g, J] = \{[g, x] : x \in J\}$ is contained in $[G_{c-l}, G_j]$. As a consequence of Lemma 20, the set $[g, L]$ is contained in G_{c-l+j}, which is itself contained in G_{c+1} thanks to Lemma 353(1). It follows that g centralizes J and $gJg^{-1} = J$. To conclude, we show that $gTg^{-1} = T$. The subgroup T is contained in G_l, so $[g, T]$ is contained in $[G_{c-l}, G_l]$. Again applying Lemma 20, we get that $[g, T]$ is contained in G_c. The subgroup G_c being contained in T, we are done by Lemma 13. ■

Lemma 356. *Let J and L be as in Lemma 354. 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 $L = \langle z \rangle$. As a consequence of Lemma 354, 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 $\alpha(\gamma) = \gamma$; the existence of γ is confirmed by Lemma 348. Define $m = (j + l - c)/2$, which is a positive integer thanks to Lemma 353(2). By Lemma 323, there exists a of depth $c - j$ in G such that $\rho^m(a) = z$. We fix a and remark that a belongs to $\mathrm{C}_G(L)$, because $[a, z] = [a, \rho^m(a)] = 1$ and z generates L. Now, x does not belong to L, but, as a consequence of Corollary 329, the jump j of J is also a jump of L in G. Since $\mathrm{wt}_G(j) = 2$, it follows from Lemma 330 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, because of Lemma 323, the exponent of G_c is p. We compute

$$\alpha(gxg^{-1}) = \alpha([g, x]x) = \alpha(\gamma^{\frac{p-1}{2}}x) = \alpha(\gamma^{\frac{p-1}{2}})\alpha(x) = \gamma^{\frac{p-1}{2}}x^{-1}\gamma =$$

$$\gamma^{\frac{p+1}{2}}x^{-1} = (\gamma^{\frac{p-1}{2}}x)^{-1} = ([g, x]x)^{-1} = (gxg^{-1})^{-1}$$

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 357. *Let J and L be as in Lemma 354. 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 355, 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 356 guarantees the existence of h. We define $g = ha$ and we claim that $g \in G_{c-j}$. The jump j is larger than the jump l, by Lemma 353(1), and therefore $G_{c-l} \subseteq G_{c-j}$. It follows that the product ah belongs to G_{c-l}. ■

To conclude the proof of Lemma 351, we construct $g \in G$ such that gHg^{-1} is A-stable. Let $b \in G$ be such that bTb^{-1} is A-stable and observe that such element b exists by Lemma 346. Lemma 357, with H replaced by bHb^{-1}, provides an element $a \in G$ such that $a(bHb^{-1})a^{-1}$ is A-stable. We define $g = ab$ and the proof of Lemma 351 is complete.

11.1.2 The induction step

Under the hypotheses of Proposition 345, we want to show that α is an intense automorphism of G. In view of this, let H be a subgroup of G. If H contains G_c, then H has an A-stable conjugate in G by Lemma 346. We assume that $H \cap G_c \neq G_c$. The class c being even, it follows from Lemma 322(4) that $|G_c| = p$ and so H intersects G_c trivially. By Lemma 351, there exists an element $g \in G$ such that gHg^{-1} is A-stable. The automorphism α is intense as a consequence of Lemma 93 and the fact that H was chosen arbitrarily. Proposition 345 is proven.

11.2 The odd case, part I

In Proposition 358 an additional assumption compared to Proposition 345 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 358. *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 proof of Proposition 358 is given in Section 11.2.2.

11.2.1 Some lemmas

The goal of this section is to give all ingredients for the proof of Proposition 358 so we will keep the following assumptions until the end of Section 11.2.1. 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 363.

Lemma 359. *Let H be a subgroup of G containing G_c. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. By assumption, the automorphism α_c is intense and, by Lemma 93, there exists $g \in G$ such that $(gHg^{-1})/G_c$ is $\langle\alpha_c\rangle$-stable. It follows from the definition of α_c that gHg^{-1} is A-stable. ∎

Lemma 360. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. Then all jumps of H in G have width* 1.

Proof. As a consequence of Proposition 321(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 322(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 328(1) that $H \cap G_c \neq \{1\}$. Contradiction. ∎

Lemma 361. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. 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 360, they also all have width 1. Let now l be the least jump of H in G. Then, by Lemma 340, the subgroup H is cyclic and, by Lemma 341, 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 342, there exists $t \in G$ such that $\alpha(H) = tHt^{-1}$. Thanks to Lemma 92, there exists thus $t \in G$ such that tHt^{-1} is A-stable. In general, by Lemma 359, there exists $a \in G$ such that aTa^{-1} is A-stable. There now exists $t \in G$ such that $t(aHa^{-1})t^{-1}$ is A-stable, so we conclude by defining $g = ta$. ∎

Lemma 362. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. 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 from the assumptions that all jumps of T in G are odd. By Lemma 359, there exists $g \in G$ such that gTg^{-1} is A-stable. By Lemma 83, the subgroups gTg^{-1} and T have the same jumps in G so, as a consequence of Lemma 85, we get that $gTg^{-1} = (gTg^{-1})^-$. In particular, $gHg^{-1} = (gHg^{-1})^-$ and gHg^{-1} is A-stable. ∎

Lemma 363. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. Assume moreover that G is framed. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

The remaining part of Section 11.2.1 will be entirely dedicated to the proof of Lemma 363. 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. Let moreover H be a subgroup of G that trivially intersects G_c. If all jumps of H in G have the same parity, then we are done by Lemmas 361 and 362. We assume that H has jumps of each parity and we define i and j respectively to be the least odd jump and the least even jump of H in G. Write $T = HG_c$. We recall that, the class of G being c, the subgroup G_c is central in G.

Lemma 364. *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 360, all jumps of H in G that are smaller than k have width 1 and so, by Lemma 339, the group $H/(H \cap G_k)$ is cyclic. From Lemma 28, we get $[H, H] = [H, H \cap G_k]$. By Lemma 20, the subgroup $[H, H]$ 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 $m \leq c$. 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 336(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 360 that m is a jump of H of width 1 in G so, from Lemma 322(1), we derive $m = c$. Contradiction to H trivially intersecting G_c. ■

Lemma 365. *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 364(2), the group $\overline{H}$ is abelian so, by Corollary 76, it decomposes as $\overline{H} = \overline{H}^+ \oplus \overline{H}^-$. It follows from Lemma 85 that $\overline{H}^+$ and $\overline{H}^-$ have respectively only even jumps and only odd jumps in $\overline{G}$. Moreover, thanks to Lemma 360, all jumps of $\overline{H}$, and thus of its subgroups, in $\overline{G}$ have width 1. Lemma 339 yields that both $\overline{H}^+$ and $\overline{H}^-$ are cyclic. ■

