eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

PhD Thesis

Some topics on finite p-groups and pro-p groups

Iker de las Heras Kerejeta

Supervisor:
Gustavo Adolfo Fernández Alcober

Leioa, September 2020

This PhD thesis has been carried out at the University of the Basque Country. The author is supported by the Spanish Government grant MTM2017-86802-P and by the Basque Government grant IT974-16. He is also supported by a predoctoral grant of the University of the Basque Country.

Abstract

This thesis consists of three parts, each of them devoted to different aspects of the theory of finite p-groups and pro-p groups.

The first part is concerned with the study of the following problem: under which conditions on a group G does the verbal subgroup for a given word w coincide with the set of w-values? We will analyse this problem for different words lying in the derived subgroup of the free group, namely, the commutator word, the lower central words and general outer commutator words, under the hypothesis that G is a finite p-group.

The second part is aimed to the study of the Hausdorff dimension function. In recent decades, this fractal dimension has provided interesting and fruitful applications in the context of profinite groups, all of them based on the pioneering formula by Barnea and Shalev, according to which the Hausdorff dimension of a closed subgroup H of a profinite group G can be regarded as the "logarithmic density" of H in G. Thus, we will focus on the notion of normal Hausdorff spectrum of G with respect to a given filtration series, giving the first example of a finitely generated pro-p group with full normal Hausdorff spectra.

Finally, in the third part of the thesis, we will introduce two new classes of powerful p-groups: the powerfully solvable groups and the powerfully simple groups. These are powerful p-groups that somehow fulfil the "role" that finite solvable groups and finite simple groups have in the class of all finite groups, respectively. We will provide some results and classification concerning these groups, including a Jordan-Hölder type theorem. For this purpose, a bijective correspondence between the category of certain powerful groups and the category of alternating algebras over $\mathbb{F}_p$ will be of particular interest.

Laburpena

Tesi hau hiru zatitan banatuta dago, horietako bakoitzak p-talde finituen eta pro-p taldeen teoriaren hainbat alderdi lantzen dituelarik.

Lehenengo zatian, ondorengo problema aztertzen da: izan bitez G taldea eta w hitza; zein baldintzatan dator bat G-ren w-rekiko hitzezko azpitaldea w-balioen multzoarekin? Problema hori talde askearen azpitalde deribatuko zenbait hitzentzat aztertuko da, kommutadore hitzarentzat, hitz zentral beherakorrentzat eta kanpo kommutadore orokorrentzat alegia, hipotesi gehigarri batekin: G p-talde finitu bat izatea.

Bigarren zatian, Hausdorffen dimentsio funtzioa aztertzen da. Azken hamarkadetan, dimentsio fraktal horrek aplikazio interesgarriak eman ditu talde profinituen testuinguruan, horiek guztiak Barnea eta Shalev-en formula aitzindarian oinarrituta. Formula horren arabera, G talde profinitu baten H azpitalde itxi baten Hausdorffen dimentsioa H-k G-n duen "dentsitate logaritmikotzat" har daiteke. Horrela, G-ren filtrazio serie batekiko Hausdorffen espektro normalaren nozioan jarriko dugu arreta, espektro osoko pro-p talde finituki sortu baten lehen adibidea emanez.

Azkenik, tesiaren hirugarren zatian, bi talde mota berri aurkezten dira: p-talde boteretsuki ebazgarriak eta p-talde boteretsuki bakunak. Talde horiek p-talde boteretsuak dira eta, nolabait, talde ebazgarri finituek eta talde bakun finituek talde finitu guztien klasean duten "papera" betetzen dute, hurrenez hurren. Talde horiei buruzko emaitza eta sailkapen batzuk emango ditugu, Jordan-Hölder motako teorema bat barne. Horretarako, interes berezia izango du talde boteretsu jakin batzuen kategoriaren eta $\mathbb{F}_p$-ren gaineko aljebra alternatuen kategoriaren arteko korrespondentziak.

Sommario

Questa tesi consta di tre parti, ciascuna delle quali dedicata a diversi aspetti della teoria dei p-gruppi finiti e dei pro-p gruppi.

La prima parte analizza le condizioni che un gruppo deve soddisfare affinché il sottogruppo verbale di una parola data coincida con l'insieme dei valori che la parola assume nel gruppo. Si studierà questo problema per parole contenute nel sottogruppo derivato del gruppo libero. Ad esempio, si considereranno la parola commutatore, le parole centrali inferiori e le parole esterne nei p-gruppi finiti.

La seconda parte è incentrata sullo studio della funzione della dimensione di Hausdorff. Negli ultimi decenni, si è dimostrato che questa funzione fornisce interessanti e utili applicazioni nel contesto dei gruppi profiniti, tutti basati sulla formula di Barnea e Shalev che afferma che la dimensione di Hausdorff di un sottogruppo chiuso H su un gruppo profinito G può essere riguardata come la densità logaritmica di H in G. Si analizzerà la nozione di spettro normale di Hausdorff di G rispetto a specifiche filtrazioni e si darà il primo esempio di un pro-p gruppo finitamente generato con spettro normale di Hausdorff completo.

Nella terza parte, infine, si introdurranno due nuove classi di gruppi powerful: i gruppi powerful risolubili e i gruppi powerful semplici. Questi gruppi, in un certo qual modo, si comportano come i gruppi risolubili e semplici nella classe di tutti i gruppi finiti. Verranno, poi, fornite classificazioni di questi gruppi, tra cui un teorema del tipo Jordan-Hölder. A tale scopo, particolare rilevanza è rappresentata dalla corrispondenza biunivoca tra la categoria di specifici gruppi powerful e la categoria di algebre alternate su $\mathbb{F}_p$.

Acknowledgements - Esker onak - Ringraziamenti

Lehenik eta behin, bihotzez eskerrak Gustavo. Zuzendari bezala emandako aholkuek eta behin eta berriz eskaini didazun laguntzak izugarrizko balioa dute niretzat. Zure boligrafo gorria eta, batik bat, zure umore ona funtsezkoak izan dira tesi hau aurrera ateratzeko (eta noski, elkarrekin kantu-kantari igarotako une guztiak ere).

Thank you very much also to Benjamin Klopsch, Marta Morigi, Anitha Thillaisundaram and Gunnar Traustason for all the work that we did together, for the good advice and, above all, for making me feel at home.

Grazie mille a Cristina Acciarri e Carlo Maria Scoppola per aver speso del tempo a leggere questa tesi e per avermi dato degli utili suggerimenti.

He tenido el privilegio de poder trabajar en el fun-office del departamento. Me gustaría agradecer a todos los que, en algún momento u otro, compartieron el despacho conmigo: a Sheila, por el apoyo en mis primeros meses; Joneri, zure konpainia eta bertsolaritza klaseengatik; ad Elena e Marialaura, per la vostra simpatia; y a Natalia, por la ayuda, los consejos, las risas y, por supuesto, por el ambiente argentino que adquiría el despacho con tu mate y la cumbia.

Of course, I do not forget all the other members of the department. Eskerrik asko Xuban Fermini (edo Xubanillo Noetherianori), taldean beti giro ezin hobea sortzeagatik; gracias a Bruno, algún día seremos dueños de un pabellón donde armar mil y una piezas; Esker onak Andoniri ere, gogoratu nirekin Urrotzeko alkate izendatzen zaituztenean; a Matteo Pinto, spero che adesso che lavoriamo con gli alberi inizi a piacerti un po' la frutta; a Albert, ziur estic gure projecte aurrera sortirà dela, visca Euskalunya! Oihanari, aholkuak, laguntza eta, batez ere, barre guztiengatik; and to all the other PhD students and postdocs that have been near me during these years: Igor, Federico, Urban, Jordi, Şükran, Lander, Matteo Vannacci, etc. Thank you very much to all of you. También tengo presente a Ilya, a Montse, a Leire, a Jon, a Javi Gutiérrez, etc. por estar siempre dispuestos a ayudarme y asesorarme. Y a Raúl, Pedro y Marta por todo el apoyo en nuestros trabajos de divulgación.

Estos tres años no habrían sido lo mismo sin mis compañeros de BCAM. Sin los Javis, que hacen una pareja estupenda; sin Martina, con la que espero poder bailar salsa algún día; Tomás eta bere trikitixa gabe; y sin muchos otros como David, Massi, Andrea, Julia, etc. Valoro mucho vuestra compañía durante todo este tiempo (os prometo que algún día daré la charla del LIGHT seminar!).

Non potevo dimenticarmi degli amici di Padova. Di Paola, la migliore coinquilina che si può avere; di Giuseppina, la mia seconda mamma; di Andrea, che mi ha fatto i regali migliori che io abbia mai ricevuto; di Daniele (Marconi), che nonostante tutto, spero venga a farci una visita ai Paesi Baschi; di Mariapia, che è stata sempre gentile con me; di Enrico, per la visita a Bologna; di Almendra, perchè dobbiamo ritornare al Fishmarket al meno un'altra volta; e di Mathieu, oh là là, mon dieu! Grazie a tutti, spero di rivedervi presto. E grazie anche a Carmine, il mio buon amico di Salerno.

Vorrei fare uno speciale ringraziamento al lower team. Ho così tanti bei ricordi che non saprei da dove iniziare: le chiacchiere in ufficio, la sidreria ad Hernani, le risate a Breslavia, le canzoni a Madrid... A te Elena, per essere la voce della ragione e per prenderti sempre cura di noi. Grazie per essere la bella persona che sei. E a te Marialaura. Non ho parole per descrivere la mia gratitudine. Non solo per tutto l'aiuto che mi hai dato in questi anni, ma soprattutto per essere una vera amica. Nik ere asko maite zaitut. Ringrazio moltissimo anche la tua famiglia per avermi accolto con un tale affetto. Sono veramente fortunato di avervi conosciuto.

Bilboko Zazpikaleetan bizi izan denak badaki zein den ona bertako bizitza. Nire kasuan, bi pisukide ezin hobe gehitu behar zaizkio horri. Hirurak horren ezberdinak eta horren lagun onak aldi berean. Ez ditut inoiz ahaztuko, Dani, zurekin egindako korrika saioak, Alhondigako zine maratoiak eta elkarrekin sukaldaturiko otordu goxoak. Eta zer esanik ez, Markel, gure KFNko proiektuetan sartutako ordu luzeez eta pianoaren inguruan konposatutako kantu guztiez. Noan lekura noala faltan botako zaituztet.

Azkenik, eskerrik beroenak familiari, doktoretzan jarraitzeko indarrak emateagatik, eta kuadrilari, berriz, doktoretzaz ahazten laguntzeagatik. En especial me gustaría agradecer a mi Amama y mi Aitite, por reponer fuerzas con todas las deliciosas comidas; a mi Amoña, por tenerme siempre en tus pensamientos; eta Amona Begori, zure laguntza guztiagatik. Amaitzeko, ezin zuetaz ahaztu: Maitane, Aita, Ama, Fermin, Maider eta Maria. Mila esker beti nire ondoan egoteagatik. Asko maite zaituztet.

Contents

Abstract iii

Laburpena v

Sommario vii

Acknowledgements - Esker onak - Ringraziamenti ix

Notation xiii

Summary of the thesis xv

I Commutator words in finite p-groups 1

1 Introduction 3

2 Preliminaries 7
2.1 Basic properties 7
2.2 Powerful and potent groups 9
2.3 Powerful verbal subgroups 12
2.4 Commutator calculus 14
2.4.1 Introducing powers in lower central words 16
2.5 Some significant subgroups 24

3 Commutators 29
3.1 Cyclic derived subgroups 30
3.2 Derived subgroup with 2 generators 31
3.2.1 Finite p-groups with p odd 31
3.2.2 Finite 2-groups 32
3.3 Derived subgroup with 3 or more generators 36
3.3.1 Groups acting uniserially on their derived subgroup 38
3.3.2 Groups with 3-generator and powerful derived subgroup 40
3.3.3 Groups with 3-generator but non-powerful derived subgroup . . . 43

4 Lower central words and general outer commutator words **45**
4.1 Lower central words with cyclic verbal subgroup 45
4.2 Lower central words with non-cyclic verbal subgroup 48
4.2.1 Finite p-groups with $C_r(G) = G$ 48
4.2.2 Finite p-groups with $C_r(G) \neq G$ 51
4.3 Outer commutator words 55

5 Profinite groups **59**
5.1 Generalisation to pro-p groups 61

II Hausdorff dimension in profinite groups **63**

6 Hausdorff dimension and Hausdorff spectra in profinite groups **65**
6.1 Hausdorff dimension in profinite groups 66
6.2 The Hausdorff dimension of closed subgroups 66
6.3 p-adic analytic groups and finite Hausdorff spectra 67
6.4 Infinite Hausdorff spectra 69

7 Normal Hausdorff spectra of profinite groups **71**
7.1 A criterion for a full normal Hausdorff spectra 72
7.2 Construction of a pro-p group with full normal Hausdorff spectra 73
7.2.1 The structure of the finite groups G_k 75
7.2.2 The normal Hausdorff spectra of G 80
7.3 A pro-2 group with full normal Hausdorff spectra 85
7.3.1 Adapting structural results for $p = 2$ 85
7.3.2 The normal Hausdorff spectra for $p = 2$ 90

III Powerfully solvable and powerfully simple p-groups **93**

8 A brief introduction to powerfully nilpotent and powerfully solvable groups **95**

9 Powerfully solvable groups **99**
9.1 Powerful groups of rank 2 99
9.2 Powerful presentations 101
9.3 Classification of powerful groups of order up to p^5 103
9.4 Growth 107

10 Groups of type $(2, \ldots, 2)$ and powerfully simple groups **111**
10.1 Groups of type $(2, \ldots, 2)$ 111
10.2 The classification of powerful groups of type $(2, 2, 2)$ 117
10.2.1 The orbits of the symmetric and anti-symmetric matrices 118
10.2.2 Classification of the alternating algebras 119

Notation

$\mathbb{N}$,$\mathbb{Z}$,$\mathbb{R}$	The set of natural/integer/real numbers
$\mathbb{R}_{\geqslant 0}$	The set of the real numbers that are greater than or equal to 0
$\mathbb{F}_p$	The field of p elements
$\mathbb{Z}_p$	The ring of p-adic integers
$\mathbb{Q}_p$	The field of p-adic numbers
$a \equiv_n b$	$a \in \mathbb{Z}$ is congruent to $b \in \mathbb{Z}$ modulo $n \in \mathbb{Z}$
$\phi(g)$	The image of g under the map ϕ
$\lceil \cdot \rceil$	The ceiling function
$\lfloor \cdot \rfloor$	The floor function
$\subseteq, \subset$	Subset/proper subset
$\leqslant, <$	Subgroup/proper subgroup
$\leqslant_o, \leqslant_c, <_o, <_c$	Open/closed subgroup/proper subgroup
$\trianglelefteq, \triangleleft$	Normal subgroup/proper subgroup
$\trianglelefteq_o, \trianglelefteq_c, \triangleleft_o, \triangleleft_c$	Open/closed normal subgroup/proper subgroup
$\overline{X}$	The topological closure of X
$\langle X \rangle$	The group generated by X
S^{*n}	$\{s_1 \overset{n}{\cdot\cdot} s_n \mid s_i \in S \text{ for all } i = 1, \ldots, n\}$
$d(G)$	Minimal number of generators of G
$\exp(G)$	The exponent of G
$Z(G)$	The center of G
$\mathrm{Aut}(G)$	The group of automorphisms of G
$\mathrm{GL}(n, K)$	The general linear group of degree n over K
$M_n(K)$	The ring of square matrices of degree n over K
$H \equiv_N K$	$H \equiv K \pmod{N}$, i.e., $H, K \leqslant G$ are congruent modulo $N \trianglelefteq G$
x^y	The conjugate of x by y, i.e., $y^{-1}xy$
x^G	The conjugacy class of x in G
H^G	The normal closure of H in G
$C_G(x)$	The centraliser of x in G
$C_G(H)$	The centraliser of H in G
$[x, y]$	The commutator of x and y, i.e., $x^{-1}y^{-1}xy$
$[x, S]$	$\langle [x, s] \mid s \in S \rangle$, where $x \in G$ and $S \subseteq G$
$[R, S]$	$\langle [r, s] \mid r \in R, s \in S \rangle$, where $R, S \subseteq G$
G'	The derived subgroup or the commutator subgroup of G

$K(G)$	The set of commutators of G, i.e., $K(G) = \{[x, y] \mid x, y \in G\}$
$K_x(S)$	$\{[x, s] \mid s \in S\}$, where $x \in G$ and $S \subseteq G$
$[x_1, \ldots, x_r]$	$[[x_1, \ldots, x_{r-1}], x_r]$
$[S_1, \ldots, S_r]$	$[[S_1, \ldots, S_{r-1}], S_r]$
$[x,_n y]$	$[x, y, \overset{n}{\ldots}, y]$
$[H,_n G]$	$[H, G, \overset{n}{\ldots}, G]$
γ_r	The rth lower central word
$\gamma_r(G)$	The rth term of the lower central series of G, i.e., $[\gamma_{r-1}(G), G]$, where $\gamma_1(G) = G$
δ_r	The rth derived word
$G^{(r)}$	The rth derived subgroup of G, i.e., $[G^{(r-1)}, G^{(r-1)}]$, where $G^{(1)} = G$
G_w	The set of w-values of G
$w(G)$	The verbal subgroup of w in G
$H \times N$	The direct product of H and N
$H \ltimes N$	The semidirect product of H and N, via the action of H in N
$A \oplus B$	The direct sum of A and B
$A \oplus\!\!\!\!- B$	The direct orthogonal sum of A and B
$\varprojlim_n G_n$	The inverse limit of the inverse system $\{G_n\}_{n\in\mathbb{N}}$
$\langle \cdot, \cdot \rangle$	A bilinear form
$V^\perp$	The orthogonal complement of V
$\Phi(G)$	The Frattini subgroup of G
G^{p^i}	$\langle g^{p^i} \mid g \in G \rangle$
$\Omega_i(G)$	$\langle g \in G \mid g^{p^i} = 1 \rangle$
$\mathcal{L}$	The Lower p-series
$\mathcal{D}$	The dimension subgroup series
$\mathcal{P}$	The p-power series
$\mathcal{P}^*$	The iterated p-power series
$\mathcal{F}$	The Frattini series
$\mathrm{bdim}_G^{\mathcal{S},\mu}(X)$	The Billingsely dimension of $X \subseteq G$ in G with respect to $\mathcal{S}$ and μ
$\underline{\dim}_B^{\mathcal{S}}(X)$	The lower box dimension of $X \subseteq G$ in G with respect to $\mathcal{S}$
$\mathrm{hdim}_G^{\mathcal{S}}(X)$	The Hausdorff dimension of $X \subseteq G$ in G with respect to $\mathcal{S}$
$\mathrm{hspec}^{\mathcal{S}}(G)$	The Hausdorff spectrum of G with respect to $\mathcal{S}$
$\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteq}(G)$	The normal Hausdorff spectrum of G with respect to $\mathcal{S}$

Summary of the thesis

This thesis is split into three parts, where different aspects of finite p-groups and pro-p groups will be studied.

In Part I of the thesis, the most extensive one, we will study an old question regarding verbal subgroups of commutators words. This study started soon after the introduction of the commutator word on the eve of the 20th century, when it was observed that the product of two commutators of a group G need not be a commutator. It was then asked the following: which are the groups in which the product of two commutators is again a commutator? In other words, when does the derived subgroup G' of a group G coincide with the set of all the commutators of G? Actually, this question can be formulated for any group word w, just replacing the set of commutators with the set G_w of w-values and the derived subgroup G' with the verbal subgroup $w(G) = \langle G_w \rangle$ of G. That is:

Problem. Let w be a word and G a group. Is $w(G) = G_w$?

We will motivate and introduce this problem in more detail in Chapter 1. The words for which this problem will be studied in this thesis are the commutator word, lower central words and general outer commutator words. The groups that we will consider will be finite p-groups and pro-p groups.

Before we start analysing the problem for the aforementioned words and groups, we spend some time establishing some preliminary results in Chapter 2. Apart from developing some technical and fundamental commutator calculus, the class of powerful p-groups will be defined. These groups are, without any doubt, one of the main protagonists of this dissertation. They are usually seen as a generalisation of abelian groups, as they share many properties with them. Among other results, we will show that in almost all the groups that we will work with in the next chapters, the verbal subgroups of the words that we will consider are powerful. This gives us the opportunity to use all the tools that the theory of powerful groups provides. This is, in fact, a completely new approach to the problem, and will allow us to prove a number of results in the area.

In this setting, we will start in Chapter 3 analysing the problem for the commutator word and for finite p-groups. In this context, a great deal of results has been given over the years. One of the most celebrated one is the proof by Liebeck, O'Brien, Shalev and Tiep of the so-called Ore conjecture, according to which every element of a non-abelian finite simple group is a commutator. Sharp bounds on the order of the group and on the order of the derived subgroups have also been found, showing that all the elements of

the derived subgroup G' of a group G are commutators whenever G or G' satisfy these bounds.

However, we will focus on restrictions involving the number of generators of the derived subgroup (and in general, in the next chapters, of the verbal subgroup). In this direction, we will generalise some results due to Guralnick. In these results, Guralnick always works under the condition that the derived subgroup G' of a group G is abelian. We will show in the following two theorems that the condition that G' is abelian is not necessary (these results are published in the Israel Journal of Mathematics [18] and in the Journal of Algebra [32] respectively, and they correspond to Theorems 3.9 and 3.18).

Theorem. *Let G be a finite p-group. If G' can be generated by 2 elements, then $G' = \{[x, g] \mid g \in G\}$ for a suitable $x \in G$.*

Theorem. *Let G be a finite p-group with $p \geqslant 5$. If G' can be generated by 3 elements, then G' consists only of commutators.*

Moreover, it was shown by Guralnick himself that these results are no longer true if G' can be generated by 3 elements with $p = 2$ or 3; or if the minimal number of generators of G' exceeds 3, whatever prime we choose. Since the result for cyclic derived subgroups was already shown to hold by Rodney in another paper, this means that the study of this problem in terms of the number of generators of the derived subgroup for finite p-groups is already complete. We get, furthermore, some partial results if G' is generated by more than 3 elements, adding the condition that the action of G on G' is uniserial modulo $(G')^p$ (this is published in the Journal of Algebra [32], and it corresponds to Theorem 3.19).

Theorem. *Let G be a finite p-group and write $d = \log_p |G' : (G')^p|$. If $d \leqslant p - 1$ and the action of G on G' is uniserial modulo $(G')^p$, then there exists $x \in G$ such that $G' = \{[x, g] \mid g \in G\}$.*

In Chapter 4, following with finite p-groups, we consider lower central words instead of the common commutator word. It was proved, again by Guralnick, that a finite p-group G with $p \geqslant 5$ and with $\gamma_r(G)$ abelian and generated by 2 elements for some $r \geqslant 2$ satisfies that

$$\gamma_r(G) = \{[g_1, \ldots, g_r] \mid g_i \in G \text{ for all } i = 1, \ldots, r\}.$$

Besides that, he also proved that the result is not true anymore if $p = 2$, while the case $p = 3$ remained unsolved. We will again show that this result remains true if we drop the assumption that $\gamma_r(G)$ is abelian. Moreover, we show that the result is also satisfied for $p = 3$, closing in that way the gap between the primes 2 and 5. More precisely, we prove the following (this result will appear in the journal Publicacions Matemàtiques [34], and it corresponds to Theorem 4.10).

Theorem. *Let G be a finite p-group and let $r \geqslant 3$. If $\gamma_r(G)$ is cyclic or if p is odd and $\gamma_r(G)$ can be generated with 2 elements, then there exist $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_r \in G$ with $1 \leqslant j \leqslant r$ such that*

$$\gamma_r(G) = \{[x_1, \ldots, x_{j-1}, g, x_{j+1}, \ldots, x_r] \mid g \in G\}.$$

For every $r \geqslant 3$, we will also modify an existing example to produce a finite p-group, for arbitrary p, with $\gamma_r(G)$ central and generated by 3 elements such that

$$\gamma_r(G) \neq \{[g_1, \ldots, g_r] \mid g_i \in G \text{ for all } i = 1, \ldots, r\},$$

showing in this way that, again, we have completed the study of this property for lower central words in finite p-groups in terms of the number of generators of the verbal subgroup.

The next natural step is considering outer commutator words. We will devote the last part of Chapter 4 to the study of these words. Unfortunately, the only result achieved in this context is the following (this is Theorem 4.17).

Theorem. *Let G be a finite p-group with G'' cyclic. Then there exist $x_1, x_2, x_3 \in G$ such that*

$$G'' = \{[[x_1, x_2], [x_3, g]] \mid g \in G\}.$$

In other words, nothing is known neither for words other than the second derived word or the lower central words, nor for finite p-groups with 2-generator verbal subgroup. Nevertheless, the above theorem could provide a basis for an inductive hypothesis to solve the following problem which, as we will see, could be a key step in order to go further in the study of this property for general outer commutator words.

Problem. Let G be a finite p-group such that $G^{(r)}$ is cyclic for some $r \geqslant 3$. Is then $G^{(r)} = G_{\delta_r}$, were δ_r denotes the rth derived word?

To end with the first part of the thesis, we will dedicate Chapter 5 to generalising all the results we have proved so far from finite p-groups to pro-p groups. Indeed, after making a basic introduction to these groups, the following will be proved (this is Theorem 5.8).

Theorem. *Let w be a word in r variables and let G be a profinite group such that $w(G/N) = (G/N)_w$ for every open normal subgroup N of G. Then $w(G) = G_w$. Moreover, if for every open normal subgroup N of G there exist $1 \leqslant j_N \leqslant r$ and $x_1, \dots, x_{j_N-1}$, $x_{j_N+1}, \dots, x_r \in G/N$ such that*

$$w(G/N) = \{w(x_1, \dots, x_{j_N-1}, g, x_{j_N+1}, \dots, x_r) \mid g \in G/N\},$$

then there exists $1 \leqslant j \leqslant r$ and $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r \in G$ such that

$$w(G) = \{w(x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r) \mid g \in G\}.$$

This result can be directly applied to all of our results, obtaining in this way a generalised version of them for pro-p groups.

After all this, and once profinite groups have been defined, Part II of the thesis is devoted to the analysis of some aspects of the theory of Hausdorff dimension in profinite groups.

In the last decades, the concept of Hausdorff dimension has provided interesting results in the theory of countably based profinite groups. This started with the pioneering work of Barnea and Shalev where, based on Abercrombie's work, they found a group theoretic formula to compute explicitly the Hausdorff dimension $\mathrm{hdim}_G^{\mathcal{S}}(H)$ of a closed subgroup H of a countably based profinite group G with respect to a filtration series $\mathcal{S} : G = G_0 \geqslant G_1 \geqslant \cdots$ of G. More precisely, they showed that

$$\mathrm{hdim}_G^{\mathcal{S}}(H) = \liminf_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|} \in [0, 1].$$

Thus, for a profinite group G and a filtration series $\mathcal{S}$, it is natural to consider what is called the Hausdorff spectrum $\mathrm{hspec}^{\mathcal{S}}(G)$ of G with respect to the filtration series $\mathcal{S}$. This is a subset of the real unit interval $[0,1]$ that reflects the range of the values of the Hausdorff dimensions that the closed subgroups of a profinite group take. We will give in Chapter 6 a brief review of the most important results concerning the Hausdorff spectra of G, introducing some related open problems. We will put special attention on the Hausdorff dimension of p-adic analytic groups with respect to the five standard filtration series, namely: the lower p-series $\mathcal{L}$, the dimension subgroup series $\mathcal{D}$, the p-power series $\mathcal{P}$, the iterated p-power series $\mathcal{P}^*$ and the Frattini series $\mathcal{F}$.

We will focus more, however, on the so-called normal Hausdorff spectrum. For a profinite group G and a filtration series $\mathcal{S}$ of G, the normal Hausdorff spectrum $\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteq}(G)$ of G with respect to the filtration series $\mathcal{S}$ is the subset of the (usual) Hausdorff spectrum $\mathrm{hspec}^{\mathcal{S}}(G)$ that arises when considering closed *normal* subgroups instead of just closed subgroups. In a recent paper, Klopsch and Thillaisundaram asked whether there exists a finitely generated pro-p group whose normal Hausdorff spectrum with respect to any of the five standard filtration series covers the full unit interval $[0,1]$. Thus, in Chapter 7, we will produce the first example of a finitely generated pro-p group that gives an affirmative answer to this question. More precisely, we show the following (this result, for p odd, will appear in the journal Mathematische Nachrichten [33], and it corresponds to Theorem 7.7. The case $p = 2$ is in preparation [35] and it corresponds to Theorem 7.20).

Theorem. *For every prime p, there exists a 2-generator pro-p group G with full normal Hausdorff spectra with respect to the five standard filtration series, that is,*

$$\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteq}(G) = [0,1]$$

for every $\mathcal{S} \in \{\mathcal{L}, \mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$.

Apart from the question by Klopsch and Thillaisundaram, this theorem also answers a question by Shalev.

As said before, the theory of powerful groups has a great importance in the first part of the thesis. Thus, in Part III we will deepen in this topic, introducing two new classes of powerful groups, namely, the powerfully solvable groups and the powerfully simple groups. This is motivated by the recent work of Traustason and Williams where they defined what they called the class of powerfully nilpotent groups.

In Chapter 9 different questions about powerfully solvable groups will be studied. On the one hand we will give an explicit classification of all powerful groups or rank 2 and all powerful groups of order up to p^5. In particular, we will see that there are $22 + 2p$ powerfully solvable groups of order p^5. On the other hand, we will show that the growth of the number of powerfully solvable groups of order p^n and exponent p^2 is $p^{\alpha n^3 + o(n^3)}$, where $\alpha = \frac{-1+\sqrt{2}}{6}$.

While the powerful nilpotence and the powerful solvability have good behaviour when considering homomorphic images, we will see that this is not the case when taking subgroups. This problem disappears, though, if we consider a rich class of powerful groups, namely, the class of powerful groups of type $(2, \overset{r}{\ldots}, 2)$ for some $r \geqslant 0$. We will show in Chapter 10 that there exists a bijective correspondence between the category of these well-behaved groups and the category of alternating algebras of dimension r over

$\mathbb{F}_p$. With this, the notion of powerfully simple groups will be defined and, in close analogy to general finite groups, we also define powerful composition series. Thus, a Jordan-Hölder type theorem will be proved (this is pending acceptance and it is prepublished on the arXiv [36]; it corresponds to Theorem 10.19):

Theorem. *Let G be a powerful p-group of type $(2, \dots, 2)$ with two powerful composition series, say*

$$1 = H_0 \lhd_{\mathcal{P}} H_1 \lhd_{\mathcal{P}} \cdots \lhd_{\mathcal{P}} H_n = G$$

and

$$1 = K_0 \lhd_{\mathcal{P}} K_1 \lhd_{\mathcal{P}} \cdots \lhd_{\mathcal{P}} K_m = G.$$

Then $m = n$ and the powerfully simple factors $H_1/H_0, H_2/H_1, \dots, H_n/H_{n-1}$ are isomorphic to K_1/K_0, K_2/K_1, $\dots, K_n/K_{n-1}$ (in some order).