Lemma 366. *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 365, 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 62, so it follows from Lemma 77 that $R = R^-$. Moreover, by Corollary 76, 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, with G and N respectively replaced by T and H, Lemma 325 yields $JG_c = (H \cap S)G_c = S \cap (HG_c) = S$. 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. What is left to show is that indeed $H = I \oplus J$. The subgroup H is abelian by Lemma 364(2) and $I \cap J = \{1\}$, since $R \cap S = G_c$. The subgroup $I \oplus J$ is contained in H and

$$\overline{I \oplus J} = \overline{I} \oplus \overline{J} = \overline{R} \oplus \overline{S} = \overline{H}^+ \oplus \overline{H}^- = \overline{H},$$

so we derive $H = I \oplus J$. ∎

Lemma 367. *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 364 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 323. As a consequence of Proposition 336, 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

$$\rho^{\frac{j}{2}}(a) = \rho^{s+r}(a) = \rho^s(\rho^r(a)) = \rho^s(y) = y^{p^s}.$$

Now, the group G_c being central, Lemma 22 implies that the commutator map $G_{c-j} \times G_j \to G_c$ is bilinear so $[a, x]^B = [a^B, x]$. We define

$$n = Ap^s \quad \text{and} \quad d = a^B$$

and get $\gamma = y^n[d, x]$. To conclude, the element d belongs to $\mathrm{C}_G(y)$, because d and y belong to $\langle a \rangle$. ∎

Lemma 368. *Assume that $\alpha(T) = T$. Let I and J be as in Lemma 366. 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 one has $\mathrm{dpt}_G(y) = i$ and $\mathrm{dpt}_G(x) = j$. As a consequence of Lemma 366(3), there exists $\gamma \in G_c$ such that $\alpha(x) = x\gamma$. We fix γ and we want to construct g. Let $n \in \mathbb{Z}$ and $d \in \mathrm{C}_G(y) \cap G_{c-j}$ be such that $\gamma = y^n[d, x]$; the existence of n and d is given by Lemma 367. 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 62, the restriction of α to G_c coincides with the map $z \mapsto z^{-1}$. To conclude, the commutator map $G_{c-j} \times G_j \to G_c$ is bilinear by Lemma 22. 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 363. By Lemma 359 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 366 and H replaced by aHa^{-1}. By Lemma 368, 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

$$\alpha(gHg^{-1}) = \alpha(baHa^{-1}b^{-1}) = \alpha(bIb^{-1} \oplus bJb^{-1}) = \alpha(I \oplus bJb^{-1}) =$$

$$\alpha(I) \oplus \alpha(bJb^{-1}) = I \oplus \alpha(bJb^{-1}) \subseteq gHg^{-1}.$$

It follows that $\alpha(gHg^{-1}) = gHg^{-1}$ and gHg^{-1} is itself A-stable. The proof of Lemma 363 is now complete.

11.2.2 The induction step

In this paragraph we give the proof of Proposition 358 and we work thus under the assumptions of the very same proposition. Let H be a subgroup of G; we will show that H has an A-stable conjugate. If H contains G_c, then, by Lemma 359, there exists $g \in G$ such that gHg^{-1} is A-stable. Assume now that G_c is not contained in H, i.e. $H \cap G_c = \{1\}$. Thanks to Lemma 363, the subgroup H has an A-stable conjugate. In other words, by Lemma 93, the subgroups H and $\alpha(H)$ are conjugate in G. As the choice of H was arbitrary, α is intense and the proof of Proposition 358 is complete.

11.3 The odd case, part II

Proposition 369. *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.*

The proof of Proposition 369 is given in Section 11.3.2.

11.3.1 Some lemmas

The purpose of this section is laying the ground for the proof of Proposition 369. We will therefore, until the end of Section 11.3.1, work under the assumptions of Proposition 369. Denote $A = \langle \alpha \rangle$.

Lemma 370. *Let H be a subgroup of G containing G_c. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. We write $\overline{G} = G/G_c$ and we use the bar notation for the subgroups of $\overline{G}$. By hypothesis, the automorphism α_c is intense so, by Lemma 93, there exists $g \in G$ such that $\alpha_c(\overline{gHg^{-1}}) = \overline{gHg^{-1}}$. The map α_c being induced from α, it follows that $\alpha(gHg^{-1}) = gHg^{-1}$ and gHg^{-1} is A-stable. ■

Lemma 371. *Let H be a subgroup of G such that $H \cap G_c \neq \{1\}$. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. Let $N = H \cap G_c$. If $N = G_c$, then, by Lemma 370, there exists $g \in G$ such that gHg^{-1} is A-stable. We assume that $N \neq G_c$. The group N being non-trivial, it follows from Proposition 321(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 88(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 363, there exists $\bar{g} \in \overline{G}$ such that $\bar{g}\overline{H}\bar{g}^{-1}$ is A-stable, and so there exists $g \in G$ such that gHg^{-1} is A-stable. ■

Lemma 372. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. Then H has only even jumps.*

Proof. The index c is odd and $H \cap G_c = \{1\}$. It follows from Corollary 329 that H cannot have odd jumps. ■

Lemma 373. *Let H be a subgroup of G such 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. By Lemma 372, all jumps of H in G are even so, as a consequence of Lemma 322(2), all jumps of H have width 1. It follows from Lemma 341 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 85, 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 342, the subgroups H and T^+ are conjugate in G. In particular, H has an A-stable conjugate. ■

Lemma 374. *Let H be a subgroup of G such that $H \cap G_c = \{1\}$. Then there exists $g \in G$ such that gHg^{-1} is A-stable.*

Proof. Define $S = HG_c$. By Lemma 370, 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 373 (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 $g = ba$. ■

11.3.2 The last step

We give here the proof of Proposition 369 and we make thus all assumptions from Proposition 369 hold, until the end of Section 11.3.2. To show that α is intense, we will show that each subgroup of G has an A-stable conjugate. Let H be a subgroup of G. If H trivially intersects G_c, then, by Lemma 374, 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 371, 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 92, 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 369.

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 343

We work under the assumptions of Theorem 343. The implication (2) $\Rightarrow$ (1) follows from the combination of Propositions 318 and 134. We now prove (1) $\Rightarrow$ (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 142 that α_4 is intense and consequently, from Proposition 345, that α is intense too. The proof of Theorem 343 is complete.

11.4.2 The proof of Theorem 344

Under the hypotheses of Theorem 344, we will work by induction on the class c of G. As a consequence of Lemma 319(1-3), the group G has class at least 2 and G/G_3 is extraspecial of exponent p. If $c = 2$, then Lemma 121 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 345, the map α is intense. Suppose that c is odd. From Proposition 321(1) it follows that the cardinality of G_c is p or p^2. In the first case we apply Proposition 358, in the second Proposition 369. Theorem 344 is now proven.

Chapter 12

A characterization for high classes

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 result.

Theorem 375. *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 Lemma 322 with Theorem 375, 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 376. *Let $p > 3$ be a prime number and let G be a p-obelisk. Write $C = \mathrm{C}_G(G_4)$. Assume that $\mathrm{wt}_G(5) = 1$ and $\mathrm{int}(G) > 1$. Then one has $\Phi(C) = G_3$.*

The goal of Section 12.1 is proving Proposition 376, so all assumption that we will make throughout the text (right now and right after Lemma 380) 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 321(2), the class of G is equal to 5. Write $C = \mathrm{C}_G(G_4)$.

Lemma 377. *The subgroup C is maximal in G.*

Proof. The commutator map induces a bilinear map $G/G_2 \times G_4/G_5 \to G_5$ whose image generates G_5, thanks to Lemma 24, and whose left kernel is C/G_2. As a consequence of Lemma 323, all quotients G_i/G_{i+1} are $\mathbb{F}_p$-vector spaces and, by assumption, $\mathrm{wt}_G(5) = 1$. By Lemma 322(2), the dimension of G_4/G_5 is equal to 1 and so Lemma 2 yields $|G : C| = p$. In other words, C is a maximal subgroup of G. ■

Lemma 378. *One has $G_4 \subseteq C^p \subseteq G_3$ and $|G_3 : C^p| = |C^p : G_4| = p$.*

Proof. The subgroup C is maximal, by Lemma 377, and it is thus normal of index p in G. It follows that C^p is normal in G and, as a consequence of Corollary 329, the number 3 is a 1-dimensional jump of C^p in G. Lemma 327(2) yields $G_4 \subseteq C^p \subseteq G_3$ and thus, thanks to Lemma 322(2), we get $|G_3 : C^p| = |C^p : G_4| = p$. ■

Lemma 379. *The subgroup C^p centralizes G_2.*

Proof. Each p-obelisk is regular, by Lemma 320, so, as a consequence of Lemma 54, the subgroups $[C, G_2^p]$ and $[C^p, G_2]$ are the same. Now, G_2^p is equal to G_4, by Lemma 323, and $[C, G_4] = \{1\}$, by definition of C. It follows that C^p centralizes G_2. ■

Lemma 380. *The group C^p is contained in* $\mathrm{Z}(C)$.

Proof. The subgroup C^p is contained in G_3, by Lemma 378, and the commutator map $C \times C^p \to G_4$ is bilinear by Lemma 22. Such commutator map factors as $\gamma : C/G_2 \times C^p/G_4 \to G_4$, as a consequence of Lemma 379 and of the definition of C. Moreover, thanks to Corollary 329, 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 $A = \langle \alpha \rangle$. 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 $H^- = H \cap G^-$. We will prove Proposition 376 *by contradiction* and, to this end, we assume that $\Phi(C) \neq G_3$. 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 $y \in G_4 \setminus G_5$. Then A acts on X in a natural way. Let X^+ be the collection of fixed points of X under A.

Lemma 381. *The exponent of C divides p^2.*

Proof. By definition, the subgroup C^{p^2} is contained in $(C^p)^p$. By Lemma 335, we have $[C,C] = C^p$ so it follows from Lemma 54 that $(C^p)^p = [C,C]^p = [C,C^p]$. As a consequence of Lemma 380, the subgroup $[C,C^p]$ is trivial, and thus $(C^p)^p = \{1\}$. In particular, the exponent of C divides p^2. ■

Lemma 382. *Let x be an element of $C \setminus G_2$. Then x has order p^2.*

Proof. As a consequence of Corollary 329, the element x^p is non-trivial so the order of x is divisible by p^2. We conclude by Lemma 381. ■

Lemma 383. *Let $H \in X$. Then H is abelian and $H \cap G_5 = \{1\}$. Moreover, if $x, y \in H$ satisfy $\mathrm{dpt}_G(x) = 1$ and $\mathrm{dpt}_G(y) = 4$, then $H = \langle x \rangle \oplus \langle y \rangle$.*

Proof. Let $(x,y) \in (C \setminus G_2) \times (G_4 \setminus G_5)$ 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 169, 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 328(1) that 5 is a jump of H in G if and only if $x^{p^2} \neq 1$. Lemma 382 yields $H \cap G_5 = \{1\}$. ■

Lemma 384. *Let $H \in X$ and, for each $i \in \mathbb{Z}_{\geq 1}$, denote $u_i = \mathrm{wt}_H^G(i)$. Then $(u_1, u_2, u_3, u_4, u_5) = (1,0,1,1,0)$ and H has order p^3.*

Proof. For each $i \in \mathbb{Z}_{\geq 1}$, write $w_i = \mathrm{wt}_G(i)$. Thanks to Lemma 322, we have $(w_1, w_2, w_3, w_4, w_5) = (2,1,2,1,1)$. Let x, y be as in Lemma 383: 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 328(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 327. Then $N \cap H = \langle y \rangle$ and, the quotient $H/\langle y \rangle$ being cyclic, so is HN/N. Thanks to Lemma 338, 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 84. ■

Lemma 385. *The cardinality of X is p^4.*

Proof. Thanks to Lemma 383, 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 Lemma 384, 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 384 and 319, we get

$$|X| = \frac{n}{m} = \frac{(p^6 - p^5)(p^2 - p)}{(p^3 - p^2)(p-1)} = p^4.$$

■

Lemma 386. *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 383, and it is A-stable. By Corollary 76, it decomposes as $H = H^+ \oplus H^-$. In view of Lemmas 384 and 85(1), we have that $H^+ = G_4^+$ and that $H \cap G_4 = G_4^+$. It follows from Lemma 383 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 387. *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 386, 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 377, and therefore it is A-stable. By Lemma 382, each element of $C^- \setminus G_2$ has order p^2 and, as a consequence of Proposition 134, the set $C^- \setminus G_2$ is equal to $C^- \setminus G_3^-$. It follows from Lemma 85 that

$$|X^+| = \frac{|C^-| - |G_3^-|}{p^2 - p} = \frac{p^4 - p^3}{p^2 - p} = p^2.$$

■

Lemma 388. *For each subgroup L of C^-, the commutator map induces a bilinear map $L \times G_3 \to G_4^+$.*

Proof. The subgroup G_4 is central in C so, by Lemma 22, the commutator map $L \times G_3 \to G_4$ is bilinear. Since L is contained in $C = \mathrm{C}_G(G_4)$, the commutator map induces a bilinear map $L \times G_3/G_4 \to G_4$. Now, thanks to Proposition 134, the map α induces the inversion map on G_3/G_4 and so, thanks to Lemma 61, we get $[L, G_3] = [L, G_3]^+$. In particular, $[L, G_3]$ is contained in G_4^+ and the proof is complete. ■

Lemma 389. *Let $H \in X^+$. Then $G_3 \subseteq \mathrm{N}_G(H)$.*

Proof. By Lemma 386, the subgroup H is of the form $\langle x \rangle \oplus G_4^+$, for some element $x \in C^- \setminus G_2$. As a consequence of Lemma 20, the subgroup $[G_3, G_4^+]$ is trivial so, from Lemma 18(1), it follows that $[G_3, H] = [G_3, \langle x \rangle]$. Lemma 388 yields that $[G_3, \langle x \rangle]$ is contained in G_4^+, a subgroup of H, and so, by Lemma 13, one has $G_3 \subseteq \mathrm{N}_G(H)$. ■

We will now prove Proposition 376 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 389, the normalizer of H contains HG_3. It follows from Lemma 384 that $\{1, 3, 4, 5\}$ is contained in $\mathcal{J}$ and, thanks also to Lemma 319(2), that $|G : \mathrm{N}_G(H)| \leq |G : HG_3| = p^2$. Now, by Lemmas 385 and 387, the cardinalities of X and X^+ are respectively p^4 and p^2. It follows from Lemma 94 that

$$p^4 = |X| \leq \sum_{K \in X^+} |G : \mathrm{N}_G(K)| \leq |X^+||G : \mathrm{N}_G(H)| \leq p^2 p^2 = p^4,$$

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 94, no two elements of X^+ are conjugate in G. As a consequence of Lemma 81, the subgroup G^+ is contained in $\mathrm{N}_G(H) = HG_3$ and so, thanks to Lemma 85(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 375, the finite p-groups of "high class" and intensity greater than 1 all need to be framed obelisks. Theorem 390 is the last result we present that still allows some "structural freedom" to p-obelisks.