Finally, we end Chapter 10 with the classification of all powerful groups of type $(2, 2, 2)$. This will be done by classifying all the possible combinations of the symmetric and anti-symmetric bilinear forms in the alternating algebras of dimension 3. In particular, we show that there are $2p + 10$ such groups, of which $p + 3$ are powerfully simple.

Part I

Commutator words in finite p-groups

Chapter 1

Introduction

A group word w in $k \geqslant 0$ variables is an element of the free group F_k on k generators. For any group G, this word defines a map (that abusing notation we still call w) from the Cartesian product of k copies of G to the group G itself by substituting group elements for the variables. More precisely, if $F_k = \langle x_1, \ldots, x_k \rangle$ and

$$w = \prod_{j=1}^{s} x_{i_j}^{\epsilon_j}$$

with $i_1, \ldots, i_s \in \{1, \ldots, k\}$ and each $\epsilon_j = \pm 1$, then

$$\begin{aligned} w : G \times \overset{k}{\cdots} \times G &\longrightarrow G \\ (g_1, \ldots, g_k) &\longmapsto \prod_{j=1}^{s} g_{i_j}^{\epsilon_j}. \end{aligned}$$

Thus, we can consider the set G_w of all values taken by this function, that is,

$$G_w = \{w(g_1, \ldots, g_k) \mid g_i \in G \text{ for all } i = 1, \ldots, k\}.$$

This set is called the *set of w-values* of w in G, and the subgroup generated by it is called the *verbal subgroup* of w in G, denoted by $w(G)$.

Example 1.1. (i) The word in 0 variables is called the *empty word*. For any group G, its verbal subgroup is just the trivial subgroup of G.

(ii) For any $n \geqslant 0$, the *power word* π_n is the word in 1 variable defined as $\pi_n(x) = x^n$. The verbal subgroup of π_n in a group G is denoted by G^n. These groups are usually called the *power subgroups* of G.

(iii) The *commutator word* γ_2 is a word in 2 variables defined as $\gamma_2(x, y) = [x, y] = x^{-1}y^{-1}xy$. Its verbal subgroup in a group G is just the derived subgroup $\gamma_2(G) = G'$ of G (also called the commutator subgroup of G).

(iv) More generally, for $r \geqslant 1$, the *r-th lower central word* γ_r is a word in r variables defined recursively by the rule $\gamma_1(x_1) = x_1$ and

$$\gamma_r(x_1, \dots, x_r) = [\gamma_{r-1}(x_1, \dots, x_{r-1}), x_r].$$

Its verbal subgroup in a group G is precisely the r-th term of the lower central series of G. The words γ_r for $r \geqslant 3$ are also known as *higher commutator words*.

(v) Another way to generalise commutator words is by considering derived words. For $r \geqslant 1$, the *r-th derived word* δ_r is a word in 2^r variables defined recursively by the rule $\delta_1(x_1, x_2) = [x_1, x_2]$ and

$$\delta_r(x_1, \dots, x_{2^r}) = [\delta_{r-1}(x_1, \dots, x_{2^{r-1}}), \delta_{r-1}(x_{2^{r-1}+1}, \dots, x_{2^r})].$$

Its verbal subgroup in a group G is the r-th derived subgroup $\delta_r(G) = G^{(r)}$.

(vi) The words in (iii), (iv) and (v) are particular instances of *outer commutator words*, also known under the name of *multilinear commutator words*. These are words obtained by nesting commutators, but using always different variables. More formally:

- The word $w(x) = x$ in one variable is an outer commutator word.
- If α and β are outer commutator words involving r and s different variables respectively, then the word $w = [\alpha, \beta]$ is an outer commutator in $r + s$ variables.

In addition, all outer commutators are constructed in this way.

(vii) For $n \geqslant 1$, the *n-th Engel word* e_n is a word in 2 variables defined as $e_n(x, y) = [x, y, \overset{n}{\dots}, y]$. Although this word is obtained by nesting commutators, it is not an outer commutator word if $n \geqslant 2$, as in that case the variable y appears more than once.

It is well known that, in general, the set of w-values G_w of a group G need not be a subgroup. In other words, we may have $G_w \subset w(G)$. This is because the product of two word values or the inverse of a word value may not be a word value again. Thus, the following longstanding problem arises naturally.

Problem 1.2. Let G be a group and let w be a word. Is $w(G) = G_w$?

If the group G is abelian, then it is immediate to see that Problem 1.2 is satisfied for any word w. Indeed, word maps are homomorphisms in abelian groups, so if $w(g_1, \dots, g_k)$ and $w(h_1, \dots, h_k)$ are two word values of G, then we have

$$w(g_1, \dots, g_k)^{-1} = w(g_1^{-1}, \dots, g_k^{-1})$$

and

$$w(g_1, \dots, g_k)w(h_1, \dots, h_k) = w(g_1h_1, \dots, g_kh_k).$$

However, for some words w, one can easily find examples of groups G such that $w(G) \neq G_w$ (see, for instance, Example 3.1 below).

In this first part of the thesis we will study this problem for several words that lie inside the commutator subgroup of the free group. Among all the results that we will see or prove, with some exceptions like Theorem 3.2, the problem is almost always reduced, in one way or another, to finite p-groups. A typical argument for that purpose is the following.

Proposition 1.3. *Let w be a word and let G be a (not necessarily finite) nilpotent group such that $w(G)$ is finite. Then, there exists a finite nilpotent group H and an isomorphism $\phi : w(G) \to w(H)$ such that $\phi(G_w) = H_w$.*

Proof. Suppose w is a word in k variables. Since $w(G)$ is finite, it contains, in particular, finitely many w-values, say $w(g_1, \dots, g_k)$, $w(g_{k+1}, \dots, g_{2k})$ and $w(g_{nk+1}, \dots, g_{(n+1)k})$ with $n \geqslant 0$ and $g_1, \dots, g_{(n+1)k} \in G$. Define $K = \langle g_1, \dots, g_{(n+1)k} \rangle$, and note that $K_w = G_w$ and $w(K) = w(G)$. Now, K is nilpotent since so is G, and being finitely generated, it follows that K is residually finite. Hence, since $w(K)$ is finite, there exists a normal subgroup N of K such that $w(K) \cap N = 1$. Consider now the factor group $H = K/N$ and let ϕ be the natural homomorphism from K to H. Clearly we have

$$w(K) = w(K)/(w(K) \cap N) \cong w(K)N/N = w(K/N) = w(H),$$

where the isomorphism is given by the restriction map $\phi\,|_{w(K)}$. Then we have

$$\phi(w(h_1, \dots, h_k)) = w(\phi(h_1), \dots, \phi(h_k))$$

for every $h_1, \dots, h_k \in K$, which shows that $\phi(K_w) = H_w$. □

If G is a finite nilpotent group, then we have $G = P_1 \times \cdots \times P_n$, where $P_1, \dots, P_n$ are the Sylow subgroups of G. Let w be a word in k variables and take $h_1, \dots, h_k \in G$. Then, for every $1 \leqslant i \leqslant k$ there exist $g_{i1} \in P_1, \dots, g_{in} \in P_n$ such that $h_i = g_{i1} \cdots g_{in}$, and it is easy to see that

$$w(g_{11} \cdots g_{1n}, \dots, g_{k1} \cdots g_{kn}) = w(g_{11}, \dots, g_{k1}) \cdots w(g_{1n}, \dots, g_{kn}).$$

This shows that the study of Problem 1.2 for finite nilpotent groups is clearly reduced to finite p-groups. Thus, in view of Proposition 1.3 and because of the fact that there are a number of useful structural results regarding finite p-groups, almost all of our analysis of Problem 1.2 will be focused on them.

Before we give our main results, we will present some preliminaries in Chapter 2, some of which will be used more than once along the dissertation. Among other things, we will develop some theory concerning powerful groups, which will allow us to introduce a completely new approach in this topic. As a matter of fact, this new point of view will be essential in our proofs, since as we will see, the behaviour of the commutator map is much better when the verbal subgroup in consideration is powerful.

In Chapter 3 we will start our study of the commutator word. Our main results in this chapter are proved in Sections 3.2 and 3.3, where we will study finite p-groups with derived subgroup generated by 2 and 3 elements, respectively. Thus, we will solve Problem 1.2 in both cases, showing that $G' = \{[x, y] \mid x, y \in G\}$. Moreover, since this property is already known to hold for finite p-groups with cyclic derived subgroups, and since it is already known to fail for finite p-groups with derived subgroup generated by more than 3 elements, our results complete the study of this problem for finite p-groups when imposing conditions on the number of generators of the derived subgroup.

We will then dedicate Chapter 4 to more general words, namely, to lower central words and, in the end of the chapter, to general outer commutator words. Thus, being a good platform to work, we will continue analysing the problem in finite p-groups. Here we will give, on the one hand, a simple proof of the fact that $\gamma_r(G) = G_{\gamma_r}$ whenever G is a finite p-group and the verbal subgroup $\gamma_r(G)$ is cyclic, which was already proved by

Dark and Newell in [12], and, on the other hand, we will prove the same result for finite p-groups such that $\gamma_r(G)$ is generated by 2 elements. In this way, and using Proposition 1.3 to deduce from an existing example that the problem is no longer true for finite p-groups with verbal subgroups generated by more than 2 elements, we again complete the study of this property in terms of the number of generators of the verbal subgroup in the context of finite p-groups.

The next natural step is to consider general outer commutator words. For these words the problem looks much harder and nothing can be found in the existing literature, even if the verbal subgroup is cyclic. Yet, we break new ground and show that for a finite p-group G we have $G'' = G_{\delta_2}$ whenever G'' is cyclic.

Finally, we will extend in Chapter 5 all the results achieved in the previous chapters from finite p-groups to pro-p groups. Actually the argument we will give to generalise all these results is quite general and works for all words and for all profinite groups in general.

Notation. Let G be a group, and let $H \leqslant G$ and $N \trianglelefteq G$. We write $H \max G$ to denote that H is maximal in G, and $H \max_G N$ to denote that H is maximal among the proper subgroups of N that are normal in G. We set $K(G) = \{[x, y] \mid x, y \in G\}$ and if $x \in G$ then we write $K_x(H) = \{[x, h] \mid h \in H\}$ and $[x, H] = \langle K_x(H) \rangle$. If G is finitely generated, $d(G)$ stands for the minimum number of generators of G. Finally, we write $[G,_n N]$ for $[G, N, \overset{n}{\ldots}, N]$, where $n \geqslant 0$.

Chapter 2

Preliminaries

Before we prove the main results we have achieved regarding Problem 1.2, we spend some time establishing some preliminary results. In fact, many of these results are of independent interest and one may apply them in a more general context than that of this topic.

First we recall in Section 2.1 some basic facts about commutator calculus and finite p-groups that will be frequently used along the thesis.

Without any doubt, one of the main important concepts in this thesis is that of a powerful group. We will define these groups in Section 2.2, where we will also introduce the notion of potent groups. We will thus exhibit some well-known facts and prove some easy results about such groups.

Then we study in Section 2.3 the connection between verbal subgroups and powerful groups. Indeed, we show that if the verbal subgroup of an outer commutator word in a finite p-group G is generated by "few" elements, then it must be powerful. As said in the introduction, this gives a completely new approach to the problem. Actually, this is key to prove our main results, as it allows us to use all the machinery of powerful groups presented in Section 2.2.

We follow in Section 2.4 with some technical results about outer commutator words. These results will be particularly helpful to show that certain quotients of a finite p-group consist only of word values. For instance, we show that the property that a section of a group consists only of commutators of certain type is closed under extensions (Lemma 2.23), and we will give special attention to finding conditions under which a pth power can be introduced inside a lower central commutator (Section 2.4.1).

Finally, in Section 2.5, different subsets (most of them, actually, subgroups) of a finite p-group are defined. These subsets will be of great importance, as the position of them in the group will provide information not only about the presence of some specific commutators in some specific subgroups, but also general information about the group structure itself.

2.1 Basic properties

We start with a well-known fact about finite p-groups, which, in some cases, allows us to assume that certain subgroups of a group are trivial.

Lemma 2.1. *Let G be a finite p-group and N, K normal subgroups of G. If $N \leqslant KN^p[N,G]$, then $N \leqslant K$.*

Proof. Factor out K and just note that if N is non-trivial, then $N^p[N,G]$ is a proper subgroup of N, which is a contradiction. □

The following standard commutator identities will be freely used along the thesis (for the proofs see, for instance, [67, 5.1.5]).

Lemma 2.2. *Let x, y, z be elements of a group. Then:*

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

(ii) $[xy,z] = [x,z]^y[y,z]$, *and* $[x,yz] = [x,z][x,y]^z$.

(iii) $\left[x,y^{-1}\right] = [y,x]^{y^{-1}}$, *and* $\left[x^{-1},y\right] = [y,x]^{x^{-1}}$.

(iv) $[x,y^{-1},z]^y\,[y,z^{-1},x]^z\,[z,x^{-1},y]^x = 1$ *(the Hall-Witt identity).*

As a consequence of the identities above one deduces the next well-known properties. For the reader's convenience we collect them in a lemma.

Lemma 2.3. *Let G be a group. Then:*

(i) *If N and L are two normal subgroups of G and $n \in \mathbb{Z}$, then*

$$[N^n, L] \leqslant [N,L]^n[N,L,N].$$

(ii) *Let $X, Y, Z \leqslant G$ and $N \trianglelefteqslant G$. If $[X,Y,Z], [Y,Z,X] \leqslant N$, then $[Z,X,Y] \leqslant N$. This is known as the* three subgroup lemma.

(iii) *As a consequence, if N is a normal subgroup of G, then $[N, \gamma_n(G)] \leqslant [N,_n G]$ for every $n \geqslant 1$.*

The previous lemmas will be used tacitly, as well as the fact that for each $n \geqslant 0$, if $N \leqslant L$ are two normal subgroups of a finite p-group G such that $|L:N| = p^n$, then $[L,_n G] \leqslant N$. In particular, if L/N is cyclic then $[L,_n G] \leqslant L^{p^n}N$.

The following lemma, probably the most used tool in the thesis, is known as the *Hall-Petresco identity*. It was introduced by Hall and Petresco in [29] and [66] respectively, and it can be proved using the so-called commutator collecting process (for a more modern proof see, for example, [8, Appendix A.1]).

Lemma 2.4. *Let $F_2 = \langle x, y\rangle$ be the free group on 2 generators. Then, there exist words $d_i \in \gamma_i(G)$ for all $i \geqslant 2$ such that for every $n \geqslant 0$ we have*

$$x^n y^n = (xy)^n d_2^{\binom{n}{2}} d_3^{\binom{n}{3}} \cdots d_{n-1}^{\binom{n}{n-1}} d_n.$$

In particular, there exist words $c_i \in \gamma_i(\langle (y^{-1})^x, y\rangle) = \gamma_i(\langle [x,y], y\rangle)$ for all $i \geqslant 2$ such that for every $n \geqslant 0$ we have

$$[x,y^n] = [x,y]^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \cdots c_{n-1}^{\binom{n}{n-1}} c_n.$$

Since these formulas hold in the free group F_2, they apply to any two elements g, h in any group G.

On some occasions a more explicit version of the Hall-Petresco identity will be required. In order to state it, we first need the following notion.

Definition 2.5. Let G be a group and $S \subseteq G$. Let also $c \in G$ and $s \in S$. Then:

- If $c \in S$, then we say that c is a *commutator in* S and that the *weight* of c in S is 1. In addition, if $c = s$, then the weight of c in s is 1, while if $c \neq s$ then the weight of c in s is 0.
- If $c \notin S$ but $c = [x, y]$, where x and y are commutators in S, then c is also a commutator in S and the weight of c in S (in s) is the sum of the weights of x and y in S (in s).

The proof of the next lemma can be found in [55, Proposition 1.1.32].

Lemma 2.6. *Let G be a finite p-group, $x, y \in G$ and $n \in \mathbb{N}$. Let $K(u, v)$ denote the normal closure in G of (i) all commutators in $\{u, v\}$ of weight at least p^n that have weight at least 2 in v, together with (ii) the pth powers of all commutators in $\{u, v\}$ of weight less than p^n and of weight at least 2 in v. Then:*

$$(xy)^{p^n} \equiv_{K(x,y)} x^{p^n} y^{p^n} [y,x]^{\binom{p^n}{2}} [y,x,x]^{\binom{p^n}{3}} \cdots [y,x,\overset{p^n-2}{\ldots},x]^{\binom{p^n}{p^n-1}} [y,x,\overset{p^n-1}{\ldots},x],$$

$$[x^{p^n}, y] \equiv_{K(x,[x,y])} [x,y]^{p^n} [x,y,x]^{\binom{p^n}{2}} \cdots [x,y,x,\overset{p^n-2}{\ldots},x]^{\binom{p^n}{p^n-1}} [x,y,x,\overset{p^n-1}{\ldots},x].$$

In most of the cases, it will be essential knowing when a power of p divides the binomial coefficients $\binom{p^n}{i}$ that appear in both the Hall-Petresco Identity and in Lemma 2.6. The following classical theorem, which will be loosely used, gives an answer to this.

Theorem 2.7 ([53])**.** *Let s and t be integers with $0 \leqslant s \leqslant t$. If α is a positive integer and p a prime, then p^α divides $\binom{t}{s}$ if and only if α carries are needed when adding s and $t - s$ in base p.*

It is thus easy to see that if $t = p^n$ and $s = p^\alpha r$ with $p \nmid r$, then $p^{n-\alpha}$ is the biggest power of p that divides $\binom{p^n}{p^\alpha r}$. In particular, if p is odd then $p^{n-(i-2)}$ divides $\binom{p^n}{i}$ for $2 \leqslant i \leqslant n+2$, while if $p = 2$ then $p^{n-(i-1)}$ divides $\binom{p^n}{i}$ for $2 \leqslant i \leqslant n+1$.

2.2 Powerful and potent groups

Powerful groups are a special type of finite p-groups that were defined by Lubotzky and Mann in [57], even if they were first considered in [38] by Hobby, and some of their results had already been anticipated by other authors (see, for example, [4] and [61]). A finite p-group G is said to be *powerful* if the commutator subgroup G' is contained in $G^p = \langle g^p \mid g \in G \rangle$ for p odd or in $G^4 = \langle g^4 \mid g \in G \rangle$ if $p = 2$. Note that if p is odd, then a finite p-group G is powerful if and only if $\Phi(G) = G^p$, as happens with abelian groups. Indeed, these groups are usually seen as a generalisation of abelian groups, as they share many structural features with them.

While quotients of powerful groups are again powerful, it is not true in general that the subgroups of powerful groups are powerful. There are some subgroups H, however, that are not only powerful subgroups of G, but are *powerfully embedded* in G, meaning that $[H, G] \leqslant H^p$ if p is odd or $[H, G] \leqslant H^4$ if $p = 2$. Most of the important subgroups of a powerful group G are powerfully embedded in G. Indeed, G is obviously powerfully

embedded in G, and if H and K are powerfully embedded subgroups of G, then H^p, HK and $[H,K]$ are also powerfully embedded in G (see [48, Theorem 11.4]).

The reason why these groups are called powerful is in (i) of the next proposition, as it is shown that these groups are somehow "full of powers". A proof of this proposition can be found in [48, Theorems 11.10, 11.11, and 11.15].

Proposition 2.8. *Let G be a powerful group. Then:*

(i) $G^{p^i} = \langle g^{p^i} \mid g \in G\rangle = \{g^{p^i} \mid g \in G\}$ *for every* $i \geqslant 0$.

(ii) $(G^{p^i})^{p^j} = G^{p^{i+j}}$ *for every* $i, j \geqslant 0$.

(iii) *If* $G = \langle x_1, \ldots, x_r\rangle$, *then* $G^{p^i} = \langle x_1^{p^i}, \ldots, x_r^{p^i}\rangle$ *for every* $i \geqslant 0$.

(iv) *The power map* $g \mapsto g^p$ *induces an epimorphism from* $G^{p^i}/G^{p^{i+1}}$ *to* $G^{p^{i+1}}/G^{p^{i+2}}$ *for every* $i \geqslant 0$.

Remark 2.9. By (iv) of the previous proposition, the power map $g \to g^{p^i}$ induces an epimorphism from G/G^p to $G^{p^i}/G^{p^{i+1}}$ for every $i \geqslant 0$. This, in particular implies that if $G^p \leqslant N \leqslant L \leqslant G$, then

$$|L^{p^i} : N^{p^i}| \leqslant |L : N|$$

(and hence $|N : N^{p^i}| \leqslant |L : L^{p^i}|$), and if $L/N = \langle x_1, \ldots, x_n\rangle N$, then

$$L^{p^i}/N^{p^i} = \langle x_1^{p^i}, \ldots, x_n^{p^i}\rangle N^{p^i}.$$

In respect of the generating sets of powerful groups, the following abelian-like properties are really helpful. For the proofs see [13, Corollary 2.8, Theorem 2.9, and Exercise 9 of Chapter 2].

Proposition 2.10. *Let G be a powerful group with $d(G) = d$. Then:*

(i) $d(H) \leqslant d$ *for every* $H \leqslant G$.

(ii) *If* $G = \langle x_1, \ldots, x_d\rangle$ *for some* $x_1, \ldots, x_d \in G$, *then* $G = \langle x_1\rangle \cdots \langle x_d\rangle$.

(iii) G *has a basis, meaning that there exist* $x_1, \ldots, x_d \in G$ *such that* $G = \langle x_1\rangle \cdots \langle x_d\rangle$ *and* $o(x_1) \cdots o(x_d) = |G|$. *Hence, the elements of* G *are precisely* $x_1^{i_1} \cdots x_d^{i_d}$, *where* $0 \leqslant i_j \leqslant o(x_j) - 1$ *for every* $j = 1, \ldots, d$, *without repetitions.*

Other important characteristic subgroups are the so-called *omega subgroups* of G, defined by

$$\Omega_i(G) = \langle g \in G \mid o(g) \leqslant p^i\rangle.$$

These are analogous to the power subgroups G^{p^i} (in fact, the power subgroups G^{p^i} are sometimes called agemo subgroups and denoted by $\mho_i(G)$). It is clear that if G is abelian, then $\Omega_i(G) = \{g \in G \mid o(g) \leqslant p^i\}$. Again, for powerful groups, at least if p is odd, the same result can be deduced. Parts (i), (ii) and (iii) of the following proposition are proved by Wilson in [82] and [83] and by Héthelyi and Lévai in [37] respectively (a short proof of these facts is given by Fernández-Alcober in [17]).

Proposition 2.11. *Let G be a powerful group. Then:*

(i) *If p is odd, then* $\exp(\Omega_i(G)) \leqslant p^i$ *for every* $i \geqslant 0$.

(ii) *If* $p = 2$ *then, unlike for abelian groups, we have* $\exp(\Omega_i(G)) \leqslant 2^{i+1}$ *for every* $i \geqslant 0$.

(iii) $|G : G^{p^i}| = |\Omega_i(G)|$ *for every* $i \geqslant 0$.

To end with powerful groups, we formulate what is known as Shalev's interchanging lemma.

Lemma 2.12 ([72, Lemma 3.1])**.** *Let* G *be a powerful group and let* H *and* K *be powerfully embedded subgroups of* G. *Then* $[H^{p^i}, K^{p^j}] = [H, K]^{p^{i+j}}$ *for every* $i, j \geqslant 0$.

A more extensive background on powerful groups can be found in [13, Chapter 2] or [48, Chapter 11].

We can generalise the concept of powerful groups even more with the notion of *potent* p-group, which will also have an important role in Section 3.3. Indeed, as we will see in the proof of Theorem 3.19, if a group satisfies the conditions of the theorem, then its derived subgroup must be potent. These groups where considered for the first time by Arganbright in [4], even if they were not called potent until González-Sanchez and Jaikin-Zapirain did it in [23]. A finite p-group G is said to be potent if $\gamma_{p-1}(G) \leqslant G^p$ for odd p or if $G' \leqslant G^4$ for $p = 2$ (note that if $p = 2$ or 3, then potent groups are defined in the same way as powerful groups). Potent p-groups are thus a further generalisation of abelian groups. Indeed, it is shown in [23] that if G is a potent p-group with p odd, then the following holds.

(i) $G^{p^i} = \{g^{p^i} \mid g \in G\}$ for all $i \geqslant 0$.

(ii) $\Omega_i(G) = \{g \in G \mid o(g) \leqslant p^i\}$ for all $i \geqslant 0$.

(iii) $|G : G^{p^i}| = |\Omega_i(G)|$ for all $i \geqslant 0$.

A group satisfying these three properties is called *power abelian*. In this context, the following lemma, which is a reduced version of the main theorem in [23], will be particularly helpful.

Lemma 2.13 ([23, Theorem 1.1])**.** *Let* G *be a potent* p*-group with* $p \geqslant 3$. *Then:*

(i) *If* $N \trianglelefteq G$, *then* N *is power abelian.*

(ii) *If* $N \leqslant G^p$ *and* $N \trianglelefteq G$, *then* N *is powerful.*

If p is odd, then Remark 2.9 can be stated in a more general way. Indeed, if G is a potent p-group with p odd, then the indices of the power subgroups of the subgroups of G have a particularly good behaviour.

Lemma 2.14. *Let* G *be a potent* p*-group with* $p \geqslant 3$. *If* $N \leqslant L$ *are two normal subgroups of* G, *then* $|N : N^{p^i}| \leqslant |L : L^{p^i}|$ *for all* $i \geqslant 0$. *In particular* $|L^{p^i} : N^{p^i}| \leqslant |L : N|$.

Proof. By Lemma 2.13, the subgroups N and L are power abelian, so in particular $|N : N^{p^i}| = |\Omega_i(N)|$ and $|L : L^{p^i}| = |\Omega_i(L)|$. Since obviously $|\Omega_i(N)| \leqslant |\Omega_i(L)|$, the result follows. □

For $p = 2$, though, we have a much weaker result.

Lemma 2.15. *Let G be a powerful group and H a powerful subgroup of G. Then $|G^{p^i} : H^{p^i}| \leqslant |G : H|$ for all $i \geqslant 0$.*

Proof. Since G is powerful, we have $d(H) \leqslant d(G)$ by Proposition 2.10. Since H is also powerful, this amounts to $|H : H^p| \leqslant |G : G^p|$, which yields the result for $i = 1$. Now G^p and H^p are again powerful, and we have $G^{p^i} = (G^p)^{p^{i-1}}$ and similarly for H, so the general case follows immediately by induction on i. □

In view of Theorem 2.18 below, we will deal several times with 2-generator powerful groups (see Sections 3.2 and 4.2). In those cases, next lemma will be really useful.

Lemma 2.16. *Let G be a powerful group. If $d(G) = 2$, then every subgroup of G is also powerful.*

Proof. By induction on the group order, it suffices to show that every maximal subgroup M of G is powerful. Now since G is powerful and $d(G) = 2$, we have $|M : G^p| = p$. Since G^p is powerfully embedded in G, it follows from [48, Lemma 11.7] that M is powerful. □

2.3 Powerful verbal subgroups

In our study of Problem 1.2, our main goal will be generalising some results that are already known to hold when the verbal subgroup of the corresponding word w is abelian. According to the last section, a reasonable way to generalise this condition is requiring the verbal subgroup to be not abelian, but powerful. Actually, we will see that almost all the groups we will consider turn out to have powerful verbal subgroups. The main result we have obtained in this direction is a generalised version of the following theorem by Blackburn, where a presentation of the derived subgroup G' of a finite p-group G is given, provided that $d(G') = 2$.

Lemma 2.17 ([9, Theorem 1])**.** *Let G be a finite p-group such that $d(G') \leqslant 2$. Then either G' is abelian or it can be generated by two elements a and b with defining relations $a^{p^m} = b^{p^{n+k}} = 1$ and $[a, b] = b^{p^n}$, with $k > 0$ and $n \geqslant m \geqslant 2k$. In particular, $G'' \leqslant (G')^{p^2}$ and G' is powerful.*

We extend this to more general normal subgroups other than the derived subgroup in the following theorem.

Theorem 2.18. *Let G be a finite p-group and N a normal subgroup of G. If $d(N) = n$, then:*

(i) *If $N \leqslant \gamma_{2n-1}(G)$, then $N' \leqslant N^{p^2}$. In particular N is powerful.*

(ii) *If p is odd and $N \leqslant \gamma_n(G)$, then N is powerful.*

Proof. (i) In order to show that $N' \leqslant N^{p^2}$ we may assume that $N^{p^2} = 1$, and by Lemma 2.1, that $[N', G] = (N')^p = 1$. Since $d(N) = n$ we have $|N : \Phi(N)| = p^n$, and so $[N,_n G] \leqslant \Phi(N)$. First, observe that

$$[\Phi(N), N] = [N^p N', N] \leqslant (N')^p [N', N] = 1,$$

so in particular $\Phi(N)$ is abelian and $\Phi(N)^p = (N^p)^p(N')^p = N^{p^2} = 1$. Moreover, we have

$$\begin{aligned}[\Phi(N),_n G] &= [N^pN',_n G] = [N^p,_n G] \\ &\leqslant [N,_n G]^p \prod_{i=0}^{n} [N,_{n-i} G, N,_i G] \\ &= [N,_n G]^p [N,_n G, N] \\ &\leqslant \Phi(N)^p[\Phi(N), N] = 1,\end{aligned} \tag{2.1}$$

where the first inclusion follows since $(N')^p = 1$ and the third equality follows repeatedly using that $[N', G] = 1$.

If $[N,_{n-1} G] \leqslant \Phi(N)$, then by (2.1) we have

$$\begin{aligned}N' = [N, N] &\leqslant [N, \gamma_{2n-1}(G)] \\ &\leqslant [N,_{2n-1} G] \leqslant [\Phi(N),_n G] = 1,\end{aligned}$$

as desired.