Theorem 390. *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, 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 Theorem 390 and we will thus work under the hypotheses of such theorem.

Assume first (1). As a consequence of Proposition 95 and Corollary 284, the prime p is larger than 3 and so, thanks to Proposition 318, the group G is a p-obelisk. Thanks to Theorem 125(1), there exists an intense automorphism α of order 2 of G, which induces the inversion map on G/G_2 by Proposition 134. Proposition 376 yields $\Phi(C) = G_3$.

Assume now that $p > 3$, that G is a p-obelisk, 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 322, we have $(w_1, w_2, w_3, w_4, w_5) = (2, 1, 2, 1, 1)$ and so, thanks to Proposition 321(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 320, the group G is regular and so, given any subgroup K of G, Lemma 52 yields that $\rho^k(K) = K^{p^k}$.

Lemma 391. *One has $\rho^2(C) = G_5$.*

Proof. The group $\Phi(C)$ is equal to $C^p[C, C]$ and $\Phi(C) = G_3$, by assumption. It follows from Lemma 328(1) that $\Phi(C)^p = G_5$. Now, the group C is maximal in G, by Lemma 377, and so, as a consequence of Lemma 319(2), the quotient C/G_2 is cyclic. Lemma 28 yields $[C, C] = [C, G_2]$. Now, by Lemma 54, one has $[C, G_2]^p = [C, G_2^p]$ and so, thanks to Lemma 323, one gets $[C, G_2]^p = [C, G_4] = \{1\}$. It follows that $\Phi(C)^p$ is equal to C^{p^2} and therefore $\rho^2(C) = G_5$. ■

Lemma 392. *Let $\alpha_5 : G/G_5 \to G/G_5$ denote the automorphism that is induced by α. Then α_5 is intense.*

Proof. Let $\overline{G}$ denote G/G_5 and use the bar notation for the subgroups of $\overline{G}$. The automorphism α_5 induces the inversion map on $\overline{G}/\overline{G_2}$, because α does so on G/G_2. Moreover, thanks to Lemma 326, the group $\overline{G}$ is a p-obelisk of class 4. We conclude by applying Theorem 343. ■

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 Lemma 392, the automorphism that α induces on G/G_5 is intense. If G_5 is contained in H, then, thanks to Lemma 359, 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 360, all jumps of H in G have dimension 1 and, if they all have the same parity, Lemmas 361 and 362 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.

Lemma 393. *One has $u_4 = 1$.*

Proof. The group G having class 5, we have $j \in \{2, 4\}$. It follows from Corollary 329 that $0 \neq u_4 \leq w_4$ and therefore $u_4 = 1$. ■

Lemma 394. *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 $i = 1$. As a consequence of Lemma 393, the subgroups G_4 and $(H \cap G_4)G_5$ are equal. The group G_5 being central, it follows from Lemma 18(1) that

$$G_5 = [G, G_4] = [G, (H \cap G_4)G_5] = [G, H \cap G_4].$$

Thanks to Lemma 20, the group $[G_2, G_4]$ is trivial ans so Lemma 18(2) yields

$$[HG_2, G_4] = [H, G_4] = [H, H \cap G_4] \subseteq H \cap G_5 = \{1\}.$$

In particular, H is contained in C and so, as a consequence of Lemma 328(1), we get $\rho^2(H) = \rho^2(C)$. It follows from Lemma 391 that H contains G_5. Contradiction to $H \cap G_5 = \{1\}$. ■

Let D be a maximal subgroup of G with the property that $(H \cap G_3)G_4 = D^pG_4$ and note that, thanks to Corollary 329, the subgroup D is uniquely determined by H. Since D^p is characteristic in the normal subgroup D, Lemma 327 yields $D^p = D^pG_4$ and therefore, from Corollary 329, one gets $|D^p : G_4| = p$.

Lemma 395. *One has $\rho^2(D) = \{1\}$.*

Proof. From the definition of D together with Lemma 328(1), it follows that $\rho^2(D) = \rho(D^p) = \rho(H \cap G_3)$. As a consequence of Lemma 323, the subgroup $\rho(H \cap G_3)$ is contained in $H \cap G_5 = \{1\}$ and thus $\rho^2(D) = \{1\}$. ■

Lemma 396. *One has $D \neq C$ and $[D, G_4] = G_5$.*

Proof. The subgroups D and C are both maximal in G and so, as a consequence of Lemmas 391 and 395, they are distinct. Moreover, the class of G being 5, the subgroup $[D, G_4]$ is non-trivial. Lemma 20 gives that $[D, G_4]$ is contained in G_5 and, since $w_5 = 1$, we get $[D, G_4] = G_5$. ■

Lemma 397. *One has $[G_2, D^p] = G_5$.*

Proof. The group G is regular, by Lemma 320, and therefore, by Lemma 54, the subgroups $[G_2, D^p]$ and $[G_2^p, D]$ are equal. By Lemma 323, we have $G_2^p = G_4$ and so, from Lemma 396, we derive $[G_2, D^p] = G_5$. ■

Lemma 398. *The subgroup H is abelian.*

Proof. As a consequence of Lemma 394, the subgroup H is contained in G_2 and, since $w_2 = 1$, the quotient $H/(H \cap G_3)$ is cyclic. It follows from Lemma 28 that $[H, H] = [H, H \cap G_3]$ and so, thanks to Lemma 20, one gets $[H, H] \subseteq H \cap G_5 = \{1\}$. In particular, H is abelian. ■

Lemma 399. *One has $(i, j) = (3, 4)$.*

Proof. By Lemma 394, 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 one has $u_2 = w_2 = 1$ and so $G_2 = HG_3$. By Lemma 397, the subgroups $[G_2, D^p]$ and G_5 coincide and so, the group G_5 being central, Lemma 22 ensures that the commutator map $G_2 \times D^p \to G_5$ is bilinear and differs from the trivial map. Now, the induced map $G_2/G_3 \times D^p/G_4 \to G_5$, derived from Lemma 20, is non-trivial and so $[H, H \cap G_3] \neq 1$. Contradiction to Lemma 398. ■

Lemma 400. *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 399, we have $(u_1, u_2, u_3, u_4, u_5) = (0, 0, 1, 1, 0)$. The subgroup H is thus contained in G_3 and so, by Lemma 323, one has $H^p \subseteq G_5 \cap H = \{1\}$. It follows from Lemma 398 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 82 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 395 and 398, 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 401. *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 402. *One has $\mathrm{N}_G(H) \cap D = \mathrm{N}_G(H) \cap G_2$.*

Proof. Assume by contradiction that $\mathrm{N}_G(H) \cap D \neq \mathrm{N}_G(H) \cap G_2$. As a consequence of Lemma 393, we have that $(H \cap G_4)G_5 = G_4$ and, the group G_5 being central, it follows from Lemma 18(1) that $[D, G_4] = [D, H \cap G_4]$. Lemma 13 yields $[D, G_4] \subseteq H$ and thus, by Lemma 396, the subgroup G_5 is contained in H. Contradiction. ■

Lemma 403. *One has $\mathrm{N}_G(H) \cap G_2 = G_3$.*

Proof. As a consequence of Lemma 399, the subgroup H is contained in G_3 and, thanks to Lemma 20, one has $[G_3, G_3] \subseteq G_6 = \{1\}$. In particular, G_3 normalizes H. Assume by contradiction that 2 is a jump of $\mathrm{N}_G(H)$ in G. Thanks to Lemma 20, the group G_2 centralizes G_4 and, by definition of D, we have $(H \cap G_3)G_4 = D^p$. It follows from Lemma 18(1) that $[G_2, D^p] = [G_2, H \cap G_3]$ and so, thanks to Lemma 13, the subgroup $[G_2, D^p]$ is contained in H. Lemma 397 yields $G_5 \subseteq H$. Contradiction. ∎

We claim that the action of G on X is transitive. As a consequence of Lemma 401, we have that $p^2 = |X| \geq |G : \mathrm{N}_G(H)|$ and therefore, applying Lemmas 402 and 403, we get

$$p^2 \geq |G : \mathrm{N}_G(H)| \geq |D : G_2||G_2 : G_3| = |D : G_3|.$$

As a consequence of Lemma 319(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 93 yields that α is intense and so $\mathrm{int}(G) > 1$. The proof of Theorem 390 is now complete.

12.3 Proving the main theorem

In this section we prove Proposition 404 and Theorem 375. 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 404. *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 318, the group G is a p-obelisk so, thanks to Proposition 321(1), the width $\mathrm{wt}_G(5)$ is either 1 or 2. The 4-th width of G is 1, thanks to Lemma 322(2), so, if $\mathrm{wt}_G(5) = 1$, then Proposition 321(2) 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 322, 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 330, 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 327 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 376 yields $\Phi(\overline{M}) = \overline{G_3}$. The subgroup $\Phi(M)$ being normal in G, it follows from Lemma 327 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 375. 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 344. Assume now (1). Since $\mathrm{wt}_G(5) \neq 1$, the class of G is at least 5. Moreover, thanks to Proposition 95 and Corollary 284, the prime p is larger than 3. Proposition 404 yields that G is a framed p-obelisk. As a consequence of Theorem 125, 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 134, induces the inversion map on G/G_2. The proof of Theorem 375 is complete.

Chapter 13

A generalization to 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 $S \rtimes C$, 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 405, 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 $\mathrm{k} = \mathrm{ij} = -\mathrm{ji}$. 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 405. *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 405.

Theorem 406. *Let $p > 3$ be a prime number. Then, for any positive integer c, there exists a finite p-group G 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 86 for pro-p-groups. In the subsequent sections we will pave the way to proving Theorem 405. 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 405 in Section 13.6.1 and give that of Theorem 406 in Section 13.6.2. We will close Chapter 13 with Section 13.6.3, where we will draw a bridge between Theorem 405 and Theorem 406.

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. A full list of the symbols we use can be found at the beginning of this thesis (see List of Symbols).

Definition 407. *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 408. *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 409. *Let G be a profinite group. The* lower central series $(G_i)_{i \geq 1}$ *of G is defined by*

$$G_1 = G \quad \textit{and} \quad G_{i+1} = \mathrm{cl}([G, G_i]).$$

In Section 1.2, we have defined the lower central series for any abstract group, which should not be confused with that of a profinite group. In the case of finite groups, they however coincide. 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 410. *Let G be a profinite group. The* rank *of G is*

$$\mathrm{rk}(G) = \sup\{\mathrm{rk}(G/N) : N \textit{ is normal open in } G\}.$$

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 410. In [DdSMS91, Proposition 3.11], a series of equivalent definitions of rank is given.

Definition 411. *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 412. *A profinite group is* just-infinite *if it is infinite and each of its proper quotients is finite.*

Definition 413. *Let p be a prime number and let G be a pro-p-group. The* Frattini subgroup *of G is $\Phi(G) = \mathrm{cl}(G^p[G, G])$.*

As for the case of finite p-groups, the Frattini subgroup $\Phi(G)$ of a pro-p-group G is the unique closed normal subgroup of G minimal with the property that $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$.

Lemma 414. *Let p be a prime number and let G be a pro-p-group. Then G is topologically finitely generated if and only if $\Phi(G)$ is open in G.*

Proof. This is Proposition 1.14 from [DdSMS91]. ∎

In Chapter 3 of [DdSMS91] it is proven that, if G is a finitely generated group, then the cardinality of a minimal set of topological generators of G is equal to $\dim_{\mathbb{F}_p}(G/\Phi(G))$.

Definition 415. *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 416. *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* $\dim(U)$.

Lemma 417. *Let p be an odd prime number and let G be a pro-p-group of finite rank. Then G has a characteristic open uniform subgroup.*

Proof. See Corollary 4.3 from [DdSMS91]. ■

Lemma 418. *Let p be an odd prime number and let G be a pro-p-group. Then all open uniform subgroups of G have the same dimension.*

Proof. See [DdSMS91, Corollary 4.6]. ■

Definition 419. *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.*

Lemmas 417 and 418 guarantee the consistency of Definition 419.

13.2 Properties and intensity

In Section 13.2 we give several properties of topologically intense automorphisms and, for a given prime number p, we define the intensity of a pro-p-group.

Lemma 420. *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.*

Proof. Let N be an open normal subgroup of G. Then $\alpha(N) = N$ and α induces an automorphism $\overline{\alpha}$ of G/N. Now each subgroup $\overline{H}$ of G/N corresponds to an open subgroup H of G, which is sent to a conjugate by α. As a consequence, also $\overline{\alpha}(\overline{H})$ and $\overline{H}$ are conjugate in G/N and, the choice of $\overline{H}$ being arbitrary, it follows that $\overline{\alpha}$ is intense. ■

If G is a profinite group and Υ denotes the set of open normal subgroups of G, then $\mathrm{Aut}(G)$ has a natural topology, the "congruence topology", for which a basis of open neighbourhoods of the identity is given by

$$\{\Gamma(N) = \{\alpha \in \mathrm{Aut}(G) : \alpha \equiv \mathrm{id} \bmod N\}\}_{N\in\Upsilon}.$$

For more information on the subject see for example [DdSMS91, Ch. 5.2].