Suppose then $[N,_{n-1} G] \nleqslant \Phi(N)$, and observe that in this case the quotient group

$$N/[N, G]\Phi(N)$$

must be cyclic since $d(N) = n$. Hence, again by (2.1)

$$\begin{aligned}N' = [N, [N, G]\Phi(N)] &= [N, [N, G]] \\ &\leqslant [N,_{2n} G] \leqslant [\Phi(N),_n G] = 1,\end{aligned}$$

and the proof of part (i) is complete.

(ii) The proof is very similar to the previous one. In this case, by Lemma 2.1, we may assume that $N^p = [N', G] = 1$. Thus, we have $\Phi(N) = N'$. Since $d(N) = n$ we have $|N : N'| = p^n$, and so $[N,_n G] \leqslant N'$.

Now, if $[N,_{n-1} G] \leqslant N'$, then we have

$$\begin{aligned}N' = [N, N] &\leqslant [N, \gamma_n(G)] \\ &\leqslant [N,_n G] \leqslant [N', G] = 1,\end{aligned}$$

as desired.

If $[N,_{n-1} G] \nleqslant N'$, then the quotient $N/[N, G]$ must be cyclic. Thus, we have

$$\begin{aligned}N' = [N, [N, G]] &\leqslant [N,_{n+1} G] \\ &\leqslant [N', G] = 1.\end{aligned}$$

The theorem follows. □

Remark 2.19. Part (ii) of Theorem 2.18 can be deduced from [55, Theorem 6.1.14]. Though, we have provided a proof for it that follows the same ideas as the proof of part (i).

The following example, taken from [41, Example 14.24, page 376] and extended to all primes, shows that the condition $N \leqslant \gamma_n(G)$ in (ii) of Theorem 2.18 is best possible, in the sense that the result is no longer true if $N = G'$ and $d(G') = 3$.

Example 2.20. Let $p \geqslant 5$ and consider the groups $A = \langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle \cong C_p \times C_p \times C_p$ and $B = \langle b_1 \rangle \times \langle b_2 \rangle \cong C_p \times C_p$. Define $Y = A \rtimes B$ via the automorphisms

$$a_1^{b_1} = a_1 a_3^{-1}, \quad a_2^{b_1} = a_2 a_3, \quad a_3^{b_1} = a_3,$$
$$a_1^{b_2} = a_1 a_3^{-1}, \quad a_2^{b_2} = a_2, \quad a_3^{b_2} = a_3.$$

Now, consider $X = \langle x \rangle \cong C_p$ and define $G = Y \rtimes X$ via the automorphism

$$a_1^x = a_1 a_2^{-1}, \quad a_2^x = a_2, \quad a_3^x = a_3,$$
$$b_1^x = b_1 b_2^{-1}, \quad b_2^x = b_2 a_1^{-1}.$$

The group G is a p-group of class 5, order p^6 and exponent p such that $d(G') = 3$ and $G'' = \gamma_5(G) \neq 1$, so G' is not powerful.

If $p = 3$, then the same construction works, but taking $X = \langle x \rangle \cong C_9$. Thus we get a group with similar properties but of order 3^7.

If $p = 2$, then we take $A = \langle a_1 \rangle \times \langle a_2 \rangle \cong C_4 \times C_2$ and write $a_3 = a_1^2$. We also take $X = \langle x \rangle \cong C_8$, and we construct the group in the same way as before. In this case the order of G is 2^8.

2.4 Commutator calculus

For a group G, the standard property in (ii) of Lemma 2.2 shows that the commutator map γ_2 from $G \times G$ to G is not bilinear in general, and this fact immediately extends to all outer commutator words. We give a generalised version of (ii) of Lemma 2.2 reaffirming this.

Lemma 2.21. *Let G be a group and let w be an outer commutator word in r variables. Let $x_1, \ldots, x_{j-1}, h, x_{j+1}, \ldots, x_r \in G$. Then there exist $h_1, \ldots, h_r \in \langle h \rangle^G$ such that for every $g \in G$,*

$$w(x_1, \ldots, x_{j-1}, gh, x_{j+1}, \ldots, x_r)$$
$$= w(x_1^{h_1}, \ldots, x_{j-1}^{h_{j-1}}, g^{h_j}, x_{j+1}^{h_{j+1}}, \ldots, x_r^{h_r}) w(x_1, \ldots, x_{j-1}, h, x_{j+1}, \ldots, x_r).$$

Proof. We proceed by induction on the number of variables appearing in the outer commutator word w. If such number is 1, i.e. if $w = x$, then the result is obvious. Hence, assume $w = [\alpha, \beta]$, where α and β are outer commutator words involving k and $r - k$ variables with $k < r$, respectively. Assume also that $j > k$, so that

$$w(x_1, \ldots, x_{j-1}, gh, x_{j+1}, \ldots, x_r)$$
$$= [\alpha(x_1, \ldots, x_k), \beta(x_{k+1}, \ldots, x_{j-1}, gh, x_{j+1}, \ldots, x_r)].$$

By induction, we have

$$\beta(x_{k+1}, \ldots, x_{j-1}, gh, x_{j+1}, \ldots, x_r)$$
$$= \beta(x_{k+1}^{h_{k+1}}, \ldots, x_{j-1}^{h_{j-1}}, g^{h_j}, x_{j+1}^{h_{j+1}}, \ldots, x_r^{h_r}) \beta(x_{k+1}, \ldots, x_{j-1}, h, x_{j+1}, \ldots, x_r),$$

where $h_{k+1}, \ldots, h_r \in \langle h \rangle^G$.

For simplicity, write

$$z_1 = \beta(x_{k+1}^{h_{k+1}}, \ldots, x_{j-1}^{h_{j-1}}, g^{h_j}, x_{j+1}^{h_{j+1}}, \ldots, x_r^{h_r})$$

and

$$z_2 = \beta(x_{k+1}, \dots, x_{j-1}, h, x_{j+1}, \dots, x_r),$$

and notice that

$$\begin{aligned}[\alpha(x_1, \dots, x_k), z_1 z_2] &= [\alpha(x_1, \dots, x_k), z_2][\alpha(x_1, \dots, x_k), z_1]^{z_2} \\ &= [\alpha(x_1, \dots, x_k), z_1]^{z_2^{\alpha(x_1,\dots,x_k)}}[\alpha(x_1, \dots, x_k), z_2].\end{aligned}$$

Since clearly $z_2 \in \langle h \rangle^G$, the result follows.

The case $j \leqslant k$ is similar. □

Repeatedly applying Lemma 2.21 we obtain Corollary 2.22 below, where it is shown that the commutator map, even if it is not multilinear in general as we have seen before, it does have a multilinear nature. This is also proved in [73, Proposition 1.2.1].

Corollary 2.22. *Let G be a group. Then, for every $i = 1, \dots, n$ and for every $g, x_1, \dots, x_{i-1}, x_{i+1}, \dots x_n \in G$, $h \in \gamma_s(G)$ we have*

$$\begin{aligned}&[x_1, \dots, x_{i-1}, gh, x_{i+1}, \dots, x_n] \equiv \\ &\quad [x_1, \dots, x_{i-1}, g, x_{i+1}, \dots, x_n][x_1, \dots, x_{i-1}, h, x_{i+1}, \dots, x_n] \pmod{\gamma_{n+s}(G)}.\end{aligned}$$

In particular, if $h \in G'$ then

$$\begin{aligned}&[x_1, \dots, x_{i-1}, gh, x_{i+1}, \dots, x_n] \equiv \\ &\qquad [x_1, \dots, x_{i-1}, g, x_{i+1}, \dots, x_n] \pmod{\gamma_{n+1}(G)}.\end{aligned}$$

We now introduce one of the principal tools of this part. It shows how to extend the covering of a subgroup with w-values from a factor group to the whole group, where w is an outer commutator word. This somehow reflects the strategy we will mainly follow when proving that the verbal subgroup $w(G)$ consists only of w-values. Indeed, we will construct a series from $w(G)$ to 1 with the property that every element of each factor group of two consecutive subgroups in the series can be written as a w-value in a suitable way. Lemma 2.23 below will then allow us to go up in this series, proving that actually all the subgroups in the series consist of w-values, until we reach $w(G)$.

Lemma 2.23. *Let G be a group and w an outer commutator word on r variables. Let $N \leqslant L \leqslant G$ with N normal in G and suppose that for some $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r \in G$, the following two conditions hold:*

(i) $L \subseteq \bigcup_{g \in G} N w(y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r)$ *for every* $y_i \in x_i^G$.

(ii) $N \subseteq \{w(y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r) \mid g \in G\}$ *for every* $y_i \in x_i^G$.

Then, $L \subseteq \{w(y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r) \mid g \in G\}$ for every $y_i \in x_i^G$.

Proof. Take an arbitrary coset $Nw(y_1, \dots, y_{j-1}, h, y_{j+1}, \dots, y_r)$ of N in L, with $y_i \in x_i^G$ and $h \in G$. Take $h_1, \dots, h_r$ as in Lemma 2.21 and let z be an arbitrary element of N. By assumption, there exists $u \in G$ such that $z = w(y_1^{h_1}, \dots, y_{j-1}^{h_{j-1}}, u, y_{j+1}^{h_{j+1}}, \dots, y_r^{h_r})$ and we may write u in the form $u = g^{h_j}$ with $g \in G$.

So, by Lemma 2.21 our arbitrary element $zw(y_1, \dots, y_{j-1}, h, y_{j+1}, \dots, y_r)$ of the above coset can be written as

$$\begin{aligned}&w(y_1^{h_1}, \dots, y_{j-1}^{h_{j-1}}, g^{h_j}, y_{j+1}^{h_{j+1}}, \dots, y_r^{h_r}) w(y_1, \dots, y_{j-1}, h, y_{j+1}, \dots, y_r) \\ &\qquad = w(y_1, \dots, y_{j-1}, gh, y_{j+1}, \dots, y_r),\end{aligned}$$

as desired. □

Remark 2.24. As a matter of fact, Lemma 2.23 can be stated in a slightly more general way. Indeed, if we relax condition (i) and just put

$$L \subseteq \bigcup_{g \in G} Nw(x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r),$$

then, following the same proof, we obtain

$$L \subseteq \{w(x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r) \mid g \in G\}.$$

However, the way in which we have stated it allows us to apply the lemma in an ascending series of subgroups of G, as if we apply it in two subgroups of the series, then the resulting inclusion is precisely the condition we need to continue applying it in the subgroups above.

For the commutator word this remark is not necessary, as Corollary 2.25 shows.

Corollary 2.25. *Let G be a group and let $N \leqslant L \leqslant G$, with N normal in G. Suppose that for some $x \in G$ the following two conditions hold:*

(i) $L/N \subseteq K_{xN}(G/N)$.

(ii) $N \subseteq K_x(G)$.

Then $L \subseteq K_x(G)$.

Proof. Just note that since N is normal in G, then for every $g \in G$ we have

$$N = N^g = K_x(G)^g = K_{x^g}(G^g) = K_{x^g}(G),$$

and thereby condition (ii) of Lemma 2.23 holds. The result follows now from Remark 2.24. □

The previous corollary will be often used in combination with the following result, whose proof is straightforward.

Lemma 2.26. *Let G be a group and let $N \leqslant L \leqslant G$, with N normal in G. If $L/N = \langle [x,s]N \mid s \in S \rangle$ for some $x \in G$ and some $S \subseteq G$ with $[L,S] \subseteq N$, then $L/N \subseteq K_{xN}(\langle S \rangle N/N) \subseteq K_{xN}(G/N)$.*

Proof. It follows immediately since for every $s, t \in S$ we have

$$[x, st] = [x, s][x, t]g$$

for some $g \in [x, S, S] \leqslant [L, S] \subseteq N$. □

2.4.1 Introducing powers in lower central words

As pointed out at the beginning of Section 2.4, outer commutator words are not multilinear in general. In particular, for a finite p-group G and for $x, g \in G$, it is not always true that $[x,g]^{p^i} = [x, g^{p^i}]$, with $i \geqslant 1$. In the following three sections we will see that under certain conditions we can ensure that the power p^i can be introduced in a commutator modulo some subgroups. This will ensure that certain sections of a group consist only of commutators of a certain type, so it will be essential in order to use Lemma 2.23. We will deal with three different cases, namely, with finite p-groups with a 2-generator powerful subgroup; finite p-groups with $p \geqslant 3$ such that $d((G')^{p^k})$ is "small" for some $k \geqslant 0$; and finite p-groups such that $d(\gamma_r(G)) \leqslant 2$ for some $r \geqslant 2$.

Finite p-groups with a 2-generator powerful subgroup

The next lemma is the key to our proof of Theorem 3.9. As said, it shows that under a specific hypothesis we can introduce powers in commutators but, apart from that, it also shows that, with some additional conditions, covering a factor group L/L^p with commutators of a given element x is enough to cover the whole subgroup L.

Lemma 2.27. *Let G be a finite p-group and let $N \leqslant L$ be normal subgroups of G, with L powerful and $d(L) \leqslant 2$. Then the following hold:*

(i) *If there exist $x, g \in G$ such that $L/N = \langle [x,g]N \rangle$ and $[x,g,g] \in N^p$, then $L^{p^i}/N^{p^i} = \langle [x, g^{p^i}]N^{p^i} \rangle$ for every $i \geqslant 1$.*

(ii) *Assume furthermore that $L^p \leqslant N$ and $|L : N| = p$. If there exist $x, g, h \in G$ such that $L/N = \langle [x,g]N \rangle$ and $N/L^p = \langle [x,h]L^p \rangle$ with $[x,g,g] \in N^p$ and $[x,h,h] \in L^{p^2}$, then $L \subseteq K_x(G)$.*

Proof. (i) We argue by induction on i. Assume first $i = 1$. Since L is powerful and $L = \langle [x,g], N \rangle$, it follows that $L^p = \langle [x,g]^p, N^p \rangle$, and thus $L^p/N^p = \langle [x,g]^p N^p \rangle$. Now, from the hypothesis $[x,g,g] \in N^p$ we get

$$[x, g^p] \equiv [x,g]^p \pmod{N^p}, \tag{2.2}$$

and consequently $L^p/N^p = \langle [x,g^p]N^p \rangle$.

Now let $i > 1$. By Lemma 2.16, N is also powerful. If we prove that $[x, g^p, g^p] \in N^{p^2}$, then we can apply the induction hypothesis with L^p and N^p playing the role of L and N, and g^p playing the role of g, and we are done. Observe that $|N^p : N^{p^2}| \leqslant p^2$, since N^p is powerful and $d(N^p) \leqslant d(L) \leqslant 2$. Since N is normal in G, it follows that $[N^p, G'] \leqslant [N^p, G, G] \leqslant N^{p^2}$. As a consequence,

$$[N^p, G^p] \leqslant [N^p, G]^p [N^p, G, G] \leqslant N^{p^2}$$

and then (2.2) yields that

$$[x, g^p, g^p] \equiv [[x,g]^p, g^p] \pmod{N^{p^2}}.$$

On the other hand, since $[x,g,g] \in N^p$ implies that $[x,g,g^p] \in N^p$ as well, it follows that $[[x,g], g^p, [x,g]] \in [N^p, G'] \leqslant N^{p^2}$, and we obtain as desired that

$$[x, g^p, g^p] \equiv [[x,g]^p, g^p] \equiv [x,g,g^p]^p \equiv 1 \pmod{N^{p^2}}.$$

(ii) Consider the following normal series of G:

$$L \geqslant N \geqslant L^p \geqslant N^p \geqslant L^{p^2} \geqslant N^{p^2} \geqslant \cdots \geqslant 1. \tag{2.3}$$

By hypothesis, we have $|L : N| = p$. Also, since L is powerful and $d(L) \leqslant 2$, we have $|L : L^p| \leqslant p^2$, and therefore $|N : L^p| \leqslant p$. As a consequence, if R and S are two consecutive terms of (2.3) then $|R : S| \leqslant p$, by using Lemma 2.15. Hence the section R/S is central in G. On the other hand, by (i), $R/S = \langle [x,y]S \rangle$ for some $y \in G$. Then $R/S \subseteq K_{xS}(G/S)$ by Lemma 2.26, and by going up in the series (2.3) and using Corollary 2.25, we conclude that $L \subseteq K_x(G)$. □

Finite p-groups where $d((G')^{p^k})$ is "small"

Similarly, we now give a result concerning finite p-groups with $p \geqslant 3$ such that $(G')^{p^k}$ is powerful and $d((G')^{p^k}) \leqslant p^{k+1} - p^k - 1$.

Lemma 2.28. *Let G be a finite p-group with $p \geqslant 3$ and $(G')^{p^k}$ powerful for some $k \geqslant 0$, and let L, N be two normal subgroups of G such that $((G')^{p^k})^p \leqslant N \leqslant L \leqslant (G')^{p^k}$. Write $d = d((G')^{p^k})$ and suppose $d \leqslant p^{k+1} - p^k - 1$. If $L/N = \langle [x,g]N \rangle$ where $x \in G$ and $g \in G^{p^k}$, then*

$$[x,g]^{p^i} \equiv [x, g^{p^i}] \pmod{N^{p^i}},$$

and $L^{p^i}/N^{p^i} = \langle [x, g^{p^i}]N^{p^i} \rangle$ for every $i \geqslant 0$.

Proof. We will argue by induction on i. If $i = 0$ then the result follows trivially, so assume $i \geqslant 1$ and suppose

$$[x,g]^{p^{i-1}} \equiv [x, g^{p^{i-1}}] \pmod{N^{p^{i-1}}}$$

and $L^{p^{i-1}}/N^{p^{i-1}} = \langle [x, g^{p^{i-1}}]N^{p^{i-1}} \rangle$. By Lemma 2.13, L and N are power abelian, so $(L^{p^{i-1}})^p = L^{p^i}$ and $(N^{p^{i-1}})^p = N^{p^i}$. Since $((G')^{p^k})^{p^{i-1}}$ is powerful, Remark 2.9 yields

$$L^{p^i}/N^{p^i} = \langle [x, g^{p^{i-1}}]^p N^{p^i} \rangle.$$

Thus, we only have to prove that

$$[x, g^{p^{i-1}}]^p \equiv [x, g^{p^i}] \pmod{N^{p^i}}.$$

By the Hall-Petresco identity,

$$[x, g^{p^{i-1}}]^p = [x, g^{p^i}] c_2^{\binom{p}{2}} c_3^{\binom{p}{3}} \cdots c_p,$$

where $c_j \in \gamma_j(\langle [x, g^{p^{i-1}}], g^{p^{i-1}} \rangle) \leqslant [L^{p^{i-1}}, {}_{j-1}\, G^{p^k}]$ for every $2 \leqslant j \leqslant p$. Note that L/N is cyclic of exponent p, so $|L : N| \leqslant p$ and again by Remark 2.9 we have $|L^{p^{i-1}} : N^{p^{i-1}}| \leqslant p$, so that $[L^{p^{i-1}}, G] \leqslant N^{p^{i-1}}$. Hence, since N is power abelian, if $2 \leqslant j \leqslant p-1$ we have $c_j^{\binom{p}{j}} \in N^{p^i}$.

If $j = p$, then $c_p \in [L^{p^{i-1}}, {}_{p-1}\, G^{p^k}]$. Recall that $(G')^{p^k}$ is powerful, so we have $|((G')^{p^k})^{p^{i-1}} : ((G')^{p^k})^{p^i}| \leqslant p^d$, and hence $|N^{p^{i-1}} : N^{p^i}| \leqslant p^d$. If $k = 0$, since $d \leqslant p-2$, we get

$$c_p \in [L^{p^{i-1}}, {}_{p-1}\, G] \leqslant [L^{p^{i-1}}, {}_{d+1}\, G] \leqslant [N^{p^{i-1}}, {}_{d}\, G] \leqslant N^{p^i}.$$

If $k \geqslant 1$, then it can be proved using again the Hall-Petresco identity that for every normal subgroup H of G we have

$$[H, G^{p^k}] \leqslant [H,G]^p [H, {}_{p^k}\, G],$$

so

$$\begin{aligned} c_p \in [L^{p^{i-1}}, {}_{p-1}\, G^{p^k}] &\leqslant [L^{p^{i-1}}, G]^p [L^{p^{i-1}}, {}_{(p-1)p^k}\, G] \\ &\leqslant N^{p^i} [N^{p^{i-1}}, {}_{(p-1)p^k - 1}\, G] \leqslant N^{p^i}, \end{aligned}$$

where the last equality holds since $d \leqslant p^{k+1} - p^k - 1$. The result follows. □

Thus, combining Corollary 2.25, Lemma 2.26 and Lemma 2.28 we get the following useful result. Recall that if $L, N \trianglelefteqslant G$, then L/N is a *chief factor* of G if it is a minimal normal subgroup of G/N.

Lemma 2.29. *Let G be a finite p-group with $p \geqslant 3$ and $(G')^{p^k}$ powerful for some $k \geqslant 0$. Write $d((G')^{p^k}) = d$ and suppose $d \leqslant p^{k+1} - p^k - 1$. If there exist $x \in G$, $g_0, \dots, g_{d-1} \in G^{p^k}$ and a series from $(G')^{p^k}$ to $((G')^{p^k})^p$*

$$((G')^{p^k})^p = N_d < N_{d-1} < \cdots < N_0 = (G')^{p^k}$$

in which each factor N_j/N_{j+1} is a chief factor of G generated by the commutator $[x, g_j]N_{j+1}$, then $(G')^{p^k} = K_x(G)$.

Proof. Since $(G')^{p^k}$ is powerful we have $|(G')^{p^k} : ((G')^{p^k})^p| = p^d$. By Remark 2.9, we have $|N_j^{p^i}/N_{j+1}^{p^i}| \leqslant p$ for every $i \geqslant 0$, and furthermore, by Lemma 2.28, this quotient is generated by $[x, g_j^{p^i}]N_{j+1}^{p^i}$ for every i and j. Therefore, it follows from Lemma 2.26 that

$$N_j^{p^i}/N_{j+1}^{p^i} \subseteq K_{xN_{j+1}^{p^i}}(G/N_{j+1}^{p^i}).$$

In this way, we have a series from $(G')^{p^k}$ to 1 in which all factors are chief factors of G and all elements of each chief factor are images of commutators of the form $[x, g]$ with $g \in G$. The result follows by applying Corollary 2.25 again and again. □

Remark 2.30. Lemma 2.29 (and hence also Lemma 2.28) will be used with $k \neq 0$ only when proving Theorem 3.18, where we use it with $k = 1$. The general result has been proved for completeness.

Finite p-groups with $d(\gamma_r(G)) \leqslant 2$

Unlike the previous cases, one must be much more thorough when introducing powers in lower central words. In this case we deal with finite p-groups such that $d(\gamma_r(G)) \leqslant 2$ if p is odd and $\gamma_r(G)$ cyclic if $p = 2$. Because of the high level of technicality required in the proof of Lemma 2.33, though, we prove it step by step, proving first Lemma 2.31 and Lemma 2.32.

Lemma 2.31. *Let G be a finite p-group such that for some $r \geqslant 2$ we have $d(\gamma_r(G)) \leqslant 2$ if p is odd or $d(\gamma_r(G)) = 1$ if $p = 2$. Then, for every $2 \leqslant j \leqslant r$ and every normal subgroup R of G contained in $\gamma_j(G)$ we have*

$$[y, x_{j+1}, \dots, x_r]^{p^k} \equiv [y^{p^k}, x_{j+1}, \dots, x_r] \pmod{[R, {}_{r-j}\, G]^{p^{k+1}}}$$

for all $y \in R$, $x_{j+1}, \dots, x_r \in G$ and $k \geqslant 0$. Moreover,

$$[R, {}_{r-j}\, G]^{p^k} = [R^{p^k}, {}_{r-j}\, G].$$

Proof. We will proceed by induction on $r - j$. If $r = j$ then there is nothing to prove, so assume $j < r$ and that the result holds for all $r - i$ with $j < i \leqslant r$. Fix a normal subgroup $R \leqslant \gamma_j(G)$ of G and $y \in R$. Thus, since $[R, G]$ normal in G, by induction we have

$$[y, x_{j+1}, \dots, x_r]^{p^k} \equiv [[y, x_{j+1}]^{p^k}, x_{j+2}, \dots, x_r] \pmod{[R, {}_{r-j}\, G]}.$$

Now, by the Hall-Petresco identity, we obtain

$$[y, x_{j+1}]^{p^k} = [y^{p^k}, x_{j+1}]c_2^{\binom{p^k}{2}} \cdots c_{p^k}$$

with $c_n \in \gamma_n(\langle [y, x_{j+1}], y\rangle)$ for $2 \leqslant n \leqslant p^k$, and since $j \geqslant 2$ and $y \in R \leqslant \gamma_j(G)$, it follows that

$$c_n \in [R, {}_{j(n-1)+1}\ G] \leqslant [R, {}_{2(n-1)+1}\ G]$$

for every n. Note that $p^{k-(n-2)}$ divides $\binom{p^k}{n}$ if p is odd and that $p^{k-(n-1)}$ divides $\binom{p^k}{n}$ if $p = 2$. So, if p is odd, we get

$$c_n^{\binom{p^k}{n}} \in [R, {}_{2(n-1)+1}\ G]^{\lceil p^{k-(n-2)} \rceil},$$

and if $p = 2$ we get

$$c_n^{\binom{2^k}{n}} \in [R, {}_{2(n-1)+1}\ G]^{\lceil 2^{k-(n-1)} \rceil}$$

(note that here, the ceiling function is used since $k-(n-2)$ (or $k-(n-1)$) could be negative, in which case we want the power $p^{k-(n-2)}$ (or the power $2^{k-(n-1)}$) to be 1). Since $d(\gamma_r(G)) \leqslant 2$, it follows by Theorem 2.18 that $\gamma_r(G)$ is powerful. From Lemma 2.16 we then deduce that for all $m \geqslant 0$, $[R, {}_{r-j}\ G]^{p^m}$ is also powerful and $d([R, {}_{r-j}\ G]^{p^m}) \leqslant 2$, so

$$|[R, {}_{r-j}\ G]^{p^m} : [R, {}_{r-j}\ G]^{p^{m+1}}| \leqslant p^2$$

for all $m \geqslant 0$. This implies, in particular, that

$$[[R, {}_{r-j}\ G]^{p^m}, G, G] \leqslant [R, {}_{r-j}\ G]^{p^{m+1}}$$

for all $m \geqslant 0$, and therefore

$$[R, {}_{r-j+2(n-1)}\ G]^{\lceil p^{k-(n-2)} \rceil} \leqslant [R, {}_{r-j}\ G]^{p^{k+1}}.$$

Now, if p is odd, using the inductive hypothesis we have

$$\begin{aligned} &[[R, {}_{2(n-1)+1}\ G]^{\lceil p^{k-(n-2)} \rceil}, {}_{r-j-1}\ G] \\ &\qquad = [R, {}_{r-j+2(n-1)}\ G]^{\lceil p^{k-(n-2)} \rceil} \\ &\qquad \leqslant [R, {}_{r-j}\ G]^{p^{k+1}}. \end{aligned} \tag{2.4}$$

If $p = 2$ then we argue in the same way, taking into account the fact that, in this case, $\gamma_r(G)$ is cyclic and hence

$$[[R, {}_{r-j}\ G]^{2^m}, G] \leqslant [R, {}_{r-j}\ G]^{2^{m+1}}.$$

Thus, the first assertion follows.

For the second assertion, just observe that $[R^{p^k}, {}_{r-j}\, G]$ is generated by elements of the form $[y^{p^k}, x_{j+1}, \ldots, x_r]$ with $y \in R$ and $x_{j+1}, \ldots, x_r \in G$, and

$$[y^{p^k}, x_{j+1}, \ldots, x_r] \equiv [y, x_{j+1}, \ldots, x_r]^{p^k} \pmod{[R, {}_{r-j}\ G]^{p^{k+1}}}.$$

□

Lemma 2.32. *Let G be a finite p-group such that for some $r \geqslant 2$ we have $d(\gamma_r(G)) \leqslant 2$ if p is odd and $d(\gamma_r(G)) = 1$ if $p = 2$. Assume that H and K are normal subgroups of G, with K generated by γ_{j-1}-values, where $1 \leqslant j \leqslant r$. Then for every $k \geqslant 0$ we have*

$$[K, H^{p^k}, {}_{r-j}\, G] \leqslant [K, H, {}_{r-j}\, G]^{p^k}.$$

Proof. We use induction on k. The case $k = 0$ is trivial, so assume $k = 1$ first, and suppose $p \geqslant 3$ (if $p = 2$ the proof follows in the same way). As p divides $\binom{p}{i}$ for $2 \leqslant i < p$ and $\gamma_3(\langle [K, H], H\rangle) \leqslant [K, H, H, H]$, the Hall-Petresco identity yields

$$[K, H^p] \leqslant [K, H]^p [K, H, H, H].$$

Note that $[K, H]$ is generated by elements of the type $[x_1, \ldots, x_{j-1}, x_j]$, where $x_1, \ldots, x_{j-1} \in G$ and $x_j \in H$, so by Lemma 2.31, we have

$$[[K, H]^p, {}_{r-j}\, G] = [K, H, {}_{r-j}\, G]^p.$$

On the other hand, $\gamma_r(G)$ is powerful by Theorem 2.18. Thus, it follows from Lemma 2.16 that

$$|[K, H, {}_{r-j}\, G] : [K, H, {}_{r-j}\, G]^p| \leqslant p^2,$$

so we obtain

$$\begin{aligned} [K, H, H, H, {}_{r-j}\, G] &\leqslant [[K, H, {}_{r-j}\, G], G, G] \\ &\leqslant [K, H, {}_{r-j}\, G]^p. \end{aligned}$$

Hence,

$$[K, H^p, {}_{r-j}\, G] \leqslant [[K, H]^p [K, H, H, H]], {}_{r-j}\, G] \leqslant [K, H, {}_{r-j}\, G]^p,$$

as desired.

Assume now $k \geqslant 2$. Then, by induction,

$$\begin{aligned} [K, H^{p^k}, {}_{r-j}\, G] &\leqslant [K, (H^p)^{p^{k-1}}, {}_{r-j}\, G] \\ &\leqslant [K, H^p, {}_{r-j}\, G]^{p^{k-1}} \\ &\leqslant ([K, H, {}_{r-j}\, G]^p)^{p^{k-1}}, \end{aligned}$$

and since $[K, H, {}_{r-j}\, G]$ is powerful by Lemma 2.16, we conclude

$$([K, H, {}_{r-j}\, G]^p)^{p^{k-1}} = [K, H, {}_{r-j}\, G]^{p^k}.$$

Thus, the proof is complete. □

Lemma 2.33. *Let G be a finite p-group and let N, L be normal subgroups of G such that $\gamma_r(G)^p \leqslant N \leqslant L \leqslant \gamma_r(G)$ with $r \geqslant 2$ and $|L : N| = p$. Assume that there exist some j with $1 \leqslant j \leqslant r$ and $x_1, \ldots, x_{j-1}, h, x_{j+1}, \ldots, x_r \in G$ such that*

$$L = \langle [x_1, \ldots, x_{j-1}, h, x_{j+1}, \ldots, x_r] \rangle N.$$

Let H be the normal closure of $\langle h \rangle$ in G and assume also that one of the following conditions holds:

(i) *p is odd, $d(\gamma_r(G)) \leqslant 2$ and the subgroup*

$$[\gamma_{j-1}(G), H, H, {}_{r-j}\ G]$$

is central of exponent p modulo N^p.