Lemma 421. *Let G be a profinite group and let Υ denote the collection of open normal subgroups of G. Then one has*

$$\mathrm{Int}_{\mathrm{c}}(G) = \varprojlim_{N\in\Upsilon} \mathrm{Int}(G/N).$$

Proof. Let Υ denote the collection of open normal subgroups of G. Then, thanks to Lemma 420, we have a natural homomorphism

$$\pi : \mathrm{Int}_{\mathrm{c}}(G) \to \prod_{N\in\Upsilon} \mathrm{Int}(G/N).$$

The map π is injective, because $\ker\pi$ is contained in $\cap_{N\in\Upsilon}\Gamma(N) = \{1\}$, and the image of π is equal to $\varprojlim_{N\in\Upsilon} \mathrm{Int}(G/N)$, thanks to Lemma 88(2). ∎

Lemma 422. *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 423. *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 420, 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 422, the set $X = \varprojlim X_{\overline{G}}$ is non-empty. Let $x \in X$. As a consequence of the definition of X, 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

$$\alpha(H) = \mathrm{cl}(\alpha(H)) = \bigcap_{N\in\Upsilon} \alpha(H)N = \bigcap_{N\in\Upsilon} \alpha(HN) =$$

$$= \bigcap_{N\in\Upsilon} xHx^{-1}N = \mathrm{cl}(xHx^{-1}) = xHx^{-1}.$$

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 424. *Let p be a prime number and let G be a pro-p-group. Then*

$$\mathrm{Int_c}(G) = S \rtimes C,$$

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 88(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 Lemma 421 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 101, 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 89 yields that C is isomorphic to a subgroup of $\mathbb{F}_p^*$. Moreover, thanks to Lemma 97, 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 $\mathrm{Int}_{\mathrm{c}}(G) = S \rtimes C$. 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 101. ■

Let p be a prime number and let G be a pro-p-group. Let moreover C be as in Proposition 424. The *intensity* $\mathrm{int}(G)$ of G is defined to be the cardinality of C. Thanks to Proposition 424, the intensity of G is also equal to the greatest common divisor of the set $\{\mathrm{int}(G/N) : N \text{ normal open in } G,\ N \neq G\}$.

Corollary 425. *Let p be a prime number and let G be an abelian pro-p-group. If G is non-trivial, then* $\mathrm{int}(G) = p - 1$.

Proof. If G is non-trivial, then Theorem 86 yields $\mathrm{int}(G) = p - 1$. ■

13.3 Non-abelian groups, part I

The main purpose of Section 13.3 is to give a proof of Proposition 426. We refer to Section 13.1 for the definitions of just-infinite profinite groups and of p-adic analytic groups and their dimensions.

Proposition 426. *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 Propositions 424 and 133.

Lemma 427. *The automorphism α induces an intense automorphism of order* 2 *on each non-trivial discrete quotient of G.*

Proof. Let C be as in proposition 424 and, without loss of generality, assume that $\alpha \in C$. Then, as a consequence of Lemma 420, given any open normal subgroups N and M of G such that $N \subseteq M \neq G$, we get a commutative diagram

$$\begin{tikzcd}
C \arrow[r] \arrow[d] & \mathrm{Int}(G/M) \\
\mathrm{Int}(G/N) \arrow[ur] &
\end{tikzcd} .$$

Moreover, the map α being non-trivial, there exists a discrete quotient of G on which α induces an automorphism of order 2. The choice of M and N being arbitrary, it follows that α induces an intense automorphism of order 2 on each non-trivial discrete quotient of G. ■

Lemma 428. *Assume that $p > 3$. Then each discrete quotient of G of class at least 4 is a p-obelisk.*

Proof. Let $\overline{G}$ be a discrete quotient of class at least 4 of G. By Lemma 427, the map α induces an intense automorphism of order 2 of $\overline{G}$. It follows from Proposition 318 that $\overline{G}$ is a p-obelisk. ■

Lemma 429. *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 165 that $C < 3$ and so $C = 2$. Let now $M, N \in \Upsilon$ be such that G/N has class 2 and $M \subsetneq N$. Let $K = G/M$ and let $\pi : G \to K$ denote the canonical projection. Then K has class 2 and, as a consequence of Lemma 427, the intensity of K is greater than 1. By Theorem 105, the group K is extraspecial and, $\pi(N)$ being non-trivial and normal in K, it follows from Lemma 29 that $\pi(N)$ contains $\mathrm{Z}(K) = [K, K]$. In particular, $K/\pi(N)$ is abelian and therefore so is G/N. Contradiction. ■

Lemma 430. *The set $\{G_i\}_{i \geq 1}$ is a base of open neighbourhoods of* 1 *in G.*

Proof. Let moreover Υ denote the collection of all open normal subgroups N of P with the property that G/N has class at least 3. As a consequence of Lemma 429, the group G is equal to $\varprojlim_{N \in \Upsilon} G/N$. Moreover, each subgroup G_i being closed, we also have $G_i = \varprojlim_{N \in \Upsilon} (G/N)_i$. Thanks to Lemma 427, whenever $N \in \Upsilon$, the quotient G/N has intensity greater than 1 and so Theorem 218 yields that $\{G_i\}_{i \geq 1}$ is a base of open neighbourhoods of 1 in G. ■

Lemma 431. *Assume that $p > 3$. Then* $\mathrm{rk}(G) = 3$ *and G is p-adic analytic.*

Proof. By Lemma 427, the automorphism α induces an intense automorphism of order 2 on each non-trivial discrete quotient of G and, as a consequence of Lemma 429, the group G has finite quotients of any possible class. It follows that $\mathrm{rk}(G) = \sup\{\mathrm{rk}(G/N) : G/N \text{ has class at least } 4\}$ and hence Proposition 222 yields $\mathrm{rk}(G) = 3$. The group G being a pro-p-group of finite rank, it is p-adic analytic. ■

Lemma 432. *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 430, 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 of $\pi_k(N)$ in G/G_k is l. Now, by Lemma 428, whenever $k \geq 5$, the quotient G/G_k is a p-obelisk. It follows from Lemma 327(2) that, whenever $k > \max\{l, 5\}$, the subgroup 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). To conclude, since each G_k is open in G, the subgroup N is open and the quotient G/N is finite. Because of the arbitrary choice of N, the group G is just-infinite. ■

Lemma 433. *Assume that $p > 3$. Then G is torsion-free.*

Proof. By Lemma 428, whenever k is at least 5, the quotient G/G_k is a p-obelisk. It follows from Corollary 329 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 429, there is no bound on the class of the finite quotients of G, and therefore G is torsion-free. ■

Lemma 434. *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 429. As a consequence of Lemma 428, the group $\overline{G}$ is a p-obelisk and so Lemma 322 yields $|\overline{G}_2 : \overline{G}_4| = p^3$. The subgroup $\overline{G}_2^p$ is equal to $\overline{G}_4$, thanks to Lemma 323, and so, as a consequence of Lemma 20, the quotient $\overline{G}_2/\overline{G}_2^p = \overline{G}_2/\overline{G}_4$ 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 431, 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 433, 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 430. ∎

We conclude Section 13.3 by giving the proof of Proposition 426. Assume that $p > 3$. Then G is p-adic analytic, by Lemma 431, and it has dimension 3 thanks to Lemma 434. Moreover, G is just-infinite by Lemma 432. The proof of Proposition 426 is now complete.