(ii) *$p = 2$, the subgroup $\gamma_r(G)$ is cyclic and*

$$[x_1, \dots, x_{j-1}, h, x_{j+1}, \dots, x_r]^2 \equiv [x_1, \dots, x_{j-1}, h^2, x_{j+1}, \dots, x_r] \pmod{N^2}.$$

Then,

$$[x_1, \dots, x_{j-1}, h, x_{j+1}, \dots, x_r]^{p^k} \equiv [x_1, \dots, x_{j-1}, h^{p^k}, x_{j+1}, \dots, x_r] \pmod{N^{p^k}}$$

for every $k \geqslant 0$. In particular,

$$L^{p^k} = \langle [x_1, \dots, x_{j-1}, h^{p^k}, x_{j+1}, \dots, x_r] \rangle N^{p^k}.$$

Proof. We use induction on k. If $k = 0$ there is nothing to prove and, if $p = 2$ and $k = 1$, then the result follows from the hypothesis. Thus, assume $k \geqslant 1$ if p is odd or $k \geqslant 2$ if $p = 2$, and suppose, by induction, that

$$[x_1, \dots, x_{j-1}, h, x_{j+1}, \dots, x_r]^{p^{k-1}} = [x_1, \dots, x_{j-1}, h^{p^{k-1}}, x_{j+1}, \dots, x_r]y$$

for some $y \in N^{p^{k-1}}$.

Write $u = [x_1, \dots, x_{j-1}, h^{p^{k-1}}, x_{j+1}, \dots, x_r] \in \gamma_r(G)$ and note that $(uy)^p = u^p y^p c$ where $c \in [N^{p^{k-1}}, \gamma_r(G)] \leqslant [N^{p^{k-1}}, G, G] \leqslant (N^{p^{k-1}})^p = N^{p^k}$. Thus,

$$([x_1, \dots, x_{j-1}, h^{p^{k-1}}, x_{j+1}, \dots, x_r]y)^p \equiv [x_1, \dots, x_{j-1}, h^{p^{k-1}}, x_{j+1}, \dots, x_r]^p \pmod{N^{p^k}}.$$

Moreover, by Lemma 2.32, we have

$$[\gamma_{j-1}(G), H^{p^{k-1}}, {}_{r-j}\ G]^{p^2} = [\gamma_{j-1}(G), H, {}_{r-j}\ G]^{p^{k+1}} \leqslant \gamma_r(G)^{p^{k+1}} \leqslant N^{p^k},$$

so using Lemma 2.31 with $R = [\gamma_{j-1}(G), H^{p^{k-1}}]$ we obtain

$$\begin{aligned}[x_1, \dots, x_{j-1}, h, x_{j+1}, \dots, x_r]^{p^k} &\equiv [x_1, \dots, x_{j-1}, h^{p^{k-1}}, x_{j+1}, \dots, x_r]^p \\ &\equiv [[x_1, \dots, x_{j-1}, h^{p^{k-1}}]^p, x_{j+1}, \dots, x_r] \pmod{N^{p^k}}.\end{aligned}$$

Suppose now p is odd. We first prove that

$$[\gamma_{j-1}(G), H^{p^{k-1}}, H^{p^{k-1}}, {}_{r-j}\ G] \text{ is central of exponent } p \text{ modulo } N^{p^k}. \tag{2.5}$$

Recall that L, N and $[\gamma_{j-1}(G), H, H, {}_{r-j}\ G]$ are powerful by Theorem 2.18 and Lemma 2.16. From Lemma 2.32 and hypothesis (i) of the statement we then get

$$\begin{aligned}[\gamma_{j-1}(G), H^{p^{k-1}}, H^{p^{k-1}}, {}_{r-j+1}\ G] & \\ &\leqslant [\gamma_{j-1}(G), H, H, {}_{r-j+1}\ G]^{p^{k-1}} \\ &\leqslant (N^p)^{p^{k-1}} = N^{p^k}\end{aligned}$$

and

$$\begin{aligned}[\gamma_{j-1}(G), H^{p^{k-1}}, H^{p^{k-1}}, {}_{r-j}\ G]^p & \\ &\leqslant ([\gamma_{j-1}(G), H, H, {}_{r-j}\ G]^{p^{k-1}})^p \\ &\leqslant (N^p)^{p^{k-1}} = N^{p^k}.\end{aligned}$$

This proves (2.5).

By the Hall-Petresco identity, since $p \geqslant 3$, we get

$$[x_1, \dots, x_{j-1}, h^{p^{k-1}}]^p = [x_1, \dots, x_{j-1}, h^{p^k}] z_2^p z_3,$$

where $z_i \in \gamma_i(\langle [\gamma_{j-1}(G), H^{p^{k-1}}], H^{p^{k-1}} \rangle)$ for $i = 2, 3$. Write

$$R = [\gamma_{j-1}(G), H^{p^{k-1}}, H^{p^{k-1}}],$$

so that $z_2 \in R$ and $z_3 \in [R, G]$.

On the one hand, by (2.5) we have

$$[z_3, x_{j+1}, \dots, x_r] \in [R, {}_{r-j+1}\ G] \leqslant N^{p^k}.$$

On the other hand it follows from Lemma 2.32 with $H = R$ and $K = G$ and from (2.5) that

$$[z_2^p, x_{j+1}, \dots, x_r] \in [R, {}_{r-j}\ G]^p \leqslant N^{p^k}.$$

Therefore, by Lemma 2.21,

$$\begin{aligned}[x_1, \dots, x_{j-1}, h, x_{j+1}, \dots, x_r]^{p^k} &\equiv [[x_1, \dots, x_{j-1}, h^{p^k}] z_2^p z_3, x_{j+1}, \dots, x_r] \\ &\equiv [x_1, \dots, x_{j-1}, h^{p^k}, x_{j+1}, \dots, x_r] \pmod{N^{p^k}}\end{aligned}$$

as we wanted.

If $p = 2$, since $\gamma_r(G)$ is cyclic, we have $L = \gamma_r(G)$, $N = \gamma_r(G)^2$ and the inductive step easily follows from the Hall-Petresco identity. Namely,

$$[x_1, \dots, x_{j-1}, h^{2^{k-1}}]^2 = [x_1, \dots, x_{j-1}, h^{2^k}] z_2,$$

where $z_2 \in [\gamma_{j-1}(G), G^{2^{k-1}}, G^{2^{k-1}}]$. By Lemma 2.32 and since $k \geqslant 2$ we have

$$[\gamma_{j-1}(G), G^{2^{k-1}}, G^{2^{k-1}}, {}_{r-j}\ G] \leqslant \gamma_{r+1}(G)^{2^{2k-2}} \leqslant \gamma_r(G)^{2^{k+1}} = N^{2^k},$$

so the result follows as above. □

2.5 Some significant subgroups

In this last section of Chapter 2 we define some subgroups (or subsets) that will play a fundamental role in Chapters 3 and 4. As mentioned at the beginning of the chapter, these subgroups (or subsets) are interesting on their own, as they provide information about the group structure itself.

The following subgroups were essential in [24], and so are in our results.

Definition 2.34. Let G be a finite p-group. For $r \geqslant 2$, we define

$$C_r(G) = C_G(\gamma_r(G)/\gamma_r(G)^p).$$

If p is odd and if $\gamma_r(G)$ is powerful, then, by definition, $\gamma_r(G)$ is powerfully embedded in $C_r(G)$, and so all power subgroups $\gamma_r(G)^{p^i}$ are also powerfully embedded in $C_r(G)$. In other words, we have $[\gamma_r(G)^{p^i}, C_r(G)] \leqslant \gamma_r(G)^{p^{i+1}}$. As it turns out, if $\gamma_r(G)$ is powerful, this is true for all primes, and similar inclusions hold for other commutator subgroups involving $C_r(G)$. We collect these and other properties in Proposition 2.36 below. Before, however, we need a lemma that, actually, generalises the "powerfully embeded" condition.

Lemma 2.35. *Let G be a finite p-group and let N be a powerful normal subgroup of G. Write $C_i = C_G(N/N^{p^i})$. Then,*

$$[N^{p^k}, C_i^{p^j}] \leqslant N^{p^{i+j+k}},$$

with $i \geqslant 1$ and $j, k \geqslant 0$.

Proof. We argue by induction on j. Assume first $j = 0$, and consider the factor group $G/N^{p^{i+k}}$. Thus, we have to check that the subgroups $N^{p^k}/N^{p^{i+k}}$ and $C_i/N^{p^{i+k}}$ commute, or equivalently, that their generators commute. Take $g \in N$ and $h \in C_i$. The Hall-Petresco identity yields

$$[g^{p^k}, h] = [g, h]^{p^k} c_2^{\binom{p^k}{2}} c_3^{\binom{p^k}{3}} \cdots c_{p^k},$$

where

$$c_n \in \gamma_n(\langle g, [g, h]\rangle) \leqslant [N, C_i, N, \overset{n-1}{\ldots}, N] \leqslant [N^{p^i}, N, \overset{n-1}{\ldots}, N].$$

Recall that N is powerful, so if $p = 2$, this subgroup lies in $N^{2^{i+2n-2}}$, while if $p > 2$ it lies in $N^{p^{i+n-1}}$. In any case, $c_n^{\binom{p^k}{n}} \in N^{p^{i+k}}$, and since

$$[g, h]^{p^k} \in [N, C_i]^{p^k} \leqslant (N^{p^i})^{p^k} = N^{p^{i+k}},$$

we conclude that $[g^{p^k}, h] \in N^{p^{i+k}}$, as we wanted.

Consider now a general j. Again, we consider the factor group $G/N^{p^{i+j+k}}$, and we have to see that the generators of $N^{p^k}/N^{p^{i+j+k}}$ and $C_i^{p^j}/N^{p^{i+j+k}}$ commute. Take $g \in G$ and $h \in C_i$ and observe that

$$[g^{p^k}, h^{p^j}] = [g^{p^k}, (h^{p^{j-1}})^p] = [g^{p^k}, h^{p^{j-1}}]^p d_2^{\binom{p}{2}} \cdots d_p$$

where

$$d_n \in \gamma_n(\langle [g^{p^k}, h^{p^{j-1}}], h^{p^{j-1}}\rangle) \leqslant [N^{p^k}, C_i^{p^{j-1}}, C_i^{p^{j-1}}] \leqslant N^{p^{k+2j+2i-2}}$$

by induction. Since $i, j \geqslant 1$ we have $k + 2j + 2i - 2 \geqslant i + j + k$, and since $[g^{p^k}, h^{p^{j-1}}]^p \in (N^{p^{i+j+k-1}})^p$, the theorem follows. □

Proposition 2.36. *Let G be a finite p-group with $\gamma_r(G)$ powerful for some $r \geqslant 2$. Then:*

(i) *We have $[\gamma_r(G)^{p^i}, C_r(G)] \leqslant \gamma_r(G)^{p^{i+1}}$ for all $i \geqslant 0$.*

(ii) *$[\gamma_{r-1}(G), C_r(G)^{p^i}] \leqslant \gamma_r(G)^{p^i}$ for every $i \geqslant 0$.*

Moreover, if $d(\gamma_r(G)) = 2$, then:

(iii) *$|G : C_r(G)| \leqslant p$.*

(iv) *We have $G = C_r(G)$ if and only if $\gamma_{r+1}(G) \leqslant \gamma_r(G)^p$. In this case, all subgroups U such that $\gamma_r(G)^p < U < \gamma_r(G)$ are normal in G. Otherwise, $C_r(G) \neq G$ and there is only one normal subgroup U of G such that $\gamma_r(G)^p < U < \gamma_r(G)$, namely $U = \gamma_{r+1}(G)\gamma_r(G)^p$.*

Proof. (i) It follows immediately from Lemma 2.35 taking $N = \gamma_r(G)$ and $i = 1$.

(ii) We argue by induction on i, the case $i = 0$ being obvious. If $i > 0$ then

$$\begin{aligned}[\gamma_{r-1}(G), C_r(G)^{p^i}] &\leqslant [\gamma_{r-1}(G), C_r(G)^{p^{i-1}}]^p [\gamma_{r-1}(G), C_r(G)^{p^{i-1}}, C_r(G)^{p^{i-1}}] \\ &\leqslant (\gamma_r(G)^{p^{i-1}})^p [\gamma_r(G)^{p^{i-1}}, C_r(G)] \leqslant \gamma_r(G)^{p^i},\end{aligned}$$

where the last inclusion follows from (i).

(iii) Since $\gamma_r(G)$ is powerful, the quotient $\gamma_r(G)/\gamma_r(G)^p$ is an elementary abelian p-group of rank 2. The result follows from the fact that the quotient group $G/C_r(G)$ embeds in a Sylow p-subgroup of the automorphism group of $\gamma_r(G)/\gamma_r(G)^p$, which has order $p(p^2-1)(p-1)$.

(iv) The first assertion follows immediately from the definition of $C_r(G)$. Now, if $C_r(G) = G$, then for $U \max \gamma_r(G)$ we clearly have $[U, G] \leqslant [\gamma_r(G), G] \leqslant \gamma_{r+1}(G)$, so U is normal in G. However, note that there are $p+1$ subgroups that are maximal in $\gamma_r(G)$, so if there exists a non-normal subgroup U of G with $\gamma_r(G)^p < U < \gamma_r(G)$ then, the conjugacy class of U has size p, and it follows that $\gamma_{r+1}(G)\gamma_r(G)^p$ is the only normal subgroup of G which is maximal in $\gamma_r(G)$. □

We now draw our attention to another type of subgroups (or subsets). The importance of these will become clear soon.

Definition 2.37. Let G be a finite p-group and let $U \max_G \gamma_r(G)$ for some $r \geqslant 2$. We define

$$D_r(U) = C_{\gamma_{r-1}(G)}(G/U).$$

In other words, for $x \in \gamma_{r-1}(G)$ we have $x \in D_r(U)$ if and only if $[x, G] \leqslant U$.

Definition 2.38. Let G be a finite p-group and let $U \max_{\gamma_{r-1}(G)} \gamma_r(G)$ for some $r \geqslant 2$. We define

$$E_r(U) = \{x \in G \mid [x, \gamma_{r-1}(G)] \leqslant U\}.$$

Remark 2.39. The subset $E_r(U)$ may not be a subgroup of G if U is not normal in G. Nevertheless, if U is normal in G, then $E_r(U)$ is also normal in G as it coincides with the subgroup $C_G(\gamma_{r-1}(G)/U)$.

The significance of these subgroups (or subsets) lies on the fact that one can extract useful information about the group if there exists an element avoiding them, as the next lemma shows.

Proposition 2.40. *Let G be a finite p-group and let $r \geqslant 2$. Then, for $x \in \gamma_{r-1}(G)$, we have $\gamma_r(G) = [x, G]$ if and only if*

$$x \notin \bigcup \{D_r(U) \mid U \max_G \gamma_r(G)\}.$$

Similarly, $\gamma_r(G) = [\gamma_{r-1}(G), y]$ if and only if

$$y \notin \bigcup \{E_r(U) \mid U \max_{\gamma_{r-1}(G)} \gamma_r(G)\}.$$

Proof. Let $x \in \gamma_{r-1}(G)$. First note that $[x, G]$ is normal in G since

$$[x, g]^h = [x, h]^{-1}[x, gh]$$

for every $g, h \in G$. Consequently we have $[x, G] < \gamma_r(G)$ if and only if $x \in D_r(U)$ for some $U \max_G \gamma_r(G)$, and the first assertion follows. Similarly, since $[\gamma_{r-1}(G), y]$ is normalised by $\gamma_{r-1}(G)$, we have $[\gamma_{r-1}(G), y] < \gamma_r(G)$ if and only if $y \in E_r(U)$ for some $U \max_{\gamma_{r-1}(G)} \gamma_r(G)$. □

We now present some properties of the subgroups $D_r(U)$. These will be used when $r = 2$ and $d(G') = 2$, but we prove them in more generality for completion.

Proposition 2.41. *Let G be a finite p-group and $U \max_G \gamma_r(G)$ with $r \geqslant 2$. Then:*

(i) $\gamma_{r-1}(G)^p \gamma_r(G) \leqslant D_r(U)$. *In particular* $\Phi(G) \leqslant D_2(U)$.

(ii) *If $r = 2$, then $\log_p |G : D_2(U)|$ is even.*

(iii) *If $d(\gamma_r(G)) \leqslant r$, then $D_r(U) \leqslant C_r(G)$.*

(iv) *If $d(G') \leqslant 2$, then $\bigcup \{D_2(V) \mid V \max_G G'\}$ is a proper subset of G.*

Proof. (i) We have

$$[\gamma_{r-1}(G)^p \gamma_r(G), G] = [\gamma_{r-1}(G)^p, G]\gamma_{r+1}(G) \leqslant \gamma_r(G)^p \gamma_{r+1}(G) \leqslant U,$$

and so $\gamma_{r-1}(G)^p \gamma_r(G) \leqslant D_r(U)$.

(ii) By (i), the quotient $G/D_2(U)$ can be seen as a vector space over $\mathbb{F}_p$. Thus, since $G'/U \cong \mathbb{F}_p$, the commutator map in G/U induces a non-degenerate alternating form on $G/D_2(U)$. Then, $\dim_{\mathbb{F}_p} G/D(U)$ must be even by [40, Proposition 1].

(iii) We have

$$[D_r(U), \gamma_r(G)] \leqslant [D_r(U),_r G] \leqslant [U,_{r-1} G] \leqslant \gamma_r(G)^p$$

since $|U : \gamma_r(G)^p| \leqslant p^{r-1}$, and consequently $D_r(U) \leqslant C_r(G)$.

(iv) Write $D = \bigcup \{D_2(V) \mid V \max_G G'\}$ and assume for a contradiction that $D = G$. If $|G' : (G')^p| = p$ then $D = D((G')^p)$ and consequently $G' = [D, G] \leqslant (G')^p$, a contradiction. Thus $|G' : (G')^p| = p^2$. Let $x \in G$ be arbitrary. Then $x \in D(W)$ for some $W \max_G G'$ and the image of $[x, G]$ in $\overline{G} = G/(G')^p$ has order at most p. It follows that all conjugacy class lengths in $\overline{G}$ are either 1 or p, so by [8, Lemma 2.12] this implies that $|\overline{G}'| \leqslant p$, which is again a contradiction. □

Remark 2.42. By the previous proposition, if $d(G') \leqslant 2$ then there always exists $x \in G$ such that $G' = [x, G]$. Since $|G : C_2(G)| \leqslant p$ by Proposition 2.36 and

$$\bigcup \{D_2(U) \mid U \max_G G'\} \subseteq C_2(G)$$

by Proposition 2.41, we can choose $x \notin \cup\{D_2(U) \mid U \max_G G'\}$ such that $G = \langle x \rangle C_2(G)$, and then we get $G' = [x, C_2(G)]$.

We end this chapter with some properties that the subgroups and subsets $D_r(U)$ and $E_r(V)$ have in common.

Proposition 2.43. *Let G be a finite p-group and let $r \geqslant 2$. Let $U, V, W \max_G \gamma_r(G)$ with $V \neq W$ and $R, S, T \max_{\gamma_{r-1}(G)} \gamma_r(G)$ with $S \neq T$. Then:*

(i) *$D_r(U) \neq \gamma_{r-1}(G)$ and $E_r(R) \neq G$.*

Moreover, if $d(\gamma_r(G)) = 2$, then:

(ii) *$D_r(V) \cap D_r(W) \leqslant D_r(U)$ and $E_r(S) \cap E_r(T) \subseteq E_r(R)$.*

(iii) *If $U \neq R$, then $[D_r(U), E_r(R)] \leqslant \gamma_r(G)^p$.*

Proof. (i) It is obvious, since $D_r(U) = \gamma_{r-1}(G)$ implies that $\gamma_r(G) \leqslant U$, and similarly $E_r(R) = G$ implies that $\gamma_r(G) \leqslant R$. In both cases we have a contradiction.

(ii) As $d(\gamma_r(G)) = 2$, the subgroup $\gamma_r(G)$ is powerful by Theorem 2.18, so $\gamma_r(G)^p = \Phi(\gamma_r(G))$. Hence, $V \cap W \leqslant \gamma_r(G)^p \leqslant U$ and $S \cap T \leqslant \gamma_r(G)^p \leqslant R$. Then, the result follows from the fact that $x \in D_r(V) \cap D_r(W)$ if and only if $[x, G] \leqslant V \cap W$ and $y \in E_r(S) \cap E_r(T)$ if and only if $[y, \gamma_{r-1}(G)] \leqslant S \cap T$.

(iii) We have $[D_r(U), E_r(R)] \leqslant U \cap R \leqslant \gamma_r(G)^p$. □

Chapter 3

Commutators

We are finally ready to study Problem 1.2 for several words inside the commutator subgroup of the free group. Being the simplest one, we will start with the common commutator word γ_2.

The definition of this word is attributed to Dedekind; according to Frobenius [21], and in modern notation, Dedekind proved in 1880 that the derived subgroup G' of a group G is normal in G and that $G' \leqslant N$ for every $N \trianglelefteq G$ such that G/N is abelian. These results, though, were first published by Miller in [62]. Miller himself was the first labelling these elements as "commutators" in [63] and [64], where he dealt with them as objects that are of interest in their own right. Moreover, in [64], he found a criterion to ensure that the product of two commutators is again a commutator (property (ii) of Lemma 2.2), and with the help of this identity he showed that every element of the alternating group A_n with $n \geqslant 5$ is a commutator, a result rediscovered over 50 years later by Ito [42] and Ore [65] (in fact, Ore stated his famous conjecture, which will be addressed later, in this paper).

The first explicit statement of Problem 1.2 for commutators can be found in Weber's 1899 textbook [78], which was the first textbook to introduce commutators and the commutator subgroup. It was Fite, however, who provided in [20] the first example of a group whose derived subgroup is strictly bigger that the set of commutators. As we show now, [60, Lemma 1] provides a great deal of groups G for which the derived subgroup G' does not coincide with the set of commutator $K(G)$ of G (much more information of the origin of the commutator can be found in the introduction of [47]).

Example 3.1. Let $G = F_d/\gamma_3(F_d)F_d^p$, where F_d is the free group on $d \geqslant 6$ generators and $p > 2$ is a prime. This group, even if it has exponent p and is nilpotent of class 2, does not satisfy the equality $G' = K(G)$. Indeed, note that $|G'| = p^{\binom{d}{2}}$, while $|G : Z(G)| \leqslant p^d$. Thus, since $d \geqslant 6$, we have $2d < \binom{d}{2}$, so from [60, Lemma 1], the inequality holds.

Actually, it is shown in [47, Example 5.2] that $G' \neq K(G)$ holds even if $d \geqslant 4$. Moreover, for $d = 4$, one can find a suitable subgroup $N \leqslant G'$ of order p^2 such that the quotient group $H = G/N$ satisfies $H' \neq K(H)$ with $H \cong C_p \times C_p \times C_p \times C_p$ [47, Example 5.4].

We need, then, to restrict our choice of the group G to some particular family of groups if we want it to satisfy the desired property. A remarkable result is the proof by Liebeck, O'Brien, Shalev, and Tiep in 2010 of the so-called Ore Conjecture.

Theorem 3.2 (Ore Conjecture, [56]). *Let G be a non-abelian finite simple group. Then $G = K(G)$.*

Another typical approach to the problem is considering small groups or groups with small derived subgroup. The main two results in this context are Theorem 3.3 and Theorem 3.4 below.

Theorem 3.3 ([24, Theorem 1]). *Let G be a group and suppose one of the following conditions hold.*

(i) *G' is abelian and either $|G| < 128$ or $|G'| < 16$.*

(ii) *G' is non-abelian and either $|G| < 96$ or $|G'| < 24$.*

Then $G' = K(G)$. Moreover, these bounds are best possible.

For p-groups of order p^n the situation is much better, as one only needs to consider bounds on the exponent n, regardless of the prime p. In this way, as there is no bound on the prime, there is no bound on the order of the group either.

Theorem 3.4 ([45, Theorems 3.4 and 4.2]). *Let G be a p-group of order p^n. Then $G' = K(G)$ if $n \leqslant 5$ for odd p and $n \leqslant 6$ for $p = 2$.*

We will focus, though, on restrictions regarding the number of generators of the derived subgroup. Thus, we will deal separately with three cases: G' cyclic, $d(G') = 2$ and $d(G') \geqslant 3$.

A wealth of additional information about the condition $G' = K(G)$ can be found in [47].

3.1 Cyclic derived subgroups

In this case, Macdonald proved in [58] that even if G' is cyclic then Problem 1.2 may have a negative answer. Actually, much more is true.

Theorem 3.5 ([58, Theorem]). *For every $n \in \mathbb{N}$ there exists a group G such that G' is cyclic but cannot be generated by less than n commutators.*

This theorem shows how delicate the equality $G' = K(G)$ can be. The situation, fortunately, is much better for the cyclic case if G' is infinite or if G is nilpotent. We will see, actually, that in general, nilpotent groups behave specially well when it comes to Problem 1.2.

Theorem 3.6 ([68, Corollary]). *Let G be a group. If G' is cyclic and either G is nilpotent or G' is infinite, then G' consists of commutators.*

In this theorem, once it is shown that the result holds for groups with infinite derived subgroup, one can reduce the problem, as seen in Proposition 1.3, to the case in which G is finite and nilpotent. Furthermore, as said before, the study of this property for

finite nilpotent groups is obviously reduced to finite p-groups. We will thus limit our focus to them in the following chapters (and to pro-p groups in Chapter 5).

As an easy illustration of our methods, let us give an easy proof of Theorem 3.6 for finite p-groups. Let $C = C_G(G'/(G')^{p^2})$. Then $|G : C| \leqslant p$ since $|G' : (G')^{p^2}| \leqslant p^2$, and so $G' = [G, C]$. By the Burnside basis theorem, we have $G' = \langle [x, y] \rangle$ for some $x \in G$ and $y \in C$. Then $[x, y, y] \in [G, C, C] \leqslant [G', C] \leqslant (G')^{p^2}$ and we can apply Lemma 2.27 with $L = G'$ and $N = (G')^p$ to get $G' = K_x(G)$.

3.2 Derived subgroup with 2 generators

If G is a finite p-group with 2-generator derived subgroup, then Guralnick showed the following.

Theorem 3.7 ([25, Theorem A])**.** *Let G be a finite group and let $P \in Syl_p(G)$ with $P^* = P \cap G'$ abelian and $d(P^*) \leqslant 2$. Then $P^* \subseteq K(G)$.*

For the proof of Theorem 3.7 Guralnick uses a reduction argument that allows him to assume that the group G is a finite p-group. In that case, the theorem translates to the following.

Corollary 3.8. *Let G be a finite p-group with 2-generator and abelian derived subgroup. Then $G' = K(G)$.*

We have generalised Corollary 3.8, showing that the condition that G' is abelian can be dropped. Moreover, we show that all the commutators in G' have a particular form.

Theorem 3.9 ([18, Theorem A])**.** *Let G be a finite p-group. If G' can be generated by 2 elements, then $G' = \{[x, g] \mid g \in G\}$ for a suitable $x \in G$.*

We split the proof of Theorem 3.9 into two parts, proving first the result for p odd and then for $p = 2$.

3.2.1 Finite p-groups with p odd

The result for odd primes can be easily proved using Corollary 2.25.

Theorem 3.10. *Let G be a finite p-group, where p is an odd prime, and assume that $d(G') \leqslant 2$. Then $G' = K_x(G)$ for a suitable $x \in G$.*

Proof. The theorem follows from Theorem 3.6 if G' is cyclic, so assume $d(G') = 2$. We write for simplicity $C = C_2(G)$. Thus, by Remark 2.42 we have $G' = [x, C]$ for some $x \in G$ and so, by Lemma 2.26,

$$G'/(G')^p = \{[x, u](G')^p \mid u \in C\}.$$

By Corollary 2.25, we only need to prove that $(G')^p \subseteq K_x(G)$. Hence we may assume that $(G')^p \neq 1$.

Since G' is powerful by Lemma 2.17, the map $g(G')^p \longmapsto g^p(G')^{p^2}$ is an epimorphism from $G'/(G')^p$ to $(G')^p/(G')^{p^2}$ by Proposition 2.8. Thus $(G')^p/(G')^{p^2}$ consists of the cosets $[x, u]^p(G')^{p^2}$ with $u \in C$. Now if $u \in C$ then, by the Hall-Petresco identity, $[x, u^p] = [x, u]^p w$ for some $w \in (H')^p \gamma_p(H)$, where $H = \langle (u^{-1})^x, u \rangle = \langle u, [x, u] \rangle$. Then

$H' \leqslant [G,C,C] \leqslant (G')^p$ and $(H')^p \leqslant (G')^{p^2}$, and since p is odd, also $\gamma_p(H) \leqslant [(G')^p, C] \leqslant (G')^{p^2}$ by Proposition 2.36. Hence $[x,u]^p \equiv [x,u^p] \pmod{(G')^{p^2}}$ for every $u \in C$. It follows that every element of $(G')^p$ is of the form $[x,u^p]$ modulo $(G')^{p^2}$ for some $u \in C$.

Now let us choose a subgroup T between $(G')^p$ and $(G')^{p^2}$ with $|(G')^p : T| = p$. Thus both $(G')^p/T$ and $T/(G')^{p^2}$ are cyclic, generated by the image of some commutator $[x,u^p]$ with $u \in C$. By Proposition 2.36, we have $[x,u^p,u^p] \in [G,C^p,C^p] \leqslant [(G')^p,C^p] \leqslant (G')^{p^3}$. Thus we can apply (ii) of Lemma 2.27 with $L = (G')^p$ and $N = T$ to get $(G')^p \subseteq K_x(G)$, as desired. □

3.2.2 Finite 2-groups

Now we are concerned with the proof of Theorem 3.9 for finite 2-groups, which is quite more involved. The main difficulty arises when $C_2(G) = G$, and in order to deal with that case, we introduce the following subgroups.

Definition 3.11. Let G be a finite 2-group such that $(G')^2 \neq 1$. For every $U \max_G (G')^2$ we define the subgroup $R(U)$ by the condition

$$R(U)/U = C_{G/U}(G^2/U).$$

In other words, $R(U)$ is the largest subgroup of G satisfying $[R(U),G^2] \leqslant U$. We set $R = \cup\{R(U) \mid U \max_G (G')^2\}$.

Lemma 3.12. *Let G be a finite 2-group with $d(G') \leqslant 2$. Assume furthermore that $C_2(G) = G$ and that $(G')^2 \neq 1$. Then the following hold:*

(i) $[G,G^2] = (G')^2$.

(ii) $[x,G^2] = (G')^2$ *if and only if* $x \notin R$.

(iii) $G^2 \leqslant R(U) < G$ *for every* $U \max_G (G')^2$.

(iv) $R(U) \cap R(V) \leqslant R(W)$ *for every* $U,V,W \max_G (G')^2$ *with* $U \neq V$.

Proof. (i) The subgroups $[G,G^2]$ and $(G')^2$ coincide modulo $\gamma_3(G)$. Since groups of exponent 2 are abelian, we have $G' \leqslant G^2$, which implies that $\gamma_3(G) \leqslant [G,G^2]$. On the other hand, $C_2(G) = G$ implies that $\gamma_3(G) \leqslant (G')^2$. We conclude that

$$[G,G^2] = [G,G^2]\gamma_3(G) = (G')^2\gamma_3(G) = (G')^2.$$

(ii) If $[x,G^2] = (G')^2$ then obviously $x \notin R$. On the other hand, if $[x,G^2] \neq (G')^2$ then $[x,G^2] < (G')^2$ by (i). Let $N = [x,G^2](G')^4$. Then N is a proper subgroup of $(G')^2$, and normal in G, since $[(G')^2,G] \leqslant (G')^4$ by (i) of Proposition 2.36. If we consider $U \max_G (G')^2$ containing N, then $x \in R(U) \subseteq R$. This proves the result.

(iii) By (i), $R(U)$ is a proper subgroup of G. On the other hand, we have

$$[G^2,G^2] \leqslant [G,G^2]^2[G,G^2,G] = (G')^4[(G')^2,G] = (G')^4.$$

Since $(G')^4 \leqslant U$, it follows that $G^2 \leqslant R(U)$.

(iv) Notice that G' is powerful by Theorem 2.18, so in particular $d((G')^2) \leqslant 2$. Hence we have $U \cap V = (G')^4 \leqslant W$, so the result follows from the definition of $R(W)$. □

The next result will allow us to complete easily the proof of Theorem 3.9 in the case when $p = 2$ and $C_2(G) = G$. Its proof is long and technical, and it requires a careful analysis of the relative positions of the subgroups $D(T)$ and $R(U)$, where $T \max_G G'$ and $U \max_G (G')^2$.

Proposition 3.13. *Let G be a finite 2-group with $d(G') = 2$ and $C_2(G) = G$. Then there exists $x \in G$ such that $G' = [x, G]$ and $(G')^2 = [x, G^2]$.*

Proof. We know by Remark 2.42 that $G' = [a, G] = \langle [a, b], [a, c] \rangle$ for some $a, b, c \in G$. If we set $H = \langle a, b, c \rangle$ then $H' = G'$, and the result immediately follows for G once it is proved for H, taking into account that $[G^2, G] = (G')^2$ by Lemma 3.12. Thus we may assume that $d(G) \leqslant 3$ and, by Remark 2.42, also that $(G')^2 \neq 1$.

In the remainder of the proof, let $Z/(G')^2$ be the centre of $G/(G')^2$. Observe that $|G : Z| > 4$, since otherwise the derived subgroup of $G/(G')^2$ is cyclic, and consequently G' is cyclic. Since, again by Lemma 3.12, we have $\Phi(G) = G^2 \leqslant Z$, it follows that $|G : G^2| = 8$ and that $Z = G^2$.

Write $D = \cup \{D_2(T) \mid T \max_G G'\}$. By Proposition 2.40 and Lemma 3.12, it suffices to show that $D \cup R$ does not cover the whole of G, since then any $x \in G \setminus (D \cup R)$ satisfies both $G' = [x, G]$ and $(G')^2 = [x, G^2]$. Since $G^2 \leqslant D_2(T), R(U)$ for all $T \max_G G'$ and $U \max_G (G')^2$, we can prove the non-covering property by working in the group G/G^2 of order 8. Thus, if we use the bar notation in this factor group, then we need to prove that $|\overline{D} \cup \overline{R}| \leqslant 7$. We do this by first determining the order of $\overline{D}$ and then analysing the position of the subgroups $R(U)$ with respect to D and among themselves. Before proceeding, observe that G' is powerful by Theorem 2.18, and so the sections $G'/(G')^2$ and $(G')^2/(G')^4$ are central in G by Proposition 2.36, since $C_2(G) = G$. Hence the conditions $T \max_G G'$ and $U \max_G (G')^2$ are equivalent in this case to $T \max G'$ and $U \max (G')^2$, respectively.

We claim that $|\overline{D}| = 4$ and that D is a (maximal) subgroup of G. Let us consider an arbitrary $T \max_G G'$, and observe that there are three choices for T, since $d(G') = 2$. First of all, note that $|\overline{D_2(T)}| = 2$, since $\log_2 |G : D_2(T)|$ is even and $D_2(T)$ is proper in G by Proposition 2.41. Thus $D_2(T)' = [D_2(T), G^2] \leqslant (G')^2$. Now let $S \max_G G'$ with $S \neq T$. Then $[D_2(S), D_2(T)] \leqslant S \cap T \leqslant (G')^2$, and as a consequence $\langle D \rangle' \leqslant (G')^2$. Also, if $D_2(S) = D_2(T)$ then $[D_2(T), G] \leqslant (G')^2$ and $D_2(T) \leqslant Z = G^2$. Hence $|\overline{D_2(T)}| = 1$, which is a contradiction. Thus $\overline{D}$ is the union of three different subgroups of order 2, and $|\overline{D}| = 4$. Since $D \subseteq \langle D \rangle \leqslant G$ and $\langle D \rangle' \neq G'$, it follows that D is a (maximal) subgroup of G, as claimed.

Now we start the analysis of the position of the subgroups of the form $R(U)$. Since G' is a 2-generator powerful group, we have $|(G')^2 : (G')^4| \leqslant 4$. Hence $(G')^2$ has at most 3 maximal subgroups, and the intersection of two different maximal subgroups is $(G')^4$. By Lemma 3.12, all the $R(U)$ are proper in G, and if none of them is maximal in G, we immediately get $|\overline{D} \cup \overline{R}| \leqslant 7$. The same conclusion holds if $R(U) = D$ whenever $R(U) \max G$. Thus we may assume that there exists $U \max_G (G')^2$ such that $R(U) \max G$, i.e. such that $|\overline{R(U)}| = 4$, and furthermore $R(U) \neq D$.

Then $|\overline{D} \cup \overline{R(U)}| = 6$, and we may also assume that there exists another $V \max_G (G')^2$ such that $R(V) \nsubseteq D \cup R(U)$. This implies in particular that $d((G')^2) = 2$, and $(G')^2$ has exactly 3 maximal subgroups. Also, since G' is powerful, the square map induces an isomorphism between $G'/(G')^2$ and $(G')^2/(G')^4$. As a consequence,

$$g \in G' \setminus (G')^2 \implies g^2 \in (G')^2 \setminus (G')^4, \tag{3.1}$$

and also all three maximal subgroups of $(G')^2$ are of the form T^2, where $T \max_G G'$.

Let W be the third maximal subgroup of $(G')^2$, apart from U and V. If $\overline{R(W)} = \overline{1}$ then, since $R(U) \cap R(V) \leqslant R(W)$ by Lemma 3.12, it follows that $|\overline{R(V)}| \leqslant 2$ and consequently $|\overline{D} \cup \overline{R}| \leqslant 7$. Hence we may assume that $|\overline{R(W)}| \geqslant 2$.

Now we consider two separate cases:

Case 1: $R(W) \leqslant R(U)$.

Again by Lemma 3.12, we get $R(W) = R(U) \cap R(W) < R(V)$, with proper inclusion since $R(V) \nleqslant R(U)$. In particular, $|\overline{R(W)}| = 2$ and $|\overline{R(V)}| = 4$, which implies that $|\overline{R}| = 6$.

Assume first that $D \cap R(U) \neq D \cap R(V)$. In this case we have $|\overline{D} \cap \overline{R}| \geqslant 3$ and hence $|\overline{D} \cup \overline{R}| \leqslant 7$, as desired.

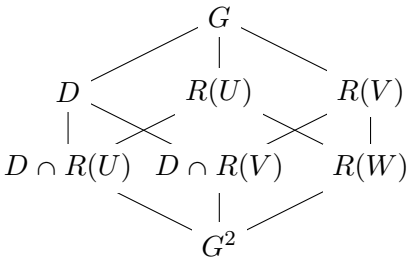

Figure 3.1: The case $D \cap R(U) \neq D \cap R(V)$.

Suppose now that $D \cap R(U) = D \cap R(V)$, so that this intersection coincides with $R(W)$. Now, by the fourth paragraph of the proof, $\overline{D}$ has three subgroups of order 2, which are all of the form $\overline{D_2(T)}$. Thus $R(W) = D_2(T)$ for some $T \max_G G'$.

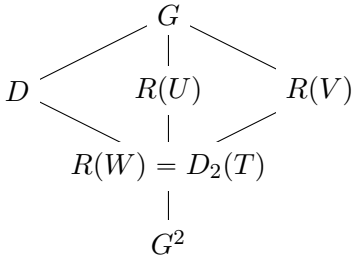

Figure 3.2: The case $D \cap R(U) = D \cap R(V)$.

Choose $g \in R(W) \setminus G^2$. Then $[g, G]$ is contained in T, but since $Z = G^2$, it is not contained in $(G')^2$. Since $G = \langle R(U), D \rangle$ and $[g, D] \leqslant D' \leqslant (G')^2$, there exists $h \in R(U)$ such that $[g, h] \in T \setminus (G')^2$. Now, we have

$$[g, h^2] \in [R(W), G^2] \leqslant [R(U), G^2] \cap [R(V), G^2] \leqslant U \cap V \leqslant (G')^4,$$

and, on the other hand,

$$[g, h^2] = [g, h]^2 [g, h, h],$$

where $[g, h]^2 \in T^2 \setminus (G')^4$ by (3.1), and $[g, h, h] \in [h, G'] \leqslant [h, G^2] \leqslant U$. Thus necessarily $U = T^2$. Since the same argument can be applied with V in the place of U, we deduce that $U = V$, which is a contradiction.

Case 2: $R(W) \nleqslant R(U)$.

We are going to prove that this case is impossible. Choose an element $x \in R(V) \setminus (D \cup R(U))$. Then $G = R(U) \cup xR(U)$. Since $R(W) \nleqslant R(U)$, there exists $y \in R(U)$ such that $xy \in R(W)$. Note that $y \notin G^2$, since otherwise $xy \in R(V) \cap R(W) \leqslant R(U)$. Now $[xy, x^2] = [y, x^2] \in W \cap U = (G')^4$, and then

$$[y, x]^2 = [y, x^2][y, x, x]^{-1} \in V,$$

since $[y, x, x] \in [G^2, x]$. By using that $[yx, y^2] = [x, y^2]$ and that $yx = (xy)^x \in R(W)$, we obtain in the same way that $[y, x]^2 \in U$. Hence $[y, x]^2 \in (G')^4$ and then, by (3.1), we get $[y, x] \in (G')^2$.

On the other hand, $x \notin D$ yields

$$G' = [x, G] = [x, \langle x \rangle R(U)] = [x, R(U)].$$

Since $y \notin G^2$ and $|\overline{R(U)}| = 4$, we can write $R(U) = \langle y, z, G^2 \rangle$ for some z. Now, since $[x, y] \in (G')^2$ and $[x, G^2] \leqslant (G')^2$, it follows that $G' = \langle [x, z], (G')^2 \rangle$. This implies that G' is cyclic, which is a contradiction. □

Example 3.14. Let $A = \langle a \rangle \times \langle b \rangle \times \langle v \rangle \cong C_4 \times C_4 \times C_4$ and $\langle u \rangle \cong C_4$. Define the semidirect product $U = \langle u \rangle \ltimes A$ via the automorphism

$$a^u = a^3 b^2, \qquad b^u = b, \qquad v^u = vba.$$

Let also $\langle x \rangle \cong C_4$ and define the group $G = \langle x \rangle \ltimes U$ via the automorphism

$$a^x = ab^2, \qquad b^x = b^3, \qquad u^x = ua^3, \qquad v^x = vb^3.$$

Then $G' = \langle a, b \rangle$ and $G^2 = \langle x^2, u^2, v^2 \rangle$, and the group G/G^2 has the same subgroup structure as the group in Figure 3.1.

Similar examples can be constructed showing that all lattices that we have in the other cases that we have considered in the proof of Proposition 3.13 are actually possible.

We can now proceed to prove Theorem 3.9 for the prime 2.

Theorem 3.15. *Let G be a finite 2-group, and assume that $d(G') \leqslant 2$. Then $G' = K_x(G)$ for a suitable $x \in G$.*

Proof. We may assume that $d(G') = 2$ and we write $C = C_2(G)$ for simplicity. Recall that G' is powerful by Theorem 2.18. We split the proof into two cases:

Case 1: $C \neq G$.

Let $T = \gamma_3(G)(G')^2$. We know from (iv) of Proposition 2.36 that $T \max_G G'$ and that it is the unique normal subgroup of G which is maximal in G'. Hence if $N \trianglelefteq G$ and $N < G'$ then $N \leqslant T$. On the other hand,

$$[G, C'] \leqslant [G, C, C] \leqslant [G', C] \leqslant (G')^2,$$

while $[G, G'] \nleqslant (G')^2$. It follows that $C' < G'$, and consequently $C' \leqslant T$.

Since T is the unique subgroup such that $T \max_G G'$, by Proposition 2.41, we have $G' = [x, G]$ for every $x \notin D_2(T)$. We are going to show that Lemma 2.27 can be applied

either with $L = G'$ and $N = T$ or with $L = T$ and $N = (G')^2$, depending on the values of some commutator subgroups. In the latter case, Corollary 2.25 will complete the proof.

Suppose first that $[G', C] \leqslant T^2$. Then we take $x \notin C$, which by Proposition 2.41 implies $x \notin D_2(T)$. Hence $G = \langle x \rangle C$ and $G'/T = \langle [x, y]T \rangle$ for some $y \in C$. Also, observe that $T/(G')^2 = \langle [x, [x, y]](G')^2 \rangle$. Now we have $[x, y, y] \in [G', C] \leqslant T^2$ and $[x, [x, y], [x, y]] \in [G', G'] \leqslant (G')^4$, since G' is powerful. Thus we are done in this case.

Therefore we assume that $[G', C] \nleqslant T^2$ in the remainder. Observe that T is powerful by Lemma 2.16 and hence $|(G')^2 : T^2| \leqslant |G' : T| = 2$ by Lemma 2.15. Since $[G', C]$ is contained in $(G')^2$ but not in T^2, we have $|(G')^2 : T^2| = 2$. Also $|T^2 : (G')^4| \leqslant 2$.

If $[T, G] \nleqslant T^2$ then since $G = \langle G \setminus C \rangle$ we can choose $x \notin C$ and $t \in T$ such that $(G')^2/T^2 = \langle [x, t]T^2 \rangle$. Since $[x, t, t] \in [(G')^2, G'] \leqslant (G')^8 \leqslant T^4$ and we can argue with the chief factor $T/(G')^2$ as in the case $[G', C] \leqslant T^2$, the result follows also in this case.

Suppose finally that $[T, G] \leqslant T^2$. Since $[G', C] \nleqslant T^2$ and

$$[G', D_2(T)] \leqslant [D_2(T), G, G] \leqslant [T, G] \leqslant T^2,$$

there exist $x \in C \setminus D_2(T)$ and $g \in G'$ such that $(G')^2/T^2 = \langle [x, g]T^2 \rangle$. Then $[x, g, g] \in [(G')^2, G'] \leqslant T^4$. On the other hand, there exists $y \in G$ such that $G'/T = \langle [x, y]T \rangle$. Since $C' \leqslant T$, we have $y \notin C$ and then $T/(G')^2 = \langle [x, y, y](G')^2 \rangle = \langle [x, y^2](G')^2 \rangle$. Now

$$[x, y^2, y^2] \in [T, G^2] \leqslant [T, G]^2[T, G, G] \leqslant [T, G]^2[T^2, G] \leqslant (G')^4,$$

which completes the proof in this case.

Case 2: $C = G$.

By Proposition 3.13, there exists $x \in G$ such that $G' = [x, G]$ and $(G')^2 = [x, G^2]$. Since $C = G$ implies by Proposition 2.36 that the sections $G'/(G')^2$ and $(G')^2/(G')^4$ are central in G, it follows from Lemma 2.26 that

$$G'/(G')^2 = K_{x(G')^2}(G/(G')^2)$$

and

$$(G')^2/(G')^4 = K_{x(G')^4}(G^2/(G')^4).$$

On the other hand, by Proposition 2.36, we have

$$[x, G^2, G^2] = [(G')^2, G^2] \leqslant (G')^8.$$

Hence we can apply Lemma 2.27 with $L = (G')^2$ and any $N \max_G (G')^2$, getting $(G')^2 \subseteq K_x(G)$. Now we are done by applying Corollary 2.25. □

Combining Theorem 3.10 and Theorem 3.15 we establish Theorem 3.9.

3.3 Derived subgroup with 3 or more generators

We now study groups with 3-generator derived subgroup. In this context, Rodney started addressing the easiest cases.

Theorem 3.16 ([69, Theorems A and B])**.** *Let G be a group with $d(G') = 3$. Suppose one of the following conditions holds.*

(i) *G is nilpotent of nilpotency class 2.*

(ii) *G is finite and G' is elementary abelian of order p^3.*

Then $G' = K(G)$.

Notice that Rodney's results in Theorem 3.16 involve only groups for which G' is abelian. Thus, Guralnick generalised these results to groups whose derived subgroup is an abelian and finite p-group with $p \geqslant 5$.

Theorem 3.17 ([25, Theorem B])**.** *Let G be a group and suppose G' is an abelian finite p-group with $p \geqslant 5$. If $d(G') \leqslant 3$, then $G' = K(G)$.*

Moreover, he found counterexamples showing that the result is false for $p = 2$ or $p = 3$, even if G' is abelian ([25], Example 3.5 and Example 3.6). In Theorem 3.18, as we have done in Theorem 3.9, we generalise Guralnick's result to finite p-groups in which G' need not be abelian (we will prove this result later on).

Theorem 3.18 ([32, Theorem A])**.** *Let G be a finite p-group with $p \geqslant 5$. If G' can be generated by 3 elements, then G' consists only of commutators.*

In this case, it is not true, in general, that there exists a fixed element $x \in G$ such that $G' = K_x(G)$, as we had in Theorem 3.9 or in Theorem 3.19 below. Indeed, let $G = F_3/\gamma_3(F_3)F_3^p$, where F_3 is the free group on 3 generators and $p \geqslant 3$ is a prime. Note that G' is 3-generator and that $|G : Z(G)| = p^3$. Now, if $x \in Z(G)$, then $K_x(G) = 1$, and if $x \notin Z(G)$, then $|G : C_G(x)| \leqslant p^2$ since $\langle Z(G), x\rangle \leqslant C_G(x)$. In particular, $|K_x(G)| = |G : C_G(x)| \leqslant p^2$.

On the other hand, as shown in Example 2.20, G' need not be powerful if it is generated by 3 elements. However, we will see that the finite p-groups with 3-generator non-powerful derived subgroup are a very special type of p-group, and with this, the proof of the result for such groups will follow easily. Thus, the theory of powerful groups will be essential also in this case.

Regarding groups whose derived subgroup is generated by more than 3 elements, Macdonald ([59, Exercise 5, page 78]) and Kappe and Morse ([47, Example 5.4]) showed that for every prime p there exist finite p-groups with 4-generator abelian derived subgroup such that $G' \neq K(G)$. These examples show that the property may fail if the derived subgroup has more than 3 generators. Therefore, with Theorem 3.9 and Theorem 3.18, we close the gap between the case when G' is abelian and can be generated by 3 elements and the case when G' is generated by more than 3 elements. With this, the study of the condition $G' = K(G)$ in terms of the number of generators of the derived subgroup is complete for finite p-groups.

A natural continuation to Theorems 3.9 and 3.18 would be considering finite p-groups with 4-generator derived subgroup. This has been done recently in [46], where a classification,, up to isoclinism (see [30]), of finite p-groups such that $|G'| = p^4$, $(G')^p = 1$ and $G' \neq K(G)$ is given.

In Theorem 3.19 we show that with some additional restrictions, groups with $d(G') \geqslant 4$ do satisfy the desired equality.

Recall that the action of a finite p-group G on a normal subgroup N of G is *uniserial* if

$$|[N, G, \overset{i}{\ldots}, G] : [N, G, \overset{i+1}{\ldots}, G]| \leqslant p$$

for every $i \geqslant 0$.

Theorem 3.19 ([32, Theorem B])**.** *Let G be a finite p-group and write $d = \log_p |G' : (G')^p|$. If $d \leqslant p-1$ and the action of G on G' is uniserial modulo $(G')^p$, then there exists $x \in G$ such that $G' = \{[x, g] \mid g \in G\}$.*

Before proving Theorem 3.18 we will first establish Theorem 3.19 in Section 3.3.1, as it is required in the proof of Theorem 3.18. We will then split the proof of Theorem 3.18 into two parts, dealing separately in Sections 3.3.2 and 3.3.3 with the case in which G' is powerful and the general case, respectively.

3.3.1 Groups acting uniserially on their derived subgroup

For a uniserial action of a group G on G', the so-called *two-step centralisers* are defined as the centralisers in G of the factors $\gamma_i(G)/\gamma_{i+2}(G)$, where $i \geqslant 2$ and $\gamma_{i+1}(G) \neq 1$ (see [10]). In view of the statement of Theorem 3.19, we will define the following subgroups, which are just the two-step centralisers modulo $(G')^p$.

Definition 3.20. Let G be a finite p-group such that the action of G on G' is uniserial modulo $(G')^p$. Then, we define

$$S_i(G) = C_G(\gamma_i(G)(G')^p/\gamma_{i+2}(G)(G')^p)$$

for every $i \geqslant 2$ such that $\gamma_{i+1}(G) \not\leqslant (G')^p$.

Remark 3.21. In the situation above, the subgroups $S_i(G)$ are all maximal in G since $|\gamma_i(G)(G')^p : \gamma_{i+2}(G)(G')^p| = p^2$ and $[\gamma_i(G)(G')^p, G] \not\leqslant \gamma_{i+2}(G)(G')^p$.

With this in mind, we can now establish Theorem 3.19.

Proof of Theorem 3.19. If $d = 1$, then G' is cyclic and the result follows from Theorem 3.6, so assume $d \geqslant 2$ (and in particular $p \geqslant 3$). For the sake of simplicity we will write $G_i = \gamma_i(G)(G')^p$, so that

$$(G')^p = G_{d+2} \leqslant G_{d+1} \leqslant \ldots \leqslant G_3 \leqslant G_2 = G'$$

is a series from G' to $(G')^p$ such that $|G_i : G_{i+1}| = p$ for all $2 \leqslant i \leqslant d+1$. Note that if $N \max_G G'$ then $G_3 \leqslant N$. Therefore, $N = G_3$ and G_3 is the unique subgroup which is maximal in G' and normal in G. Moreover, note that the index of $D_2(G_3)$ in G is strictly greater than p by Proposition 2.41. Note also that there are only $d - 1 \leqslant p - 2$ two-step centralisers, which are all maximal by Remark 3.21. Thus, we can take

$$x \in G \backslash (D_2(G_3) \cup S_2(G) \cup \ldots \cup S_d(G)). \tag{3.2}$$

By Proposition 2.40 we have $G' = [x, G]$ and since $S_2(G)$ is maximal in G we have $G' = [x, G] = [x, \langle x \rangle S_2(G)] = [x, S_2(G)]$. In particular $G'/G_3 = \langle [x, g_1]G_3 \rangle$ for some $g_1 \in S_2(G)$. Furthermore, since $x \notin S_i(G)$ for $2 \leqslant i \leqslant d$, we also have $G_{i+1}/G_{i+2} = \langle [x, g_i]G_{i+2} \rangle$ for a suitable $g_i \in G_i$. It follows from Lemma 2.26 and Corollary 2.25 that $G'/(G')^p \subseteq K_{x(G')^p}(G/(G')^p)$.

Recall that $\gamma_{d+2}(G) \leqslant (G')^p$, and since $d \leqslant p-1$, it follows that $\gamma_{p-1}(G') \leqslant \gamma_{2(p-1)}(G) \leqslant \gamma_{2d}(G)$. Thus, since $2d \geqslant d+2$ we have $\gamma_{p-1}(G') \leqslant (G')^p$, so that G' is potent. In this case the power map from $G'/(G')^p$ to $(G')^p/(G')^{p^2}$ induced from the map $x \mapsto x^p$ need not be a homomorphism. However, we can restrict its domain and

codomain in order for it to be so. We claim that the map from G_i/G_{i+1} to G_i^p/G_{i+1}^p sending gG_{i+1} to $g^pG_{i+1}^p$ is an epimorphism for every $2 \leqslant i \leqslant d+1$.

Take $x, y \in G_i$. By the Hall-Petresco identity we have

$$(xy)^p = x^p y^p c_2^{\binom{p}{2}} c_3^{\binom{p}{3}} \cdots c_p$$

with $c_j \in \gamma_j(G_i)$. Obviously if $2 \leqslant j \leqslant p-1$ then $c_j^{\binom{p}{j}} \in G_{i+1}^p$. Besides, if $j = p$, since $G_i \leqslant G'$, we have

$$c_p \in [G_i, \overset{p}{\ldots}, G_i] \leqslant [G_i, G, \overset{2(p-1)}{\ldots}, G] \leqslant G_{i+1}^p,$$

where the last inequality holds since by Lemma 2.14 we have

$$|G_i : G_{i+1}^p| = |G_i : G_i^p||G_i^p : G_{i+1}^p| \leqslant p^{d+1}$$

and $d+1 \leqslant 2(p-1)$. This proves that the map is a homomorphism. Moreover, since G' is potent it follows that G_i is power abelian, so the map must be an epimorphism. The claim is proved.

Thus, from Lemma 2.14 it follows that we have a series

$$((G')^p)^p = G_{d+2}^p \leqslant G_{d+1}^p \leqslant \cdots \leqslant G_3^p \leqslant G_2^p = (G')^p$$

in which each factor G_{i+1}^p/G_{i+2}^p has order less than or equal to p and is generated by the image of $[x, g_i]^p$ for every $1 \leqslant i \leqslant d$. Now, in order to apply Lemma 2.29 let us prove that

$$[x, g_i]^p \equiv [x, g_i^p] \pmod{G_{i+2}^p}$$

for every i. Assume first $i = 1$. We will use again the Hall-Petresco identity so that

$$[x, g_1]^p = [x, g_1^p] c_2^{\binom{p}{2}} c_3^{\binom{p}{3}} \cdots c_p$$

with $c_j \in \gamma_j(\langle [x, g_1], g_1 \rangle) \leqslant [G, S_2(G), \overset{j}{\ldots}, S_2(G)]$. If $2 \leqslant j \leqslant p-1$ then $c_j^{\binom{p}{j}} \in G_3^p$. If $j = p$, we have

$$c_p \in [G, S_2(G), \overset{p}{\ldots}, S_2(G)] \leqslant [G_4, S_2(G), \overset{p-2}{\ldots}, S_2(G)].$$

Lemma 2.14 yields $|G_4 : G_3^p| \leqslant p^{d-1}$, and since $d-1 \leqslant p-2$, we conclude $c_p \in G_3^p$. For $i \geqslant 2$ we have $g_i \in G'$, so the claim follows more easily applying the same method.

Now, $d \leqslant p-1 \leqslant p^2-p-1$, so we apply Lemma 2.29 with $j = 1$ and we get $(G')^p \subseteq K_x(G)$. Since $G'/(G')^p \subseteq K_{x(G')^p}(G/(G')^p)$, we conclude by Corollary 2.25. □

Remark 3.22. If the exponent of G' is p, that is, if $(G')^p = 1$, then, following the same method, Theorem 3.19 can be stated for $d \leqslant p+1$. Indeed, if G is the union of $p+1$ proper subgroups, then all of them must be maximal. Hence, since $|G : D_2(G_3)| > p$, we can take x as in (3.2) and conclude in the same way as in the first paragraph of the proof.

3.3.2 Groups with 3-generator and powerful derived subgroup

In order to prove Theorem 3.24 we first need the following technical lemma, which will be very helpful when using induction on the order of the group.

Lemma 3.23. *Let G be a finite p-group with $p \geqslant 5$, G' powerful and $d(G') = 3$. Assume there exist $x, u, v \in G$ such that $G' = \langle [u,v], [x,u], [x,v] \rangle$, $G' \neq [x,G]$ and $[x,G,G] \leqslant (G')^p$. Then, there exists a family of proper subgroups of G such that $[x,G](G')^p$ equals the union of their derived subgroups. Moreover, each of these derived subgroups is powerful.*

Proof. Consider the subgroups $H_i = \langle x, uv^i, v^p \rangle$ for $0 \leqslant i \leqslant p-1$ and $H_p = \langle x, v, u^p \rangle$. Let us prove that $H_i' = \langle [x, uv^i] \rangle (G')^p$ for $0 \leqslant i \leqslant p-1$ and that $H_p' = \langle [x,v] \rangle (G')^p$.