13.4 Two infinite groups

In Section 13.4 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 405.

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 $\mathfrak{M}_{0,1,1}$.

Lemma 435. *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 436. *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 $\mathfrak{B}_0 = \mathrm{cl}(\langle x \rangle)$. ■

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 437. *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 435. Let now $x \in G$ be as in Lemma 436 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 328. As a consequence of Lemma 436, 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 322(1), the width $\mathrm{wt}_{\overline{G}}(3)$ is equal to 2 so ℓ' is different from $\overline{G}_3/\overline{G}_4$. Proposition 336 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

$$\mathfrak{m}^{2s} = p^s\Delta_p \ \text{ and } \ \mathfrak{m}^{2s+1} = p^s\mathfrak{m}.$$

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 438. *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}. As a consequence of Lemma 22, 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 $M_{i+1} = \mathrm{cl}([G, G_i]) = G_{i+1}$. The choice of i being arbitrary, the proof is complete. ∎

Lemma 439. *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 438, 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 440. *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 441. *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 438, one can easily compute that $|\overline{G} : \overline{G}_3| = |G : G_3| = p^3$ and, thanks to Lemma 439, 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 440 and Proposition 336. ■

Lemma 442. *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 438, 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 443. *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 442, 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 430, 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 442 and the definition of α_K. Moreover, the class of $\overline{G}$ is at least 3 so, thanks to Lemma 441, the group $\overline{G}$ is a framed obelisk. It follows from Theorem 344 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 423 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 424 and Theorem 125. ■

13.5 Non-abelian groups, part II

The aim of this section is to give a proof of the following proposition.

Proposition 444. *Let $p > 3$ be a prime number and let P be a non-abelian infinite pro-p-group. Assume that* $\mathrm{int}(P) > 1$*. Then P 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 P be an infinite non-abelian pro-p-group of intensity greater than 1. Let $(P_i)_{i\geq 1}$ denote the lower central series of P, as defined in Section 13.1, and let α be a topologically intense automorphism of P of order 2, which exists thanks to Proposition 424. In the proof of Proposition 444, we will make heavy use of results coming from Chapters 10 and 11.

Definition 445. *Let G be a group. The* derived series $(G^{(i)})_{i\geq 0}$ *of G is defined recursively by*

$$G^{(0)} = G \quad \textit{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

The group G is solvable *if there exists $k \in \mathbb{Z}_{\geq 0}$ such that $G^{(k)} = \{1\}$.*

Lemma 446. *Every solvable just-infinite pro-p-group other than $\mathbb{Z}_p$ has torsion.*

Proof. This is Proposition 6.1 in [GSK09]. ■

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.

Lemma 447. *Let $p > 3$ be a prime number and let G be a p-adic analytic group. Assume that $\dim(G) = 3$ and that G is both torsion-free and non-solvable. Then G 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 448. *The group P is topologically isomorphic to an open subgroup of $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.*

Proof. The group P is a just-infinite p-adic analytic group of dimension 3, by Proposition 426. By Lemma 433, the torsion of P is trivial and so, by Lemma 446, the group P is not solvable. It follows from Lemma 447 that P is isomorphic to an open subgroup of $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. ■

Lemma 449. *The group P is topologically isomorphic to $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.*

Proof. Let $G \in \{\mathrm{S}(\Delta_p), \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)\}$ and let $(G_i)_{i\geq 1}$ denote the lower central series of G. From the combination of Lemmas 435 and 441, we know that, for each $k \geq 3$, the quotient G/G_k is a p-obelisk. Let now H be an open subgroup of G, such that P is topologically isomorphic to H. The existence of H is ensured by Lemma 448. By Lemma 429, the group H has discrete quotients of any class and, thanks to Lemma 428, each such quotient, of class at least 4, is a p-obelisk. The subgroup H being open, it follows from Lemma 430 that there exists $k \in \mathbb{Z}_{>4}$ such that G_k is contained in H so H/G_k is a p-obelisk. Proposition 337 yields $G = H$. ■

Lemma 450. *Each discrete quotient of P of class at least 6 is a framed p-obelisk.*

Proof. Let $\overline{G}$ be a discrete quotient of P of class at least 6. By Lemma 427, the map α induces an intense automorphism of order 2 on $\overline{G}$ and, by Lemma 428, the group $\overline{G}$ is a p-obelisk. By Lemma 322(1), the number $\mathrm{wt}_{\overline{G}}(5)$ is equal to 2 so, by Theorem 375, the p-obelisk $\overline{G}$ is framed. ■

We are finally ready to give the proof of Proposition 444. Thanks to Lemma 449, there are only two possibilities for the isomorphism type of P: that of $\mathrm{S}(\Delta_p)$ or that of $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. By Lemma 450, every discrete quotient of P of class 6 is a framed p-obelisk so, in view of Lemma 437, the group $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ is not isomorphic to P. It follows that P is topologically isomorphic to $\mathrm{S}(\Delta_p)$ and so the proof of Proposition 444 is complete.

13.6 Proving the main theorems and more

In Sections 13.6.1 and 13.6.2 we prove respectively Theorem 405 and Theorem 406. 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 451, which is proven in Section 13.6.3.

13.6.1 The proof of Theorem 405

Let p be a prime number. As a consequence of Proposition 424, 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 425, 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 429, so Theorem 231 yields that p is larger than 3. By Proposition 444, the group G is topologically isomorphic to $\mathrm{S}(\Delta_p)$, which, by Lemma 443, has indeed intensity 2. The proof of Theorem 405 is now complete.

13.6.2 The proof of Theorem 406

Let $p > 3$ be a prime number and let c be a positive integer. Write $P = \mathrm{S}(\Delta_p)$ and let $(P_i)_{i\geq 1}$ denote the lower central series of P, as defined in Section 13.1. Then the group P/P_{c+1} has class c and it is finite, as a consequence of Lemma 430. The group P being a pro-p-group, P/P_{c+1} is a finite p-group. Moreover, by Theorem 405, the intensity of P is greater than 1 and so, thanks to Proposition 424, we get $\mathrm{int}(P/P_{c+1}) > 1$. The number c was chosen arbitrarily and therefore Theorem 406 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 451. *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 406, and it follows directly from the definition of f that (2) is satisfied. Moreover, thanks to Lemma 101, 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 101, 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 124, the constant C is at least 3 and so, for each $c > C$, Theorem 218 yields that X_c is finite. By Lemma 422, 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 405. It follows that (2) is satisfied and the proof is complete. ■

Proposition 451 is the last result of this thesis and, in summary, it 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 451, 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 375, 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*, 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

Summary

Intense automorphisms of finite groups

Let G be a group. An automorphism α of G is *intense* if, for every subgroup H of G, there exists an element x of G such that $\alpha(H) = xHx^{-1}$. The collection of intense automorphisms of G is a subgroup of $\mathrm{Aut}(G)$, which is denoted by $\mathrm{Int}(G)$.