Suppose first $i \neq p$. Since $G' = \langle [u,v], [x,u], [x,v] \rangle$ and $G' \neq [x,G]$, we have $|G' : [x,G](G')^p| = p$, and since $[x,G,G] \leqslant (G')^p$, the map

$$\begin{array}{ccc} G & \longrightarrow & [x,G](G')^p/(G')^p \\ g & \longmapsto & [x,g](G')^p \end{array}$$

is a homomorphism. Therefore, we can write

$$G' = \langle [u,v], [x,uv^i], [x,v] \rangle.$$

Thus, since G' is powerful, we have

$$(G')^p = \langle [u,v]^p, [x,uv^i]^p, [x,v]^p \rangle.$$

The subgroups $[x,G](G')^p$ and $\langle [x,v] \rangle (G')^p$ are normal in G since $[x,G,G] \leqslant (G')^p$, so since $p \geqslant 5$, taking $k = 0$ in Lemma 2.28 it follows that

$$[u,v]^p \equiv [uv^i, v^p] \pmod{([x,G](G')^p)^p}$$

and

$$[x,v]^p \equiv [x,v^p] \pmod{(G')^{p^2}}.$$

Hence,

$$(G')^p = \langle [uv^i, v^p], [x,v^p], [x,uv^i]^p \rangle \leqslant H_i',$$

so that $\langle [x,uv^i] \rangle (G')^p = H_i'$, as asserted. Similar arguments imply $H_p' = \langle [x,v] \rangle (G')^p$.

It is easy to see now that $[x,G](G')^p = \bigcup_{i=0}^{p} H_i'$ (just observe that the H_i' are precisely the subgroups between $[x,G](G')^p$ and $(G')^p$). Finally, notice that $|H_i' : (G')^p| = p$ for every i, so since $(G')^p$ is powerfully embedded in G', it follows from [48, Lemma 11.7] that H_i' is powerful. Thus, the proof is complete. □

We are now in a position to prove Theorem 3.18 in the case that G' is powerful.

Theorem 3.24. *Let G be a finite p-group with G' powerful, $d(G') \leqslant 3$ and $p \geqslant 5$. Then, $G' = K(G)$.*

Proof. We proceed by induction on the order of G. For $d(G') \leqslant 2$ the result follows from Theorem 3.6 and Theorem 3.9. Now assume that $d(G') = 3$ and note that we have $|G' : (G')^p| = p^3$. We will consider three different cases depending on the position of the subgroup $\Gamma = (G')^p \gamma_3(G)$.

Case 1. $|G' : \Gamma| = p$.

If $|\Gamma : \gamma_4(G)(G')^p| = p$, then the action of G on G' is uniserial modulo $(G')^p$ and the result follows from Theorem 3.19.

Assume then $\gamma_4(G) \leqslant (G')^p$. If $G' = K_x(G)$ for some $x \in G$, then, of course, we are done, so assume $G' \neq K_x(G)$ for every $x \in G$. We claim that there exist $u, v \in G$ such that $G' = \langle [u,v], [u,v,u], [u,v,v] \rangle$. For that purpose we can suppose that $(G')^p = 1$. As seen in the proof of Theorem 3.19, the subgroup Γ is the unique subgroup such that $\Gamma \max_G G'$. Since both $C_2(G)$ and $D_2(\Gamma)$ are proper subgroups of G by Propositions 2.36 and 2.43 respectively, we can take $u \notin C_2(G) \cup D_2(\Gamma)$. Then, $G' = [u, G]$ by Proposition 2.40 and $C_{G/\Gamma}(u\Gamma) \neq G/\Gamma$. Let us write $C^*/\Gamma = C_{G/\Gamma}(u\Gamma)$.

Since $u \notin C_2(G)$ we have $[u, G'] \neq 1$. If $[u, G'] = \Gamma$, then, we can find a series of normal subgroups of G from G' to $(G')^p$ such that all factors have order p and are generated by images of elements of the form $[u, g]$ for some suitable $g \in G$. Thus, Lemma 2.29 implies $G' = K_u(G)$, which is a contradiction. Therefore, we have $|[u, G']| = p$ and hence $C_G(G'/[u, G']) \neq G$. Take thus $v \in G \backslash (C_G(G'/[u, G']) \cup C^*)$. Then, $G'/\Gamma = \langle [u, v]\Gamma \rangle$ (because $v \notin C^*$), and again, as we have seen for u, we also have $|[v, G']| = p$. It follows that $[u, v, u], [u, v, v] \neq 1$. Furthermore, since $v \notin C_G(G'/[u, G'])$, we have $[u, G'] \neq [v, G']$, and we conclude that $G' = \langle [u, v], [u, v, u], [u, v, v] \rangle$. This proves the claim.

Remove now the assumption of $(G')^p = 1$ and observe that $[[u, v], G, G] \leqslant (G')^p$, so we are in the situation of Lemma 3.23. It follows then that Γ is the union of the derived subgroups of some proper subgroups of G. These derived subgroups are all powerful, and since $d(G') = 3$, they all can be generated by 3 elements. So, by induction, $\Gamma \subseteq K(G)$.

Take now $g \in G' \backslash \Gamma$ arbitrary. We claim that g is a commutator modulo Γ^{p^i} for every $i \geqslant 0$ (and hence that g is a commutator). We proceed by induction on i. Clearly, we have $g = [x, y]z$ for some $x, y \in G$, $z \in \Gamma$, so the case $i = 0$ is satisfied. Assume then that $i \geqslant 1$ and $g = [x, y]z_1$ where $x, y \in G$ and $z_1 \in \Gamma^{p^{i-1}}$.

Note that $G'/\Gamma = \langle [x, y]\Gamma \rangle$, so since $[\Gamma, G] \leqslant (G')^p$, we have

$$\Gamma/(G')^p = \{[x, y, h](G')^p \mid h \in G\}.$$

Besides, since G' is powerful, the power map from $G'/(G')^p$ to $(G')^{p^{i-1}}/(G')^{p^i}$ is an epimorphism, so that $\Gamma^{p^{i-1}}/(G')^{p^i} = \{[x, y, h]^{p^{i-1}}(G')^{p^i} \mid h \in G\}$. By Lemma 2.28 we have

$$\Gamma^{p^{i-1}}/(G')^{p^i} = \{[x, y, h^{p^{i-1}}](G')^{p^i} \mid h \in G\}.$$

Thus,

$$g = [x, y][x, y, h^*]z_2 = [x^{h^*}, y^{h^*}]z_2$$

for some $h^* \in G$ and $z_2 \in (G')^{p^i}$. We rewrite, in order to simplify the notation, x instead of x^{h^*} and y instead of y^{h^*}, so that $g = [x, y]z_2$.

Note again that $G'/\Gamma = \langle [x, y]\Gamma \rangle$, so it follows that

$$(G')^{p^i}/\Gamma^{p^i} = \langle [x, y]^{p^i}\Gamma^{p^i} \rangle.$$

Therefore,

$$g = [x, y][x, y]^{jp^i} z_3 = [x, y]^{1+jp^i} z_3$$

with $j \geqslant 0$ and $z_3 \in \Gamma^{p^i}$. Now, the last theorem in [39] asserts that $K(G)^s \subseteq K(G)$ for all integer s such that $p \nmid s$. Therefore, there exist $x', y' \in G$ such that $[x, y]^{1+jp^i} = [x', y']$, so $g = [x', y']z_3$ with $z_3 \in \Gamma^{p^i}$, as claimed.

Case 2. $|G' : \Gamma| = p^2$.

Write $D = \cup\{D_2(U) \mid U \max_G G'\}$. We first claim that $C_2(G) \cup D \neq G$. On the one hand, as seen before, $\Gamma \leqslant N$ for all $N \max_G G'$, and since $|G' : \Gamma| = p^2$, there are exactly $p + 1$ subgroups between G' and Γ, say $U_1, \dots, U_{p+1}$. Furthermore, since they are central over Γ, they are all normal in G. Thus, $D = D_2(U_1) \cup \cdots \cup D_2(U_{p+1})$. In addition, it follows from Proposition 2.41 that $|G : D_2(U_i)| \geqslant p^2$ for every i.

On the other hand, observe again that $C_2(G) \neq G$. As a consequence, if we write $|G| = p^n$, then we have

$$\begin{aligned} |C_2(G) \cup D| &\leqslant |C_2(G)| + |D| \leqslant \sum_{i=1}^{p+1} |D_2(U_i)| + |C_2(G)| \\ &\leqslant (p+1)p^{n-2} + p^{n-1} = 2p^{n-1} + p^{n-2} < p^n, \end{aligned}$$

as we wanted. Take now $x \notin C_2(G) \cup D$. Since $x \notin D$ we have $G'/\Gamma = [x, G]\Gamma/\Gamma$ by Proposition 2.40, and since $x \notin C_2(G)$ we have $\Gamma/(G')^p = [x, G'](G')^p/(G')^p$. Thus, since all subgroups between G' and Γ are central and hence normal in G, we can construct a series from G' to $(G')^p$ where all factors have order p and are generated by images of commutators of the form $[x, g]$ with $g \in G$. Again, the result follows from Lemma 2.29.

Case 3. $\gamma_3(G) \leqslant (G')^p$.

If $G' = [x, G](G')^p$ for some x, again, all the subgroups between G' and $(G')^p$ are normal in G, so we could construct a series from G' to $(G')^p$ in such a way that we would be done by Lemma 2.29. Therefore, assume $[x, G](G')^p < G'$ for every $x \in G$. By Theorem 3.16 the result is satisfied for $G/(G')^p$, so we have $G' = \bigcup_{x\in G}[x, G](G')^p$. Thus, it suffices to prove that $[x, G](G')^p \subseteq K(G)$ for every $x \in G$.

Suppose first $|[x, G](G')^p : (G')^p| = p$. We claim that there always exists $y \in G$ such that $[x, G](G')^p \leqslant [y, G](G')^p \max G'$. For that purpose, we assume $(G')^p = 1$. Note that $|G'/[x, G]| = p^2$, so by Theorem 3.9, there exists $u \in G$ such that $G'/[x, G] = [u, G][x, G]/[x, G]$. Hence $G' = [u, G][x, G]$ with $|[u, G]| = p^2$. Observe that $C_G(u), C_G(x) \neq G$, so take $y \notin C_G(u) \cup C_G(x)$. Thus, $[x, G] = \langle[x, y]\rangle$, and $[u, y] \neq 1$. If $[u, y] \in \langle[x, y]\rangle$, then $[x, y] \in [u, G]$, a contradiction. Observe that $[x, y], [u, y] \in [y, G]$ though, so $|[y, G]| = p^2$. Since $[x, G] \leqslant [y, G]$, the claim is proved.

Hence, we only have to consider the case $|[x, G](G')^p : (G')^p| = p^2$. We claim now that there exist $u, v \in G$ such that $G' = \langle[u, v], [x, v], [x, u]\rangle$. Assume again that $(G')^p = 1$. Since $|[x, G]| = |\{[x, g] \mid g \in G\}| = p^2$, we have $|G : C_G(x)| = p^2$, and we can consider a maximal subgroup M such that $C_G(x) < M < G$. Observe that $G' = [G, G] = [G, M]$, $G = \langle G\backslash M\rangle$ and $M = \langle M\backslash C_G(x)\rangle$. Hence, there exist $u \in G\backslash M$ and $v \in M\backslash C_G(x)$ such that $[u, v] \notin [x, G]$. Furthermore, $[x, G] = \langle[x, u], [x, v]\rangle$, so $G' = \langle[u, v], [x, u], [x, v]\rangle$, as claimed.

Remove now the assumption of $(G')^p = 1$ and note that we are in the situation of Lemma 3.23 since $[x, G, G] \leqslant \gamma_3(G) \leqslant (G')^p$. Hence we have $[x, G](G')^p \subseteq K(G)$, as we wanted. □

Remark 3.25. Case 2 can be generalised for $p \geqslant 3$ using a slightly different version of Lemma 2.29, but one must be more selective in the choice of x.

3.3.3 Groups with 3-generator but non-powerful derived subgroup

As said before, G' need not be powerful if it is generated by 3 elements. We will start, hence, analyzing which kind of groups may arise when G' is non-powerful. Actually, we will see that in such a case, $G/(G')^p$ must be a very special kind of p-group, namely, a $\mathrm{CF}(m,p)$-group. These groups are a generalisation of groups of maximal class and were introduced by Blackburn in [10]. They are defined as follows.

Definition 3.26. Let $m \geqslant 3$. A finite p-group G is said to be a $\mathrm{CF}(m,p)$-*group* if the nilpotency class of G is $m-1$ and the action of G on G' is uniserial.

In particular, if G is a $\mathrm{CF}(m,p)$-group, then $|G'| = p^{m-2}$. We next define the degree of commutativity on $\mathrm{CF}(m,p)$-groups exactly in the same way as for groups of maximal class (compare [10, Page 57]).

Definition 3.27. Let G be a $\mathrm{CF}(m,p)$-group. The *degree of commutativity* of G is defined as

$$\max\{k \leqslant m-2 \mid [G_i, G_j] \leqslant G_{i+j+k} \text{ for all } i,j \geqslant 1\},$$

where $G_1 = S_2(G)$ and $G_i = \gamma_i(G)$ for all $i \geqslant 2$.

Lemma 3.29 below shows that if G' is non-powerful, then G is a very particular group, namely a $\mathrm{CF}(6,p)$-group modulo $(G')^p$. The key part of the proof is the following lemma due to Blackburn.

Lemma 3.28 ([10, Theorem 2.11])**.** *Let G be a $\mathrm{CF}(m,p)$-group with m odd and $5 \leqslant m \leqslant 2p+1$. Then G has degree of commutativity greater than 0.*

Lemma 3.29. *Let G be a finite p-group with $p \geqslant 3$, $d(G') = 3$ and G' non-powerful. Then $G/(G')^p$ is a $\mathrm{CF}(6,p)$-group.*

Proof. Clearly we can assume $(G')^p = 1$ and $G'' \neq 1$. Thus, the Frattini subgroup of G' is G'', and since $d(G') = 3$, then $|G' : G''| = p^3$. Note that $G'' \leqslant \gamma_4(G)$, so the only possibilities for $\gamma_3(G)$ are $|G' : \gamma_3(G)| = p^2$ or $|G' : \gamma_3(G)| = p$.

Suppose first, for a contradiction, that $|G' : \gamma_3(G)| = p^2$. Then, since $G'' \leqslant \gamma_4(G)$ and $|G' : G''| = p^3$ we have $G'' = \gamma_4(G)$. In addition, G' has 2 generators modulo $\gamma_3(G)$, which implies that $|G'' : \gamma_5(G)| = p$ (recall that $(G')^p = 1$). Consider the subgroup $S_3(G)$ and recall it is maximal by Remark 3.21. In the same way as in Case 2 of Theorem 3.24, it can be seen that there are only $p+1$ maximal subgroups of G' that are normal in G. Hence, making the same computations, it follows that $D \cup S_3(G) \neq G$, where $D = \cup\{D_2(U) \mid U \max_G G'\}$.

Thus, we can pick $x \in G \backslash (D \cup S_3(G))$, and we have

$$G' = [x, G] = [x, \langle x \rangle S_3(G)] = [x, S_3(G)].$$

We can then find $y, z \in S_3(G)$ such that $G' = \langle [x,y], [x,z], \gamma_3(G) \rangle$. We write $a = [x,y]$ and $b = [x,z]$ for simplicity. Thus, $\gamma_4(G) = \langle [a,b], \gamma_5(G) \rangle$, and we write, again for simplicity, $d = [a,b]$.

On the one hand,

$$[b,y]^x = [b[b,x], ya^{-1}] \equiv [b,y]d \pmod{\gamma_5(G)},$$

so that $[b,y,x] \equiv d \pmod{\gamma_5(G)}$. Similarly we get

$$[z,a]^x \equiv [z,a]d \pmod{\gamma_5(G)}$$

and so $[z,a,x] \equiv d \pmod{\gamma_5(G)}$. In particular $[b,y],[z,a] \notin \gamma_4(G)$, and since the quotient $\gamma_3(G)/\gamma_4(G)$ is of order p, we have $[z,a] \equiv [b,y]^i \pmod{\gamma_4(G)}$ for some $1 \leqslant i \leqslant p-1$. Note, however, that

$$[z,a,x] \equiv [[b,y]^i,x] \equiv [b,y,x]^i \equiv d^i \pmod{\gamma_5(G)},$$

so we get $i = 1$ and thus

$$1 \neq [b,y] \equiv [z,a] \pmod{\gamma_4(G)}. \tag{3.3}$$

On the other hand, we have $[G', S_3(G)'] \leqslant [G', S_3(G), S_3(G)] \leqslant \gamma_5(G)$. Let Z be the subgroup of G defined by $Z/\gamma_5(G) = Z(G'/\gamma_5(G))$. We have $|G' : Z| \geqslant p^2$, and since $[G', \gamma_3(G)] \leqslant \gamma_5(G)$, we get $Z = \gamma_3(G)$. In particular, we obtain $S_3(G)' \leqslant \gamma_3(G)$, and the nilpotency class of $S_3(G)$ is less than or equal to 2. Now,

$$[y,z]^x = [ya^{-1}, zb^{-1}] \equiv [y,z][b,y][z,a]d \pmod{\gamma_5(G)},$$

so that $[y,z,x] \equiv [b,y][z,a]d \pmod{\gamma_5(G)}$. This is a contradiction, since (3.3) and $p > 2$ implies $[b,y][z,a] \in \gamma_3(G)\backslash\gamma_4(G)$, but $[y,z,x], d \in \gamma_4(G)$ as $S_3(G)' \leqslant \gamma_3(G)$.

Therefore we must have $|G' : \gamma_3(G)| = p$. Thus

$$G'' = [G', G'] = [G', \gamma_3(G)] \leqslant \gamma_5(G),$$

and since $|G' : G''| = p^3$, we have $|\gamma_3(G) : \gamma_4(G)| = |\gamma_4(G) : \gamma_5(G)| = p$ and $G'' = \gamma_5(G)$. Let us write $\overline{G} = G/\gamma_7(G)$. Note that

$$\gamma_3(G') = [G'', G'] = [\gamma_5(G), G'] \leqslant \gamma_7(G),$$

so $\overline{\gamma_3(G')} = \overline{1}$ and since $d(\overline{G}') = 3$, then $d(\overline{G}'') \leqslant 2$. Indeed, we can write $G' = \langle a,b,c\rangle$ with $a \in G'\backslash\gamma_3(G)$, $b \in \gamma_3(G)\backslash\gamma_4(G)$ and $c \in \gamma_4(G)\backslash\gamma_5(G)$, and so the generators of $\overline{G}''$ are $\overline{[a,b]} \in \gamma_5(\overline{G})$ and $\overline{[a,c]} \in \gamma_6(\overline{G})$ (note that $\overline{[b,c]} \in \gamma_7(\overline{G}) = \overline{1}$). Hence $|\gamma_5(\overline{G}) : \gamma_6(\overline{G})| = p$ and $|\gamma_6(\overline{G})| \leqslant p$.

If $|\gamma_6(\overline{G})| = \overline{1}$ then $\gamma_6(G) = \gamma_7(G) = 1$ and we are done, so assume $|\gamma_6(\overline{G})| = p$. In this way, $\overline{G}$ is a CF$(7,p)$-group, and since $p \geqslant 3$, by Lemma 3.28 it follows that the degree of commutativity of $\overline{G}$ is greater than 0. In particular we have $\overline{G}'' = [\gamma_2(\overline{G}), \gamma_3(\overline{G})] \leqslant \gamma_6(\overline{G})$, which is a contradiction. The lemma follows. □

With all this, the second part of the proof of Theorem 3.18 follows easily.

Theorem 3.30. *Let G be a finite p-group with G' non-powerful, $d(G') = 3$ and $p \geqslant 5$. Then, $G' = K(G)$.*

Proof. By Lemma 3.29 the action of G on G' is uniserial modulo $(G')^p$ and, in addition, $|G' : (G')^p| = p^4 \leqslant p^{p-1}$ since $p \geqslant 5$. The result follows directly from Theorem 3.19. □

Thus, combining Theorem 3.24 and Theorem 3.30 we establish Theorem 3.18.

Chapter 4

Lower central words and general outer commutator words

Much less is known about Problem 1.2 for general outer commutator words than for the commutator word. All the results that one can find in the literature for these words consist of generalisations of some of the theorems that work for the commutator word to lower central words. Following this line of thinking, we will generalise, to the extent possible, the results we have proved in the previous chapter to lower central words. Nevertheless, for outer commutator words in general, even if we will only consider groups with cyclic verbal subgroup, the results that we obtain are less satisfactory, as we will not go further than the second derived word.

As we have seen, the equality $G' = K(G)$ works particularly well for finite p-groups. For this reason, and in view of Proposition 1.3 as well, we will continue working with finite p-groups.

We will start, as in the previous chapter, by dealing separately with different cases, depending on the number of generators of the verbal subgroup $\gamma_r(G)$: in Section 4.1 we study finite p-groups with $\gamma_r(G)$ cyclic for some $r \geqslant 2$, while in Section 4.2 finite p-groups with $d(\gamma_r(G)) = 2$ for some $r \geqslant 2$ are studied. Finally, in Section 4.3, outer commutator words in general are considered.

4.1 Lower central words with cyclic verbal subgroup

The first result for lower central words was due to Kappe in [44], where she, among other results, generalised Macdonald's counterexamples in Theorem 3.5.

Theorem 4.1 ([44, Theorem 1])**.** *Let $r \geqslant 2$. For any $n \in \mathbb{N}$, there exists a group G in which $\gamma_r(G)$ is cyclic and generated by no set of less than n γ_r-values.*

Based on Kappe's work in [44], Dark and Newell generalised Rodney's results in Theorem 3.6 from commutator words to lower central words.

Theorem 4.2 ([12, Theorems 4 and 5])**.** *Let G be a group and $r \geqslant 2$. If $\gamma_r(G)$ is cyclic and either G is nilpotent or $\gamma_r(G)$ is infinite, then $\gamma_r(G)$ consists only of γ_r-values.*

As with Theorem 3.6, once we show that Theorem 4.2 works for groups with $\gamma_r(G)$ infinite, we can assume that G is a finite p-group by Proposition 1.3. For such groups, we will give an alternative simpler proof than that of [12]. In particular we will prove the case $p = 2$ in Theorem 4.5 below, which was omitted in [12] since it was pointed out to be very technical. In fact, even if Theorem 4.5 can be modified so that it works for all primes, we will prove the case in which p is odd separately in Theorem 4.4, as the proof turns out to be much shorter in this case. First, however, we need the following simple but very helpful lemma.

Lemma 4.3. *Let N be a cyclic normal subgroup of a group G. Then, $[N, G'] = 1$.*

Proof. Since N is cyclic, the automorphism group $\mathrm{Aut}(N)$ of N is abelian. Hence, $G/C_G(N)$ is abelian as well, which implies that $G' \leqslant C_G(N)$. □

Theorem 4.4. *Let G be a finite p-group with p odd and $\gamma_r(G)$ cyclic. Then there exist $x_1, \dots, x_{r-1} \in G$ such that*

$$\gamma_r(G) = \{[x_1, \dots, x_{r-1}, g] \mid g \in G\}.$$

Proof. Let $\gamma_r(G) = \langle [x_1, \dots, x_r] \rangle$ with $x_1, \dots, x_r \in G$. Then,

$$\gamma_r(G)^{p^k} = \langle [x_1, \dots, x_r]^{p^k} \rangle$$

for every $k \geqslant 1$. The Hall-Petresco identity gives

$$[x_1, \dots, x_r]^{p^k} = [x_1, \dots, x_r^{p^k}] c_2^{\binom{p^k}{2}} \cdots c_{p^k}$$

with $c_i \in \gamma_i(\langle [x_1, \dots, x_r], x_r \rangle)$. When $i < p^k$, we have $c_i \in \gamma_{r+i-1}(G) \leqslant \gamma_r(G)^{p^{i-1}}$, and so $c_i^{\binom{p^k}{i}} \in \gamma_r(G)^{p^{k+1}}$ since $p \geqslant 3$. If $i = p^k$, then $c_{p^k} \in \gamma_{r+p^k-1}(G) \leqslant \gamma_r(G)^{p^{p^k-1}} \leqslant \gamma_r(G)^{p^{k+1}}$. Therefore,

$$\gamma_r(G)^{p^k} = \langle [x_1, \dots, x_r^{p^k}] \rangle$$

for every $k \geqslant 0$. Moreover, since $[x_1, \dots, x_r^{p^k}, G] \leqslant \gamma_r(G)^{p^{k+1}}$, the result follows from Lemma 2.26 and Corollary 2.25. □

Theorem 4.5. *Let G be a finite 2-group with $\gamma_r(G)$ cyclic. Then there exist $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r \in G$ with $1 \leqslant j \leqslant r$ such that*

$$\gamma_r(G) = \{[x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r] \mid g \in G\}.$$

Proof. Define $C = C_G(\gamma_r(G)/\gamma_r(G)^4)$. Since $\gamma_r(G)$ is cyclic, then the quotient group $\gamma_r(G)/\gamma_r(G)^4$ has order at most 4, so that $|G : C| \leqslant 2$. Let $\gamma_r(G) = \langle [x_1, \dots, x_r] \rangle$ with $x_1, \dots, x_r \in G$ and let j be the maximum number such that $x_j \in C$. Observe that we may assume $j \geqslant 2$ since $G' = [G, C]$. Suppose, in addition, that $[x_1, \dots, x_r]$ is, among all γ_r-values which are generators of $\gamma_r(G)$, the one with maximum j.

For every $i = 1, \dots, r$ consider an arbitrary element $y_i \in x_i^G$, so that $y_i = x_i[x_i, g]$ for some $g \in G$. Since $\gamma_{r+1}(G) \leqslant \gamma_r(G)^2$, it follows from Corollary 2.22 that

$$[y_1, \dots, y_r] \equiv [x_1, \dots, x_r] \pmod{\gamma_r(G)^2},$$

and since $\gamma_r(G)^2 = \Phi(\gamma_r(G))$, we have

$$\gamma_r(G) = \langle [y_1, \dots, y_r] \rangle.$$

Therefore

$$\gamma_r(G)^{2^k} = \langle [y_1, \dots, y_r]^{2^k} \rangle$$

for every $k \geqslant 1$. We claim that

$$[y_1, \dots, y_r]^{2^k} \equiv [y_1, \dots, y_j^{2^k}, \dots, y_r] \pmod{\gamma_r(G)^{2^{k+1}}}$$

for every $y_i \in x_i^G$ and $k \geqslant 1$. Take $k = 1$ first. By Lemma 2.31 we have

$$[y_1, \dots, y_r]^2 \equiv [[y_1, \dots, y_j]^2, y_{j+1}, \dots, y_r] \pmod{\gamma_r(G)^4},$$

and observe that

$$[y_1, \dots, y_j^2, \dots, y_r] = [[y_1, \dots, y_j]^2 [y_1, \dots, y_j, y_j], y_{j+1}, \dots, y_r].$$

If $[y_1, \dots, y_j, y_j, y_{j+1}, \dots, y_r] \notin \gamma_r(G)^4$, then

$$\gamma_{r+1}(G) = \gamma_r(G)^2 = \langle [y_1, \dots, y_j, y_j, y_{j+1}, \dots, y_r] \rangle,$$

and so

$$\gamma_r(G) = \langle [y_1, \dots, y_j, y_j, y_{j+1}, \dots, y_{r-1}] \rangle,$$

which contradicts the maximality of j in the choice of the generator $[x_1, \dots, x_r]$.

Hence,

$$[y_1, \dots, y_j, y_j, y_{j+1}, \dots, y_r] \in \gamma_r(G)^4,$$

and it is easy to see by Lemma 2.21 that

$$[y_1^{g_1}, \dots, y_j^{g_j}, y_j^{g_{j+1}}, y_{j+1}^{g_{j+2}}, \dots, y_r^{g_{r+1}}] \in \gamma_r(G)^4$$

for every $g_1, \dots, g_{r+1} \in G$. Therefore, again by Lemma 2.21 we obtain

$$[y_1, \dots, y_r]^2 \equiv [y_1, \dots, y_j^2, \dots, y_r] \pmod{\gamma_r(G)^4}.$$

The claim follows now from Lemma 2.33 with $L = \gamma_r(G)$, $N = \gamma_r(G)^2$.

Now we can conclude our proof in the usual way. Let 2^m be the order of $\gamma_r(G)$. We will prove by induction on $m - k$ that

$$\gamma_r(G)^{2^k} \subseteq \{[y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r] \mid g \in G\}.$$

The result is true when $k = m$, so assume $k < m$ and

$$\gamma_r(G)^{2^{k+1}} \subseteq \{[y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r] \mid g \in G\}.$$

We apply Lemma 2.23 with $L = \gamma_r(G)^{2^{k-1}}$ and $N = \gamma_r(G)^{2^k}$. As

$$L = [y_1, \dots, y_j^{2^k}, \dots, y_r]N \cup N \subseteq \bigcup_{g \in G} \gamma_r(y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r)N$$

for every $y_i \in x_i^G$, by Lemma 2.23 we get

$$\gamma_r(G)^{2^k} \subseteq \{[y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r] \mid g \in G\}.$$

In particular, when $k = 0$ we obtain

$$\gamma_r(G) \subseteq \{[y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r] \mid g \in G\},$$

for every $y_i \in x_i^G$, as we wanted. □

Thus, combining Theorem 4.4 and Theorem 4.5 we get the result for all primes when $\gamma_r(G)$ is cyclic.

4.2 Lower central words with non-cyclic verbal subgroup

The study of Problem 1.2 for 2-generator verbal subgroups was initiated by Dark and Newell in [12] and followed by Guralnick in [26], where, as Rodney did for the commutator word in Theorem 3.16, they proved the result for the easiest cases, namely, the cases in which the verbal subgroup is central or elementary abelian.

Theorem 4.6 ([12, Theorem 2])**.** *Let G be a group and $r \geqslant 2$. If $\gamma_{r+1}(G) = 1$ and $\gamma_r(G)$ is a finite group with 2 generators. Then $\gamma_r(G) = G_{\gamma_r}$.*

Theorem 4.7 ([26, Theorem 3.2])**.** *Let G be a group and $r \geqslant 2$. If $\gamma_r(G)$ is elementary abelian of order p^3, then $\gamma_r(G) = G_{\gamma_r}$.*

These theorems were again generalised by Guralnick himself. Indeed, the most important result until this point was due to him.

Theorem 4.8 ([27, Theorem A])**.** *Let G be a group, $p \geqslant 5$ a prime and $r \geqslant 2$. Suppose $\gamma_r(G)$ is finite and $P \in Syl_p(\gamma_r(G))$ is generated by 2 elements. If P is abelian, then $P \subseteq G_{\gamma_r}$.*

Thus, for finite p-groups this theorem reduces to the following.

Corollary 4.9. *Let G be a finite p-group with $p \geqslant 5$ and let $r \geqslant 2$. Suppose $\gamma_r(G)$ is abelian of rank 2. Then $\gamma_r(G) \subseteq G_{\gamma_r}$.*

In addition, he found an example of a finite 2-group with $d(\gamma_r(G)) = 2$ such that $\gamma_r(G) \neq K_r(G)$, but the case $p = 3$ remained unknown.

In this chapter we will generalise again Guralnick's result for finite p-groups, showing that the condition that $\gamma_r(G)$ is abelian is not necessary. Moreover, we prove that the result is also true if $p = 3$, closing in that way the gap between the primes 2 and 5.

Theorem 4.10. *Let G be a finite p-group and let $r \geqslant 2$. If $\gamma_r(G)$ is cyclic or if p is odd and $\gamma_r(G)$ can be generated with 2 elements, then there exist $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_r \in G$ with $1 \leqslant j \leqslant r$ such that*

$$\gamma_r(G) = \{[x_1, \ldots, x_{j-1}, g, x_{j+1}, \ldots, x_r] \mid g \in G\}.$$

Before proving Theorem 4.10 we point out that if $\gamma_r(G)$ is generated by more than 2 elements then the result is no longer true. Indeed, as shown in [12, Example 2], for every prime p and every $r \geqslant 3$, there exists an infinite metabelian group G of nilpotency class r such that $\gamma_r(G)$ is elementary abelian or order p^3 and $\gamma_3(G) \neq G_{\gamma_r}$. Even if these groups are infinite, Proposition 1.3 ensures that such examples do also exist for finite p-groups. This means that, as we have done with the commutator word, we have completed the study of Problem 1.2 for lower central words in finite p-groups in terms of the number of generators of the verbal subgroup.

We now prove Theorem 4.10 in two different sections dealing separately with two different cases, namely, $C_r(G) = G$ and $C_r(G) \neq G$.

4.2.1 Finite p-groups with $C_r(G) = G$

In order to apply Lemma 2.33 we will first need to find suitable generators for the verbal subgroup $\gamma_r(G)$. We will do so now in Lemma 4.11 below. Then, as mentioned before, we will be able to conclude by applying Lemma 2.23.

Lemma 4.11. *Let G be a finite p-group with $d(\gamma_r(G)) = 2$ for some $r \geqslant 2$. If $C_r(G) = G$, then there exist an integer j with $1 \leqslant j \leqslant r$ and $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r \in G$ such that*

$$\gamma_r(G) = \langle [y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r] \mid g \in G \rangle$$

for every $y_i \in x_i^G$.

Proof. We may assume that $\Phi(\gamma_r(G)) = 1$, so using Proposition 2.36 we also have $\gamma_{r+1}(G) \leqslant \gamma_r(G)^p = 1$. Notice that it suffices to find an integer j and $x_1, \dots, x_{j-1}$, $x_{j+1}, \dots, x_r \in G$ such that

$$\gamma_r(G) = \langle [x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r] \mid g \in G \rangle,$$

since if $y_i \in x_i^G$, then $y_i = x_i h_i$ for some $h_i \in G'$, which by Corollary 2.22 implies that

$$[y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r] = [x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r]. \tag{4.1}$$

We will proceed by induction on r. If $r = 2$, then the result is true by Theorem 3.9.

Now, if there exists $x \in G_{\gamma_{r-1}}$ such that $\gamma_r(G) = [x, G]$ then we are done. Hence, suppose $[x, G] < \gamma_r(G)$ for every $x \in G_{\gamma_{r-1}}$. Observe that all subgroups V such that $\gamma_r(G)^p \leqslant V \leqslant \gamma_r(G)$ are normal in G by Proposition 2.36, so we have

$$V \max_G \gamma_r(G) \quad \text{for every} \quad V \max \gamma_r(G).$$

If

$$D = \prod_{V \max \gamma_r(G)} D_r(V) < \gamma_{r-1}(G),$$

then we could choose a γ_{r-1}-value not belonging to D, which contradicts Proposition 2.40. Therefore, assume $D = \gamma_{r-1}(G)$.

Now, observe that there exists $U \max \gamma_r(G)$ such that $[D_r(U), G] = U$. Indeed, otherwise, $[D_r(U), G] \leqslant \gamma_r(G)^p$ for all $U \max \gamma_r(G)$, and so $D_r(U) = D_r(V)$ for all $V \max \gamma_r(G)$, which is a contradiction by (i) and (ii) of Proposition 2.43. Now, by (iii) of Proposition 2.43, we have $[D_r(U), E_r(V)] = 1$ for all $V \neq U$, and so, since by Remark 2.39 all the subsets $E_r(V)$ are actually normal subgroups of G, we obtain

$$\prod_{\substack{V \max \gamma_r(G) \\ U \neq V}} E_r(V) \neq G.$$

Hence, as G cannot be the union of two proper subgroups, we can choose

$$x_r \in G \setminus \Big(E_r(U) \bigcup \prod_{\substack{V \max \gamma_r(G) \\ U \neq V}} E_r(V) \Big),$$

and thus Proposition 2.40 yields

$$\gamma_r(G) = [\gamma_{r-1}(G), x_r].$$

Define now $C_{x_r} = C_{\gamma_{r-1}(G)}(x_r)$ and notice that C_{x_r} is normal in G since

$$[C_{x_r}, G, x_r] \leqslant [\gamma_{r-1}(G), G, x_r] \leqslant \gamma_{r+1}(G) = 1.$$

Thus, we consider the quotient group G/C_{x_r}. Since $\gamma_{r+1}(G) = 1$ the map

$$\begin{aligned} \eta : \gamma_{r-1}(G) &\longrightarrow \gamma_r(G) \\ g &\longmapsto [g, x_r] \end{aligned}$$

is a group epimorphism whose kernel is C_{x_r}, so

$$|\gamma_{r-1}(G/C_{x_r})| = p^2.$$

Furthermore, since $\gamma_r(G) \leqslant C_{x_r}$, we have $C_{r-1}(G/C_{x_r}) = G/C_{x_r}$. By inductive hypothesis, there exist an integer j with $1 \leqslant j \leqslant r-1$ and $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{r-1} \in G$ such that

$$\gamma_{r-1}(G) = \langle [x_1, \ldots, x_{j-1}, g, x_{j+1}, \ldots, x_{r-1}] \mid g \in G \rangle C_{x_r}.$$

Finally,

$$\begin{aligned} \gamma_r(G) &= [\gamma_{r-1}(G), x_r] \\ &= [\langle [x_1, \ldots, x_{j-1}, g, x_{j+1}, \ldots, x_{r-1}] \mid g \in G \rangle C_{x_r}, x_r] \\ &= \langle [x_1, \ldots, x_{j-1}, g, x_{j+1}, \ldots, x_{r-1}, x_r] \mid g \in G \rangle, \end{aligned}$$

where the last equality holds by (4.1). This concludes the proof. □

Theorem 4.12. *Let G be a finite p-group with p odd and $d(\gamma_r(G)) = 2$. If $C_r(G) = G$, then there exist an integer j with $1 \leqslant j \leqslant r$ and $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_r \in G$ such that*

$$\gamma_r(G) = \{[x_1, \ldots, x_{j-1}, g, x_{j+1}, \ldots, x_r] \mid g \in G\}.$$

Proof. By Lemma 4.11, there exist an integer j with $1 \leqslant j \leqslant r$ and $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_r \in G$ such that

$$\gamma_r(G) = \langle [y_1, \ldots, y_{j-1}, g, y_{j+1}, \ldots, y_r] \mid g \in G \rangle$$

for every $y_i \in x_i^G$. Choose arbitrarily $y_i \in x_i^G$ for all i so that

$$\gamma_r(G) = \langle [y_1, \ldots, y_{j-1}, g_1, y_{j+1}, \ldots, y_r], [y_1, \ldots, y_{j-1}, g_2, y_{j+1}, \ldots, y_r] \rangle$$

for some $g_1, g_2 \in G$. Observe that $\gamma_r(G)$ is powerful by Theorem 2.18, and let

$$U = \langle [y_1, \ldots, y_{j-1}, g_2, y_{j+1}, \ldots, y_r] \rangle \gamma_r(G)^p.$$

Notice also that U is normal in G since $C_r(G) = G$. Observe that $\gamma_{r+1}(G) \leqslant \gamma_r(G)^p$, and $\gamma_r(G)^p$ is central of exponent p modulo $\gamma_r(G)^{p^2}$ by Proposition 2.36. Therefore, we apply Lemma 2.33 to both quotients

$$\gamma_r(G)/U \quad \text{and} \quad U/\gamma_r(G)^p$$

and we get

$$\gamma_r(G)^{p^k} = \langle [y_1, \ldots, y_{j-1}, g_1^{p^k}, y_{j+1}, \ldots, y_r] \rangle U^{p^k}$$

and

$$U^{p^k} = \langle [y_1, \ldots, y_{j-1}, g_2^{p^k}, y_{j+1}, \ldots, y_r] \rangle \gamma_r(G)^{p^{k+1}}$$

for every $k \geqslant 0$. Furthermore, as $\gamma_{r+1}(G) \leqslant \gamma_r(G)^p$, it follows from Corollary 2.22 that

$$[y_1, \dots, y_{j-1}, g_1, y_{j+1}, \dots, y_r]^s \equiv [y_1, \dots, y_{j-1}, g_1^s, y_{j+1}, \dots, y_r] \pmod{U}$$

and

$$[y_1, \dots, y_{j-1}, g_2, y_{j+1}, \dots, y_r]^s \equiv [y_1, \dots, y_{j-1}, g_2^s, y_{j+1}, \dots, y_r] \pmod{\gamma_r(G)^p}$$

for each integer s. Thus, using Lemma 2.33 and Proposition 2.8 it can be easily proved that

$$\begin{aligned}[y_1, \dots, y_{j-1}, g_1^{p^k}, y_{j+1}, \dots, y_r]^s & \\ &\equiv [y_1, \dots, y_{j-1}, g_1, y_{j+1}, \dots, y_r]^{sp^k} \\ &\equiv ([y_1, \dots, y_{j-1}, g_1^s, y_{j+1}, \dots, y_r]u)^{p^k} \\ &\equiv [y_1, \dots, y_{j-1}, g_1^{sp^k}, y_{j+1}, \dots, y_r] \pmod{U^{p^k}},\end{aligned}$$

where $u \in U$, and similarly

$$\begin{aligned}[y_1, \dots, y_{j-1}, g_2^{p^k}, y_{j+1}, \dots, y_r]^s & \\ &\equiv [y_1, \dots, y_{j-1}, g_2^{sp^k}, y_{j+1}, \dots, y_r] \pmod{\gamma_r(G)^{p^{k+1}}}.\end{aligned}$$

Hence, for each $k \geqslant 0$ we have

$$\gamma_r(G)^{p^k} \subseteq \bigcup_{g \in G} \gamma_r(y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r) U^{p^k}$$

for every $y_i \in x_i^G$, and similarly

$$U^{p^k} \subseteq \bigcup_{g \in G} \gamma_r(y_1, \dots, y_{j-1}, g, y_{j+1}, \dots, y_r) \gamma_r(G)^{p^{k+1}}$$

for every $y_i \in x_i^G$.

The result now follows by repeatedly applying Lemma 2.23 to the subgroups of the series

$$1 = \gamma_r(G)^{p^e} \leqslant U^{p^{e-1}} \leqslant \gamma_r(G)^{p^{e-1}} \leqslant \cdots \leqslant \gamma_r(G)^{p^i} \leqslant U^{p^{i-1}} \leqslant \cdots \leqslant \gamma_r(G),$$

where p^e is the exponent of $\gamma_r(G)$. □

4.2.2 Finite p-groups with $C_r(G) \neq G$

To end the proof of Theorem 4.10, we need a further technical definition.

Definition 4.13. Let G be a finite p-group and let $r \geqslant 2$. We define $C_r^r(G) = \gamma_r(G)^p$ and

$$C_i^r(G) = C_{\gamma_i(G)}(G/C_{i+1}^r(G))$$

for all $2 \leqslant i \leqslant r-1$. In other words, for $x \in \gamma_i(G)$ we have $x \in C_i^r(G)$ if and only if $[x, G] \leqslant C_{i+1}^r(G)$.

As done in the previous section, we start by finding suitable generators for $\gamma_r(G)$.

Lemma 4.14. *Let G be a finite p-group with $d(\gamma_r(G)) = 2$ for some $r \geqslant 2$ and $C_r(G) \neq G$. Let $U = \gamma_{r+1}(G)\gamma_r(G)^p$. Then, there exist an integer j with $2 \leqslant j \leqslant r$, $x_1, \ldots, x_{j-1} \in G$ and $c \in C_r(G)$ such that*

$$\gamma_r(G) = \langle [y_1, \ldots, y_{j-1}, c, g_{j+1}, \ldots, g_r] \rangle U$$

for every $y_k \in x_k^G$ with $k = 1, \ldots, j-1$ and every $g_{j+1}, \ldots, g_r \in G \backslash C_r(G)$. Moreover, $[\gamma_i(G), C_r(G)] \leqslant C_i^r(G)$ for every $i \in \{j, j+1, \ldots, r\}$.

Proof. Recall that $\gamma_r(G)$ is powerful by Theorem 2.18. We will proceed by induction on r. Suppose first $r = 2$ and take an arbitrary $x \in G \backslash C_2(G)$. Since $C_2(G)$ is maximal in G by Proposition 2.36, we have $G = \langle x \rangle C_2(G)$. Also, as $D_2(U) \leqslant C_2(G)$ by Proposition 2.41, we have $x \notin D_2(U)$. Moreover, by Proposition 2.36 it follows that U is the unique subgroup such that $U \max_G \gamma_r(G)$, so Proposition 2.40 gives $G = [x, G']$. Thus we get

$$G' = [x, G] = [x, \langle x \rangle C_2(G)] = [x, C_2(G)] = \langle [x, c] \rangle U$$

for some $c \in C_2(G)$. In addition, $[G', C_2(G)] \leqslant (G')^p = C_2^2(G)$, as desired.

Take then $r \geqslant 3$ and write $C = C_r(G)$ for simplicity. We may assume $\gamma_r(G)^p = C_r^r(G) = 1$. Suppose first there exist x_1, …, $x_{r-1} \in G$ such that

$$\gamma_r(G) = [x_1, \ldots, x_{r-1}, C].$$

Since $[\gamma_r(G), C] = 1$ and since $x_i^g = x_i[x_i, g]$ for every $g \in G$, it follows from Corollary 2.22 that

$$\gamma_r(G) = [y_1, \ldots, y_{r-1}, C]$$

for all $y_i \in x_i^G$. Hence, we may assume there are no such elements. In other words, if $x \in G_{\gamma_{r-1}}$, then $[x, C] \neq \gamma_r(G)$. Note, however, that $[x, C]$ is normal in G since, as above, $[x, C]^g = [x^g, C] = [x, C]$. Since U is the only non-trivial normal subgroup of G properly contained in $\gamma_r(G)$, we get $[x, C] \leqslant U$ for every γ_{r-1}-value x. Since $\gamma_{r-1}(G)$ is generated by all γ_{r-1}-values, we have, then, $[\gamma_{r-1}(G), C] \leqslant U$. This, in particular, implies that $C \leqslant E_r(U)$. As U is normal in G, it follows that $E_r(U)$ is a subgroup by Remark 2.39, and since $E_r(U) \neq G$ by Proposition 2.43, we deduce that $C = E_r(U)$. Note that we have $V \max_{\gamma_{r-1}(G)} \gamma_r(G)$ for every $V \max \gamma_r(G)$ since

$$[\gamma_r(G), \gamma_{r-1}(G)] \leqslant [\gamma_r(G), G'] \leqslant [\gamma_r(G), G, G] = 1.$$

On the other hand, $U = \gamma_{r+1}(G)$, so for every $V \max \gamma_r(G)$ with $V \neq U$ we have $[\gamma_r(G), E_r(V)] \leqslant U \cap V = 1$, and then, $E_r(V) \leqslant C$. Therefore,

$$\bigcup \{E_r(V) \mid V \max \gamma_r(G)\} \subseteq C$$

and thus, Proposition 2.40 yields

$$\gamma_r(G) = [\gamma_{r-1}(G), g]$$

for every $g \in G \backslash C$.

As $[\gamma_r(G), \gamma_{r-1}(G)] = 1$, the map

$$\begin{aligned} \eta_g : \gamma_{r-1}(G) &\longrightarrow \gamma_r(G) \\ x &\longmapsto [x, g] \end{aligned}$$

is a group epimorphism for every $g \in G\backslash C$ whose kernel is $C_{\gamma_{r-1}(G)}(g)$. Choose an arbitrary $g \in G\backslash C$, write $C_g = C_{\gamma_{r-1}(G)}(g)$ for simplicity and note that

$$[C_g, G] = [C_g, \langle g \rangle C] = [C_g, C] \leqslant [\gamma_{r-1}(G), C] \leqslant U \leqslant C_g,$$

where the last equality holds since $U \leqslant Z(G)$. Thus, the subgroups C_g are all normal in G, and we can consider the groups G/C_g. Now, $\gamma_{r-1}(G/C_g) = \gamma_{r-1}(G)/C_g$ is isomorphic to $\gamma_r(G)$, so it has order p^2 and exponent p. In addition $\gamma_r(G) \nleqslant C_g$ since otherwise $[\gamma_r(G), g] = 1$, which contradicts the fact that $g \notin C$. Thus,

$$G/C_g \neq C_{r-1}(G/C_g).$$

Moreover, since $[\gamma_{r-1}(G), C] \leqslant U \leqslant C_g$, it follows that

$$C_{r-1}(G/C_g) = C/C_g$$

for all $g \in G\backslash C$. By Proposition 2.36, there is only one normal subgroup R of G with $C_g < R < \gamma_{r-1}(G)$, so $R = C_g\gamma_r(G)$.

We apply now the inductive hypothesis to all groups G/C_g. It follows that for each $g \in G\backslash C$, there exist $j_g \geqslant 1$, $x_{1,g}, \ldots, x_{j_g-1,g} \in G$ and $c_g \in C$ such that

$$\gamma_{r-1}(G) = \langle [y_{1,g}, \ldots, y_{j_g-1,g}, c_g, g_{j_g+1}, \ldots, g_{r-1}] \rangle C_g\gamma_r(G)$$

for every $y_{i,g} \in x_{i,g}^G$, $i = 1, \ldots, j_g - 1$ and every $g_{j_g+1}, \ldots, g_{r-1} \in G\backslash C$. Moreover, if we define

$$C_{i,g}/C_g = C_i^{r-1}(G/C_g),$$

then we have $[\gamma_i(G), C] \leqslant C_{i,g}$ for all $j_g \leqslant i \leqslant r-1$.

Define now

$$U^* = \gamma_r(G) \prod_{g \in G\backslash C} C_g,$$

which is, of course, normal in G.

We claim that $U^* = C_g\gamma_r(G)$ for all $g \in G\backslash C$. For that purpose, fix $g \in G\backslash C$ and take $h \in G\backslash C$ arbitrary. Then C_gC_h is normal in G, so either $C_gC_h = \gamma_{r-1}(G)$ or $C_h \leqslant C_g\gamma_r(G)$. In the first case we would have

$$\gamma_r(G) = [\gamma_{r-1}(G), h] = [C_hC_g, h] = [C_g, h] \leqslant C_g,$$

which is a contradiction since $[\gamma_r(G), g] \neq 1$. Hence, $C_h \leqslant C_g\gamma_r(G)$, and so $C_g\gamma_r(G) = C_hC_g\gamma_r(G)$. Since this holds for all $h \in G\backslash C$, it follows that $C_g\gamma_r(G) = U^*$, and the claim is proved.

Take now $j = \max\{j_g \mid g \in G\backslash C\}$. Then, there exist $x_1, \ldots, x_{j-1} \in G$ and $c \in C$ such that

$$\gamma_{r-1}(G) = \langle [y_1, \ldots, y_{j-1}, c, g_{j+1}, \ldots, g_{r-1}] \rangle U^*$$

for every $y_i \in x_i^G$, $i = 1, \ldots, j-1$ and every $g_{j+1}, \ldots, g_{r-1} \in G\backslash C$. Moreover, because of the choice of j, we have

$$[\gamma_i(G), C] \leqslant \bigcap_{g \in G\backslash C} C_{i,g}$$

for all $j \leqslant i \leqslant r-1$. Let us prove that

$$\bigcap_{g \in G\backslash C} C_{i,g} \leqslant C_i^r(G)$$

for every i such that $j \leqslant i \leqslant r-1$.

We proceed by induction on $r-i$. If $r-i=1$, that is, if $i=r-1$, then $C_{r-1,g} = C_g = C_{\gamma_{r-1}(G)}(g)$, and since $G = \langle G\backslash C\rangle$, it follows that

$$\bigcap_{g\in G\backslash C} C_g = C_{\gamma_{r-1}(G)}(G) = C^r_{r-1}(G).$$

Assume now $i \leqslant r-2$. Then,

$$\Big[\bigcap_{g\in G\backslash C} C_{i,g}\,, G\Big] \leqslant \bigcap_{g\in G\backslash C} C_{i+1,g} \leqslant C^r_{i+1}(G)$$

by the inductive hypothesis, and so,

$$\bigcap_{g\in G\backslash C} C_{i,g} \leqslant C^r_i(G)$$

as claimed.

Since $[\gamma_r(G), C] = 1 = C^r_r(G)$, we have $[\gamma_i(G), C] \leqslant C^r_i(G)$ for every i such that $j \leqslant i \leqslant r$.

Finally, take $g_r \in G\backslash C$ arbitrary. Observe that

$$[U^*, g_r] = [C_{g_r}\gamma_r(G), g_r] = [\gamma_r(G), g_r] = U,$$

where the last equality holds since $1 \neq [\gamma_r(G), g_r] \leqslant \gamma_{r+1}(G)$. Hence,

$$\begin{aligned}\gamma_r(G) &= [\gamma_{r-1}(G), g_r]\\ &= [\langle [y_1,\dots,y_{j-1},c,g_{j+1},\dots,g_{r-1}]\rangle U^*, g_r]\\ &= [\langle [y_1,\dots,y_{j-1},c,g_{j+1},\dots,g_{r-1}]\rangle, g_r]U\\ &= \langle [y_1,\dots,y_{j-1},c,g_{j+1},\dots,g_r]\rangle U,\end{aligned}$$

and the proof is complete. □

Theorem 4.15. *Let G be a finite p-group with p odd and $d(\gamma_r(G)) = 2$ for some $r \geqslant 2$. If $C_r(G) \neq G$, then there exist an integer j with $1 \leqslant j \leqslant r$ and $x_1,\dots,x_{j-1}$, $x_{j+1},\dots,x_r \in G$ such that*

$$\gamma_r(G) = \{[x_1,\dots,x_{j-1},c,x_{j+1},\dots,x_r] \mid c \in C_r(G)\}.$$

Proof. Let $U = \gamma_{r+1}(G)\gamma_r(G)^p$ and write $C = C_r(G)$ for simplicity. By Lemma 4.14, there exist an integer j with $1 \leqslant j \leqslant r$, $x_1,\dots,x_{j-1} \in G$ and $c \in C$ such that

$$\gamma_r(G) = \langle [y_1,\dots,y_{j-1},c,g_{j+1},\dots,g_r]\rangle U$$

for every $y_i \in x_i^G$, $i = 1,\dots,j-1$ and every $g_{j+1},\dots,g_r \in G\backslash C$. Moreover, $[\gamma_i(G), C] \leqslant C^r_i(G)$ for every $j \leqslant i \leqslant r$.

Write $x = [y_1,\dots,y_{j-1}]$. It follows from the Hall-Witt identity and standard commutator calculus that

$$[x,c,g_{j+1}] = [c,g_{j+1},x]^{-1}[g_{j+1},x,c]^{-1}z$$

for some $z \in \gamma_{j+2}(G)$. On the one hand, we have

$$[z, g_{j+2}, \dots, g_r] \in \gamma_{r+1}(G) \leqslant U.$$

On the other hand,

$$[g_{j+1}, x, c] \in [\gamma_j(G), C] \leqslant C_j^r(G) \cap \gamma_{j+1}(G),$$

and since $[C_i^r(G), G] \leqslant C_{i+1}^r(G)$ for every $i \leqslant r-1$, we have

$$[C_j^r(G) \cap \gamma_{j+1}(G), g_{j+2}, \dots, g_r] \leqslant C_{r-1}^r(G) \cap \gamma_r(G) \leqslant U,$$

where the last inequality holds since $C_{r-1}^r(G) \cap \gamma_r(G)$ is normal in G but $\gamma_r(G) \nleqslant C_{r-1}^r(G)$. Thus,

$$[x, c, g_{j+1}, \dots, g_r] \equiv [x, [c, g_{j+1}], g_{j+2}, \dots, g_r] \pmod{U},$$

so in particular

$$\gamma_r(G) = \langle [x, [c, g_{j+1}], g_{j+2}, \dots, g_r] \rangle U.$$

Take now $g_{r+1} \in G \backslash C$ arbitrary. Since, clearly, we have $[U, g_{r+1}] \leqslant \gamma_r(G)^p$, it follows that

$$U = \langle [x, [c, g_{j+1}], g_{j+2}, \dots, g_{r+1}] \rangle \gamma_r(G)^p.$$

Now, observe that on the one hand we have

$$\begin{aligned} [\gamma_{j-1}(G), C, C, {}_{r-j}\ G] &\leqslant [\gamma_j(G), C, {}_{r-j}\ G] \\ &\leqslant [C_j^r(G), {}_{r-j}\ G] \\ &\leqslant C_r^r(G) = \gamma_r(G)^p, \end{aligned}$$

which is central of exponent p modulo U^p, and on the other hand we have

$$[\gamma_{j-1}(G), G', G', {}_{r-j}\ G] \leqslant \gamma_{r+3}(G) \leqslant U^p,$$

which is central of exponent p modulo $\gamma_r(G)^{p^2}$. Therefore, we can apply Lemma 2.33 to both quotients

$$\gamma_r(G)/U \quad \text{and} \quad U/\gamma_r(G)^p.$$

As the $g_{j+1}, \dots, g_r$ are all arbitrary in $G \backslash C$, wich is a normal subset of G, we can conclude in the same way as in the proof of Theorem 4.12. □

4.3 Outer commutator words

There is nothing regarding this topic in the existing literature if we consider outer commutator words w that are not lower central words. Hence, being the simplest case, and as it has been done in the previous chapters, we start by assuming that the verbal subgroup $w(G)$ is cyclic. Nevertheless, even if solving the problem when the verbal subgroup is cyclic was not too complicated for lower central words, this is not the case when dealing with general outer commutator words. As a matter of fact, our only achievement in this direction is that if G is a finite p-group with G'' cyclic, then $G'' = G_{\delta_2}$. A simple lemma is required before we proceed to the proof.

Lemma 4.16. *Let G be a group with G'' cyclic and let $x_1, x_2, x_3 \in G$ and $g \in G'$. Then,*

$$[[x_1, x_2], [x_3, g]]^n = [[x_1, x_2], [x_3, g^n]]$$

for every $n \geqslant 0$.

Proof. By Lemma 4.3, the nilpotency class of G' is 2, so

$$[[x_1, x_2], [x_3, g]]^n = [[x_1, x_2], [x_3, g]^n].$$

Note also that $[x_3, g]^n = [x_3, g^n]c$ with $c \in G''$, whence

$$\begin{aligned}[[x_1, x_2], [x_3, g]^n] &= [[x_1, x_2], [x_3, g^n]c] \\ &= [[x_1, x_2], c][[x_1, x_2], [x_3, g^n]]^c \\ &= [[x_1, x_2], [x_3, g^n]],\end{aligned}$$

and the result follows. □

Theorem 4.17. *Let G be a finite p-group with G'' cyclic. Then there exist $x_1, x_2, x_3 \in G$ such that*

$$G'' = G_{\delta_2} = \{[[x_1, x_2], [x_3, g]] \mid g \in G\}.$$

Proof. By Lemma 4.16 we can assume that for every $x_1, x_2, x_3, x_4 \in G$ such that $G'' = \langle [[x_1, x_2], [x_3, x_4]] \rangle$ we have $x_1, x_2, x_3, x_4 \notin G'$. Thus, fix a generator $[[x_1, x_2], [x_3, x_4]]$ of G'', and it follows from Lemma 2.21 that $[[y_1, y_2], [y_3, y_4]]$ is also a generator of G'' for every $y_i \in x_i^G$ with $i = 1, 2, 3, 4$. Recall that Lemma 4.3 yields $\gamma_3(G') = 1$, so

$$[[x_1, x_2], [x_3, x_4]]^n = [[x_1, x_2]^n, [x_3, x_4]] = [[x_1, x_2], [x_3, x_4]^n]$$

for every $n \geqslant 0$. Now, let k be the maximum number such that for every $j \leqslant k$, every $0 \leqslant r \leqslant p-1$ and every $y_s \in \langle x_s \rangle^G$ with $s = 1, 2, 3, 4$ we have

$$\begin{aligned}
[[y_1, y_2], [y_3, y_4]]^{p^j r} &\equiv [[y_1^{p^j r}, y_2], [y_3, y_4]] \pmod{(G'')^{p^{j+1}}}, \\
[[y_1, y_2], [y_3, y_4]]^{p^j r} &\equiv [[y_1, y_2^{p^j r}], [y_3, y_4]] \pmod{(G'')^{p^{j+1}}}, \\
[[y_1, y_2], [y_3, y_4]]^{p^j r} &\equiv [[y_1, y_2], [y_3^{p^j r}, y_4]] \pmod{(G'')^{p^{j+1}}}, \\
[[y_1, y_2], [y_3, y_4]]^{p^j r} &\equiv [[y_1, y_2], [y_3, y_4^{p^j r}]] \pmod{(G'')^{p^{j+1}}}.
\end{aligned} \tag{4.2}$$

Thus, we may assume that

$$[[x_1, x_2], [x_3, x_4]]^{p^{k+1}} \not\equiv [[x_1, x_2], [x_3^{p^{k+1}}, x_4]] \pmod{(G'')^{p^{k+2}}}.$$

From Lemma 2.6 we obtain

$$[x_3^{p^{k+1}}, x_4] = [x_3, x_4]^{p^{k+1}} [x_3, x_4, x_3]^{\binom{p^{k+1}}{2}} \cdots [x_3, x_4, x_3, \overset{p^{k+1}-1}{\ldots}, x_3] c$$

with $c \in G''$. If

$$[[x_1, x_2], [x_3, x_4, x_3, \overset{i-1}{\ldots}, x_3]^{\binom{p^{k+1}}{i}}] \leqslant (G'')^{p^{k+2}}$$

for every $2 \leqslant i \leqslant p^{k+1}$, then

$$[[x_1, x_2], [x_3, x_4]]^{p^{k+1}} \equiv [[x_1, x_2], [x_3^{p^{k+1}}, x_4]] \pmod{(G'')^{p^{k+2}}},$$

which is a contradiction. Hence, there exist $2 \leqslant i \leqslant p^{k+1}$ and $j \leqslant k+1$ such that

$$\begin{aligned}(G'')^{p^j} &= \langle [[x_1, x_2], [x_3, x_4, x_3, \overset{i-1}{\ldots}, x_3]]^{\binom{p^{k+1}}{i}}] \rangle \\ &= \langle [[x_1, x_2], [x_3, [x_3, x_4, x_3, \overset{i-2}{\ldots}, x_3]]]^{\binom{p^{k+1}}{i}} \rangle.\end{aligned}$$

In particular it follows that

$$(G'')^{p^l} = \langle [[x_1, x_2], [x_3, [x_3, x_4, x_3, \overset{i-2}{\ldots}, x_3]] \rangle$$

for some $0 \leqslant l \leqslant j$. Now Lemma 4.16 yields

$$(G'')^{p^l} \subseteq \{[[x_1, x_2], [x_3, c]] \mid c \in G'\},$$

and in particular

$$(G'')^{p^{k+1}} \subseteq \{[[x_1, x_2], [x_3, c]] \mid c \in G'\}.$$

Observe that from Lemma 2.23 and from the congruences in (4.2) we have

$$G''/(G'')^{p^{k+1}} = \{[[x_1, x_2], [x_3, g]] \mid g \in G\},$$

and thus, for a general element h of G'' there exist $g \in G$ and $c \in G'$ such that

$$h = [[x_1, x_2], [x_3, c]][[x_1, x_2], [x_3, g]].$$

Now, since $\gamma_3(G') = 1$, we have

$$\begin{aligned}[[x_1, x_2], [x_3, c]][[x_1, x_2], [x_3, g]] &= [[x_1, x_2], [x_3, c]][[x_1, x_2], [x_3, g]^c] \\ &= [[x_1, x_2], [x_3, c][x_3, g]^c] \\ &= [[x_1, x_2], [x_3, gc]],\end{aligned}$$

so that $h \in \{[[x_1, x_2], [x_3, g]] \mid g \in G\}$, as desired. □

A key step for the sake of proving the result for all outer commutators words would be solving the following.