In this thesis we classify the pairs (p, G), where p is a prime number and G is a finite p-group but $\mathrm{Int}(G)$ is not. To this end, for each finite p-group G, we define the *intensity* $\mathrm{int}(G)$ of G to be the index of any Sylow p-subgroup of $\mathrm{Int}(G)$ in $\mathrm{Int}(G)$. We prove that finite 2-groups have intensity 1. Next, we prove that, for every prime number p, each non-trivial finite abelian p-group has intensity $p-1$. We proceed with the classification by progressively increasing the nilpotency class of the groups we are looking at. Let p be an odd prime number. We show that the finite p-groups of class 2 and intensity greater than 1 are exactly the *extraspecial* p-groups of exponent p. We prove moreover that, if the class is 3, then a finite p-group has intensity greater than 1 if and only if its abelianization has order p^2. The classification process becomes more difficult as the class increases. We prove that there exists a unique 3-group, up to isomorphism, of class at least 4 and intensity greater than 1; that group has order 729. In contrast with the case of 3-groups, we demonstrate that, if $p > 3$, there exists, for each positive integer c, a p-group G of class c for which $\mathrm{Int}(G)$ is not itself a p-group. To do so, we extend the notion of intensity to pro-p-groups and, if $p > 3$, we construct an infinite non-abelian pro-p-group of intensity greater than 1. We later prove that the infinite group we constructed is the unique infinite non-abelian pro-p-group of intensity greater than 1, up to isomorphism. In conclusion, for each prime number $p > 3$, we define a new family of 2-generated finite p-groups, which we call *p-obelisks*, and we show that they have exceptionally pleasant properties. The classification of finite p-groups of intensity greater than 1 is completed, modulo the existence of a special kind of automorphisms of p-obelisks.

Samenvatting

Intense automorfismen van eindige groepen

Zij G een groep. Een automorfisme α van G heet *intens* als er voor elke ondergroep H van G een element x in G bestaat waarvoor geldt $\alpha(H) = xHx^{-1}$. De verzameling $\mathrm{Int}(G)$ van alle intense automorfismen van G is een ondergroep van $\mathrm{Aut}(G)$.

In dit proefschrift classificeren we de paren (p, G), met p een priemgetal en G een eindige p-groep waarvoor $\mathrm{Int}(G)$ geen p-groep is. Daartoe definiëren we voor elke p-groep G de *intensiteit* $\mathrm{int}(G)$ van G als de index van een willekeurige Sylow p-ondergroep van $\mathrm{Int}(G)$ in $\mathrm{Int}(G)$. We bewijzen dat eindige 2-groepen intensiteit 1 hebben. Vervolgens bewijzen we dat, als p een priemgetal is, elke eindige non-triviale abelse p-groep intensiteit $p-1$ heeft. We vervolgen de classificatie door de nilpotentie klasse van de groepen die we bekijken te laten oplopen. Zij p een oneven priemgetal. We laten zien dat de p-groepen van klasse 2 en intensiteit groter dan 1 precies de *extraspeciale* p-groepen met exponent p zijn. We bewijzen bovendien dat, als de klasse 3 is, een eindige p-groep intensiteit groter dan 1 heeft dan en slechts dan als zijn verabelisering orde p^2 heeft. De classificatie wordt moeilijker naarmate de klasse groeit. We bewijzen dat er op isomorfie na een unieke 3-groep van klasse groter dan 4 en intensiteit groter dan 1 bestaat; deze groep heeft orde 729. In tegenstelling tot het geval van 3-groepen tonen we aan dat er, voor $p > 3$ en c een positief getal, een p-groep G van klasse c bestaat waarvoor $\mathrm{Int}(G)$ geen p-groep is. Hiertoe breiden we het begrip intensiteit uit naar pro-p-groepen en voor $p > 3$ construeren we een oneindige niet-abelse pro-p-groep van intensiteit groter dan 1. Later bewijzen we dat de oneindige groep die we hebben geconstrueerd op isomorfie na de unieke oneindige non-abelse pro-p-groep van intensiteit groter dan 1 is. Ten slotte definiëren we voor elk priemgetal $p > 3$ een nieuwe familie van 2-voortgebrachte eindige p-groepen, die we *p-obelisken* noemen, en we laten zien dat ze bijzonder aangename eigenschappen hebben. De classificatie van eindige p-groepen van intensiteit groter dan 1 is voltooid, op het bestaan van een speciaal soort automorfismen van p-obelisken na.

Acknowledgements

I would like to thank:

my supervisor, Hendrik Lenstra, for his guidance and constant help. I am grateful for the beautiful mathematics we have done together and for everything he has taught me in the last years.

the members of the Doctorate Committee, for the time they spent reading my thesis.

Andrea Lucchini, for his help through the years, both mathematical and otherwise.

Ellen Henke, for her accurate comments.

Bart de Smit, for helping me with numerous issues; so many that I lost count.

Jon Gonzàlez Sànchez, for sharing his knowledge and precious ideas.

Martin Bright, for helping me with elliptic curves and teaching issues.

Carlo Pagano, for all the maths we discussed together.

the algebra, geometry, and number theory group in Leiden; and all its evolutions over the last five years. I couldn't have asked for a better environment to grown in, as a mathematician and as a person. A big thanks to Ronald.

my friends in Leiden, back home, and all around the globe, for their support and for all the fun times that coloured my PhD adventure.

my family.

Curriculum Vitae

Mima Stanojkovski was born on August 21, 1989, in Sarajevo (YU). In 1992, her family moved to Fiera di Primiero (TN), Italy, where she entered elementary school. After the primary studies, she moved, together with her family, to Feltre (BL), Italy. There, she completed her pre-university education. From 2000 to 2003, she studied at Scuola Media G. Rocca and, from 2003 to 2008, she was a student at Liceo Scientifico G. Dal Piaz.

After finishing high school, Mima started her bachelor studies in mathematics at Università degli Studi di Trento, Italy. She graduated in 2011, and wrote a thesis titled *"Controesempi sui compatti"*, supervised by Prof. Giuseppe Vigna Suria. In 2011, she joined the ALGANT Master program. She spent, between 2011 and 2013, one year at Università degli Studi di Padova and one year at Universiteit Leiden. She obtained her master's degree, from both Padova and Leiden, in 2013. Her master thesis, entitled *"Evolving groups"*, was supervised by Prof. Hendrik Lenstra from Universiteit Leiden.

In 2013 she started her PhD at Universiteit Leiden, under the supervision of Prof. Hendrik Lenstra. In relation to the PhD project, in 2014, she visited both Dr. Jon González Sánchez and Prof. Andrea Lucchini, respectively in Bilbao and Padova. Mima expects to spend the next two academic years at Universität Bielefeld, under the mentorship of Prof. Christopher Voll.