Problem 4.18. Let G be a finite p-group such that $G^{(r)}$ is cyclic for some $r \geqslant 3$. Is then $G^{(r)} = G_{\delta_r}$?

Indeed, if one manages to give an affirmative answer to this problem, then it looks reasonable to think that a similar procedure as the one introduced by Fernández-Alcober and Morigi in [19] could be applied. If $w = [\alpha, \beta]$ is an outer commutator word, they define the *height* of w as the maximum of the heights of α and β plus 1, where the height of the word x in one variable is assumed to be 0. Thus, for $r \geqslant 1$, the words γ_r and δ_r have heights $r-1$ and r, respectively. Intuitively, one can see for a fixed height r that the derived word δ_r is the "heaviest" outer commutator word of height r, as it is the one with more variables, while the word γ_{r+1} would be the "lightest" one. Following this intuition, they introduce the notion of *defect* of an outer commutator word, which we will not define here, according to which the word δ_r has defect 0, while the word γ_{r+1} is the one with biggest defect among all outer commutator words of height r.

With this in mind, once the result holds for all the derived words, one could, following the ideas in [19], fix a height and then try to apply induction of the defect of the word, so that the result would hold for all outer commutator words.

Chapter 5

Profinite groups

A *topological group* G is a group endowed with a topology such that the function

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh^{-1} \end{aligned}$$

is a continuous function with respect to the topology. Thus, topological groups are mathematical objects with both algebraic and topological structures. The following basic properties of topological groups can be proved easily.

Proposition 5.1. *Let G be a topological group. Then:*

(i) *If H is an open (resp. closed) subgroup of G, then gH is an open (resp. closed) subset of G for every $g \in G$.*

(ii) *If H is an open subgroup of G, then H is closed in G.*

(iii) *If G is compact and H is an open subgroup of G, then H has finite index in G.*

Part (iii) of the previous proposition shows how the topological properties of a topological group can give information about its algebraic structure.

A large part of this thesis, specially Part II, is devoted to the study of a special kind of topological groups, namely, the *profinite groups*. These groups arise naturally in many different fields of mathematics such as Galois theory and algebraic geometry.

Definition 5.2. A topological group is said to be *profinite* if it is compact, Hausdorff and totally disconnected.

Therefore, by Proposition 5.1, every open subgroup of a profinite group G has finite index in G. Actually, it can be proved that the collection of all open normal subgroups of G forms an open base of the neighborhoods of the identity. This, in particular, implies that the collection of the cosets of all open normal subgroups of G forms an open base of G.

In Part II we will mainly work with countably based profinite groups. These groups can be characterised in the following way.

Theorem 5.3 ([81, Proposition 4.1.3])**.** *Let G be a profinite group. Then the following are equivalent:*

(i) *G is countably based.*

(ii) *G has countably many open normal subgroups.*

(iii) *G has a chain $G = G_0 \geqslant G_1 \geqslant \cdots$ of open normal subgroups such that $\cap_{i\geqslant 0} G_i = 1$. Moreover, the family $\{G_i\}_{i\geqslant 0}$ forms an open base of the neighborhoods of the identity.*

The most studied countably based groups are the finitely generated profinite groups. However, in the context of profinite groups, one needs to redefine what finitely generated means. Indeed, it is a well-known result that a profinite group is either finite or uncountable. Therefore, if a profinite group G is finitely generated (in the usual sense) by a finite subset S of G that is closed under taking inverses, then

$$G = \bigcup_{n\geqslant 0} S^{*n},$$

where $S^{*n} = \{h_1 \cdots h_n \mid h_i \in S \text{ for all } i = 1, \ldots, n\}$. In particular G is countable, and so finite. This problem disappears with the following definition.

Definition 5.4. A profinite group G is said to be *topologically finitely generated* or, abusing terminology, just *finitely generated*, if there exists a finite subset S of G such that $G = \overline{\langle S \rangle}$.

A well-understood type of finitely generated profinite groups are the so-called p-adic analytic pro-p groups. These are pro-p groups with the structure of an analytic manifold over $\mathbb{Q}_p$, the field of p-adic numbers. We will study these groups in more detail in Section 6.3. A typical example of a p-adic analytic pro-p group is the group $\mathbb{Z}_p$ of p-adic integers, which is defined as the inverse limit of all the cyclic groups of order p^n for $n \geqslant 0$, endowed with the discrete topology.

As a matter of fact, a profinite group is also characterised as the inverse limit of an inverse system of finite discrete groups. In this sense, these groups are usually seen as a generalisation of finite groups, as they share many properties with their finite quotients. More generally, we define the following.

Definition 5.5. Let $\mathcal{C}$ be a class of finite groups closed under taking subgroups and direct products. A *pro-$\mathcal{C}$ group* is a group which is the inverse limit of an inverse system of groups in $\mathcal{C}$ endowed with the discrete topology.

When $\mathcal{C}$ is the class of all finite groups, then a pro-$\mathcal{C}$ group is just a general profinite group. Other typical examples of the class $\mathcal{C}$ are the class of finite p-groups, the class of finite cyclic groups, the class of finite nilpotent groups, the class of finite solvable groups, etc. In those cases the pro-$\mathcal{C}$ groups that we obtain are called pro-p groups, procyclic groups, pronilpotent groups and prosolvable groups.

We end this introduction with a standard result of profinite groups that will be frequently used.

Proposition 5.6. *Let G be a profinite group and let K be a subset of G. Then*

$$\overline{K} = \bigcap_{N \trianglelefteqslant_o G} KN.$$

Since profinite groups are Hausdorff, it can be seen that the subset $\{1\}$ is closed. As a consequence we get the following.

Corollary 5.7. *Profinite groups are residually finite.*

A good and much more extensive background on these groups can be found in [13] or in [81].

5.1 Generalisation to pro-p groups

We will show in this section that all the results we have achieved in the previous chapters can be extended from abstract finite p-groups to pro-p groups. In fact, the following theorem works for any word and for profinite groups in general.

Theorem 5.8. *Let w be a word in r variables and let G be a profinite group such that $w(G/N) = (G/N)_w$ for every $N \trianglelefteq_o G$. Then $w(G) = G_w$. Moreover, if for every $N \trianglelefteq_o G$ there exist $1 \leqslant j_N \leqslant r$ and $x_1, \dots, x_{j_N-1}, x_{j_N+1}, \dots, x_r \in G/N$ such that*

$$w(G/N) = \{w(x_1, \dots, x_{j_N-1}, g, x_{j_N+1}, \dots, x_r) \mid g \in G/N\},$$

then there exists $1 \leqslant j \leqslant r$ and $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r \in G$ such that

$$w(G) = \{w(x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r) \mid g \in G\}.$$

Proof. The word map w from $G \times \overset{r}{\cdots} \times G$ to G is a continuous map, and so, since $G \times \overset{r}{\cdots} \times G$ is compact, it follows that G_w is a closed subset of G.

Thus, for the first assertion, just note that

$$\overline{w(G)} = \cap_{N \trianglelefteq_o G} w(G)N = \cap_{N \trianglelefteq_o G} G_w N = \overline{G_w} = G_w,$$

and so $w(G) = G_w$.

For the second assertion, we first claim that there exists $1 \leqslant j \leqslant r$ not depending on any open subgroup such that for every $N \trianglelefteq_o G$ there exist $x_{N,1}, \dots, x_{N,j-1}, x_{N,j+1}, \dots, x_{N,r} \in G$ such that

$$w(G)N/N = \{w(x_{N,1}, \dots, x_{N,j-1}, g, x_{N,j+1}, \dots, x_{N,r})N \mid g \in G\}.$$

Thus, for every $N \trianglelefteq_o G$, write j_N for the smallest integer such that there exist $x_{N,1}, \dots, x_{N,j_N-1}, x_{N,j_N+1}, \dots, x_{N,r} \in G$ such that

$$w(G)N/N = \{w(x_{N,1}, \dots, x_{N,j_N-1}, g, x_{N,j_N+1}, \dots, x_{N,r})N \mid g \in G\}.$$

Note that the existence of j_N is guaranteed by the hypothesis.

Let M be an open normal subgroup of G for which j_M is maximal in the set $\{j_N \mid N \trianglelefteq_o G\}$. We will prove that $j = j_M$ has the required property. Indeed, take $N \trianglelefteq_o G$ arbitrary and consider the intersection $N \cap M$, which is also open and normal in G. Now, as $N \cap M \leqslant M$, we have $j_M \leqslant j_{N \cap M}$, and by maximality, it follows that $j_M = j_{N \cap M}$. Again, since $N \cap M \leqslant N$, we have

$$w(G)N/N = \{w(x_{N,1}, \dots, x_{N,j_M-1}, g, x_{N,j_M+1}, \dots, x_{N,r})N \mid g \in G\},$$

and the claim is proved.

Now, for every $N \trianglelefteqslant_{\mathrm{o}} G$, write

$$X_N = \big\{(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r) \in G \times \overset{r-1}{\cdots} \times G \mid \\ w(G)N/N = \{w(x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r)N \mid g \in G\}\big\}.$$

Observe that if $M, N \trianglelefteqslant_o G$ such that $M \leqslant N$, then $X_M \subseteq X_N$. Hence, if $\{N_i\}_{i\in I}$ is a finite family of open normal subgroups of G, it follows that

$$\bigcap_{i\in I} X_{N_i} \supseteq X_{\cap_{i\in I} N_i},$$

and since $\cap_{i\in I} N_i$ is non-empty by assumption, we deduce that the family $\{X_N\}_{N\trianglelefteqslant_{\mathrm{o}} G}$ has the finite intersection property. Therefore, since $G \times \overset{r-1}{\cdots} \times G$ is compact, we have

$$\bigcap_{N\trianglelefteqslant_{\mathrm{o}} G} X_N \neq \varnothing.$$

Thus, if $(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r)$ belongs to this intersection, write

$$\mathcal{K}(G) = \{w(x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r) \mid g \in G\},$$

so that we have

$$w(G)N/N = \mathcal{K}(G)N/N$$

for all $N \trianglelefteqslant_{\mathrm{o}} G$.

Now, in a similar way as G_w, note that $\mathcal{K}(G)$ is also closed in G, being the image of a continuous function from G to G. Thus,

$$\overline{w(G)} = \bigcap_{N\trianglelefteqslant_{\mathrm{o}} G} w(G)N = \bigcap_{N\trianglelefteqslant_{\mathrm{o}} G} \mathcal{K}(G)N = \overline{\mathcal{K}(G)} = \mathcal{K}(G),$$

and it follows that $w(G) = \mathcal{K}(G)$. □

In particular, applying this to our results, we obtain the following.

Corollary 5.9. *Let G be a pro-p group. Then:*

(i) *If G' can be generated topologically by 2 elements, then there exists $x \in G$ such that $G' = K_x(G)$.*

(ii) *If $p \geqslant 5$ and G' is topologically generated by 3 elements, then $G' = K(G)$.*

(iii) *Suppose G' is topologically finitely generated and write $d = \log_p |G' : (G')^p|$. If $d \leqslant p - 1$ and the action of G on G' is uniserial modulo $(G')^p$, then there exists $x \in G$ such that $G' = K_x(G)$.*

(iv) *For $r \geqslant 2$, if $\gamma_r(G)$ can be generated topologically by 2 elements, then there exist $x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_r \in G$ with $1 \leqslant j \leqslant r$ such that*

$$\gamma_r(G) = \{[x_1, \dots, x_{j-1}, g, x_{j+1}, \dots, x_r] \mid g \in G\}.$$

(v) *If G'' is procyclic, then there exist $x_1, x_2, x_3 \in G$ such that*

$$G'' = \{[[x_1, x_2], [x_3, g]] \mid g \in G\}.$$

Proof. Just apply Theorem 5.8 to Theorems 3.9, 3.18, 3.19, 4.10 and 4.17. □

Part II

Hausdorff dimension in profinite groups

Chapter 6

Hausdorff dimension and Hausdorff spectra in profinite groups

Even if there is not a formal definition for the concept of the dimension of a geometrical object in general, we understand it as the space that the object covers around a point, or in other words, the number of coordinates that we need to describe it. Indeed, intuitively, we can say that the dimension of the unit disc $\mathbb{D}$, for example, is 2 because it can be described with 2 coordinates, while the dimension of its boundary $\mathbb{S}^2$ is 1, as locally it is the same as a line.

Thus, while we can talk about the area of $\mathbb{D}$ or the length of $\mathbb{S}^2$, it does not make sense to talk about the length of $\mathbb{D}$ (which intuitively would be ∞), or about the area of $\mathbb{S}^2$ (which would be 0). Nevertheless, there are some pathological objects in which the concept of dimension is not as clear as in the cases of $\mathbb{D}$ and $\mathbb{S}^2$. A good example of such an object is the so-called Koch snowflake, defined by Von Koch in [52]. This is a curve that encloses a finite area but has infinite length, somehow suggesting that its dimension should be greater than 1, but also less than 2, as it does not cover the plane.

Because of this, the concept of topological dimension was generalised to what is called *fractal dimension*, so that some objects may not have integer dimension. The problem, however, is that the way in which one can define fractal dimensions is not unique. The fractal dimension that we will mainly study in this second part of the thesis is the so-called *Hausdorff dimension*. This is one of the oldest and more common fractal dimensions in the literature and was introduced in 1918 by Felix Hausdorff (see [31]).

Even if this fractal dimension was originally defined for euclidean spaces, one can see in its definition that the only requirement for the base space is to be a metric space. As we will see, certain profinite groups, namely, the countably based profinite groups, can always be naturally equipped with a metric and, consequently, this notion can also be defined in such groups. The constructions of the Hausdorff dimension function that comes next in Section 6.1 will be directed to countably based profinite groups, but one can easily extend their definitions to general metric spaces.

6.1 Hausdorff dimension in profinite groups

For the constructions of the Hausdorff dimension function that we will give in this section, the following definition is required.

Definition 6.1. Let G be a profinite group. A *filtration series* $\mathcal{S}$ of G is a descending chain of open normal subgroups $G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots$ such that $\cap_{i\geqslant 1} G_i = 1$.

Let G be a countably based profinite group. By Theorem 5.3 this is equivalent to G having a filtration series. Thus, suppose $\mathcal{S} : G = G_0 \geqslant G_1 \geqslant \cdots$ is a filtration series of G. Then, the subgroups of $\mathcal{S}$ form an open base of neighborhoods of the identity, and thus, the family $\mathcal{B}$ consisting of all cosets of the subgroups of $\mathcal{S}$ forms an open basis of G. Moreover, the filtration series $\mathcal{S}$ induces a translation-invariant metric $d^{\mathcal{S}}$ on G defined as

$$d^{\mathcal{S}}(x, y) = \inf\{|G : G_n|^{-1} \mid xy^{-1} \in G_n\},$$

where $x, y \in G$. Then, the Hausdorff dimension function $\mathrm{hdim}_G^{\mathcal{S}}$ of G with respect to the filtration series $\mathcal{S}$ can be defined in the following way.

Let X be a subset of G. We say that $\mathcal{C}$ is a ρ-covering of X, where $\rho \in \mathbb{R}_{\geqslant 0}$, if $\mathcal{C}$ is a covering of X such that for every $B \in \mathcal{C}$ we have $\mathrm{diam}(B) \leqslant \rho$, where the diameter is defined with respect to the distance $d^{\mathcal{S}}$. For each $\delta, \rho \in \mathbb{R}_{\geqslant 0}$ we define

$$H_\rho^\delta(X) = \inf\left\{ \sum_{B\in\mathcal{C}} \mathrm{diam}(B)^\delta \mid \mathcal{C} \text{ is a } \rho\text{-covering of } X \text{ such that } \mathcal{C} \subseteq \mathcal{B} \right\},$$

and we write

$$H^\delta(X) = \lim_{\rho\to 0} H_\rho^\delta(X).$$

Now, according to [16, Page 31], there exists a real number Δ such that $H^\delta(X) = \infty$ if $\delta < \Delta$ and $H^\delta(X) = 0$ if $\delta > \Delta$. This number Δ is called the *Hausdorff dimension* of X with respect to the filtration series $\mathcal{S}$ and we denote it by $\mathrm{hdim}_G^{\mathcal{S}}(X)$.

6.2 The Hausdorff dimension of closed subgroups

In the last decades, based on the pioneering work of Abercrombie in [1] and Barnea and Shalev in [6], the concept of Hausdorff dimension has led to interesting and fruitful applications in the context of countably based profinite groups. In this work, Barnea and Shalev gave a group theoretic formula to compute the Hausdorff dimension of the closed subgroups of G.

Theorem 6.2 ([6, Theorem 2.4])**.** *Let G be a countably based profinite group and let $\mathcal{S} : G = G_0 \geqslant G_1 \geqslant \cdots$ be a filtration series of G. If H is a closed subgroup of G, then*

$$\mathrm{hdim}_G^{\mathcal{S}}(H) = \liminf_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|} \in [0, 1].$$

Thus, the Hausdorff dimension of a closed subgroup H of G can be regarded as a "logarithmic density" of H in G. At this point, it is completely natural to ask which is the range of Hausdorff dimensions of all closed subgroups of G. The following notion reflects this.

Definition 6.3. Let G be a countably based profinite group and $\mathcal{S} : G = G_0 \geqslant G_1 \geqslant \cdots$ a filtration series of G. Then, the *Hausdorff spectrum* of G with respect to $\mathcal{S}$ is

$$\operatorname{hspec}^{\mathcal{S}}(G) = \{\operatorname{hdim}_G^{\mathcal{S}}(H) \mid H \leqslant_{\mathrm{c}} G\}.$$

Even for comparatively well-behaved groups, such as p-adic analytic pro-p groups, the Hausdorff dimension function, and hence also the Hausdorff spectrum, is known to be sensitive to the choice of the underlying filtration series. The following example shows that even if the Hausdorff dimension of a closed subgroup H of a group G lies in the open interval $(0, 1)$ for a certain filtration series, there exist other filtration series for which the Hausdorff dimension of H is 0 or 1.

Example 6.4. Let p be a prime and $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Consider the closed subgroup $H = \{0\} \oplus \mathbb{Z}_p$. If we define $\mathcal{S}_1 : G = G_0 \geqslant G_1 \geqslant \cdots$ where $G_n = \mathbb{Z}_p^{p^n} \oplus \mathbb{Z}_p^{p^n}$, then

$$\operatorname{hdim}_G^{\mathcal{S}_1}(H) = \liminf_{n\to\infty} \frac{\log |HG_n : G_n|}{\log |G : G_n|} = \liminf_{n\to\infty} \frac{n}{2n} = \frac{1}{2}.$$

However, if $\mathcal{S}_2 : G = G_0 \geqslant G_1 \geqslant \cdots$ where $G_n = \mathbb{Z}_p^{p^n} \oplus \mathbb{Z}_p^{p^{n^2}}$, then

$$\operatorname{hdim}_G^{\mathcal{S}_2}(H) = \liminf_{n\to\infty} \frac{n^2}{n + n^2} = 1,$$

while if $\mathcal{S}_3 : G = G_0 \geqslant G_1 \geqslant \cdots$ where $G_n = \mathbb{Z}_p^{p^{n^2}} \oplus \mathbb{Z}_p^{p^n}$, then

$$\operatorname{hdim}_G^{\mathcal{S}_3}(H) = \liminf_{n\to\infty} \frac{n}{n + n^2} = 0.$$

For a finitely generated pro-p group G, however, there are natural choices for $\mathcal{S}$ that encapsulate group-theoretic properties of G. These are the *lower p-series* $\mathcal{L}$ of G, the *dimension subgroup series* $\mathcal{D}$ of G, the *p-power series* $\mathcal{P}$ of G, the *iterated p-power series* $\mathcal{P}^*$ of G and the *Frattini series* $\mathcal{F}$ of G, and are defined recursively by:

$$\begin{aligned}
&\mathcal{L}\colon P_1(G) = G \quad \text{and} \quad P_i(G) = P_{i-1}(G)^p[P_{i-1}(G), G] \ \text{ for } i \geqslant 2,\\
&\mathcal{D}\colon D_1(G) = G \quad \text{and} \quad D_i(G) = D_{\lceil i/p \rceil}(G)^p \prod\nolimits_{1\leqslant j<i} [D_j(G), D_{i-j}(G)] \ \text{ for } i \geqslant 2,\\
&\mathcal{P}\colon \pi_i(G) = G^{p^i} = \langle g^{p^i} \mid g \in G \rangle \text{ for } i \geqslant 0,\\
&\mathcal{P}^*\colon \pi_0^*(G) = G \quad \text{and} \quad \pi_i^*(G) = \pi_{i-1}^*(G)^p \text{ for } i \geqslant 1,\\
&\mathcal{F}\colon \Phi_0(G) = G \quad \text{and} \quad \Phi_i(G) = \Phi_{i-1}(G)^p[\Phi_{i-1}(G), \Phi_{i-1}(G)] \text{ for } i \geqslant 1.
\end{aligned}$$

Being G finitely generated ensures that all the terms of these filtration series have finite index in G, while being G a pro-p group implies that their intersections are trivial. We refer to these filtration series loosely as *the five standard filtration series*.

6.3 p-adic analytic groups and finite Hausdorff spectra

We will now focus on p-adic analytic pro-p groups. The structure of these groups is well understood, as there exist a number of characterisations of such groups. We include some of them in the following theorem. For the proofs and definitions see [13, Interlude A].

Theorem 6.5. *Let G be a pro-p group. Then the following are equivalent:*

(i) *G is p-adic analytic.*

(ii) *G has finite rank.*

(iii) *G is finitely generated and has an open normal powerful subgroup.*

(iv) *G is finitely generated and has an open normal uniform subgroup.*

(v) *G has polynomial subgroup growth.*

(vi) *G is the product of finitely many procyclic subgroups.*

It is natural to ask, at this point, whether there is a characterisation of p-adic analytic pro-p groups that involves Hausdorff dimension or the Hausdorff spectra with respect to a certain filtration series. The following theorem will motivate a possible characterisation involving the Hausdorff spectra. It was first proved by Barnea and Shalev in [6] for the p-power filtration. The result for the other filtration series was proved by Klopsch, Thillaisundaram and Zugadi-Reizabal in [51].

Theorem 6.6 ([6, Theorem 1.1] and [51, Proposition 1.5])**.** *Let G be an infinite p-adic analytic group and H a closed subgroup of G. Then, for $\mathcal{S} \in \{\mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$, we have*

$$\mathrm{hdim}_G^{\mathcal{S}}(H) = \frac{\dim(H)}{\dim(G)},$$

where $\dim(H)$ and $\dim(G)$ stand for the analytic dimension of H and G respectively.

Observe that closed subgroups of p-adic analytic pro-p groups are always p-adic analytic (this is clear from some of the characterisations of such groups in Theorem 6.5), so it makes sense to talk about the analytic dimension of closed subgroups. Theorem 6.6, in particular, shows that if G is a p-adic analytic pro-p group, then

$$\mathrm{hspec}^{\mathcal{S}}(G) \subseteq \left\{0, \frac{1}{\dim(G)}, \ldots, \frac{\dim(G)-1}{\dim(G)}, 1\right\} \tag{6.1}$$

for any $\mathcal{S} \in \{\mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$.

If $\mathcal{S} = \mathcal{L}$, then the behaviour of the Hausdorff dimension and the Hausdorff spectra is not clear. It is shown in [51, Example 4.1] that there exists a family of p-adic analytic pro-p groups $G(m,d)$, where $m, d \geqslant 0$, such that

$$\frac{|\,\mathrm{hspec}^{\mathcal{L}}(G(m,d))|}{\dim(G(m,d))} \to d+1 \quad \text{as} \quad m \to \infty,$$

which is unbounded as d tends to infinity.

Problem 6.7. Let G be a p-adic analytic pro-p group. Is then $\mathrm{hspec}^{\mathcal{L}}(G)$ finite?

Turning back to (6.1), one of the main questions in the theory of Hausdorff dimension in profinite groups is whether this fact can actually be turned into a characterisation of p-adic analytic pro-p groups. More formally:

Problem 6.8. Let G be a finitely generated pro-p group. Suppose that $\mathcal{S} \in \{\mathcal{L}, \mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$ and $|\,\mathrm{hspec}^{\mathcal{S}}(G)| < \infty$. Does it follow that G is p-adic analytic?

This problem was resolved by Klopsch, Thillaisundaram and Zugadi-Reizabal for finitely generated *solvable* pro-p groups in [51], but the general answer is not known yet. We do have, however, some structural results regarding p-adic analytic groups and Hausdorff dimension that, in fact, characterise these groups. Again, the following theorem was first proved by Barnea and Shalev for the p-power filtration and extended to other filtrations in [51].

Theorem 6.9 ([51, Theorem 1.9])**.** *Let G be a finitely generated pro-p group, and let $\mathcal{S} \in \{\mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$. Then the following are equivalent:*

(i) *The group G is p-adic analytic.*

(ii) *There exists a constant $c \in (0,1]$ such that every infinite closed subgroup $H \leqslant G$ satisfies $\mathrm{hdim}_G^{\mathcal{S}}(H) \geqslant c$.*

(iii) *Every infinite closed subgroup $H \leqslant G$ satisfies $\mathrm{hdim}_G^{\mathcal{S}}(H) > 0$.*

(iv) *The group G is finite, or there exists a closed subgroup $H \leqslant G$ such that $H \cong \mathbb{Z}_p$ and $\mathrm{hdim}_G^{\mathcal{S}}(H) > 0$.*

6.4 Infinite Hausdorff spectra

All the examples of non p-adic analytic pro-p groups that have been found so far have infinite Hausdorff spectra with respect to the five standard filtration series (and also with respect to other filtration series that arise naturally in some specific profinite groups). A much-studied example of a group with infinite Hausdorff spectra is the so-called Nottingham group (see [6, Theorem 1.6], [5], [14], [15]). Nevertheless, the Nottingham group has not full Hausdorff spectrum, meaning that its Hausdorff spectrum does not cover the full unit interval $[0,1]$. Even if Barnea and Shalev did construct in [6, Lemma 4.1, Lemma 4.3] some profinite groups with full Hausdorff spectrum, these were all infinitely generated. Therefore, they asked whether there exists a finitely generated pro-p group with full Hausdorff spectrum with respect to the p-power filtration series. Of course, this problem can be adjusted to any of the five standard filtration series:

Problem 6.10 ([6, Problem 5])**.** Does there exist a finitely generated pro-p group with full Hausdorff spectrum with respect to any of the five standard filtration series?

The first example of a finitely generated pro-p group that solves this problem was the group

$$W = C_p \mathbin{\hat{\wr}} \mathbb{Z}_p \equiv \varprojlim_n C_p \wr C_{p^n}.$$

This group can be regarded as the "minimal" finitely generated non p-adic analytic pro-p group.

Theorem 6.11 ([71, Proposition 4.5] and [49, VIII, §7])**.** *Let $\mathcal{S} \in \{\mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$. Then*

$$\mathrm{hspec}^{\mathcal{S}}(W) = [0,1].$$

Nevertheless, for the filtration series $\mathcal{L}$, the Hausdorff spectrum does not cover the full interval $[0,1]$. Indeed, as shown in [50, Corollary 2.11], we have

$$\mathrm{hspec}^{\mathcal{L}} = [0,1/2] \cup \left\{ \frac{1}{2} + \frac{m}{2p^n} \mid n \geqslant 0 \text{ and } 1 \leqslant m \leqslant p^n - 1 \right\} \cup \{1\}.$$

The group W will be studied in more detail in the next chapter.

It was also shown by Klopsch in [49] that all branch profinite groups have full Hausdorff spectrum with respect to the natural congruence filtration, so, in particular, finitely generated branch groups have full Hausdorff spectrum. More complicated examples of profinite groups with full Hausdorff spectra can be found, for example, in [2],[7] and [22].

Chapter 7

Normal Hausdorff spectra of profinite groups

As pointed out by Shalev in [71, §4.7], it is natural to consider the subset of the Hausdorff spectrum of a profinite group G that stems from considering closed *normal* subgroups of G instead of just closed subgroups. More formally, we define the following.

Definition 7.1. Let G be a countably based profinite group and $\mathcal{S} : G = G_0 \geqslant G_1 \geqslant \cdots$ a filtration series of G. Then, the *normal Hausdorff spectrum* of G with respect to $\mathcal{S}$ is

$$\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteqslant}(G) = \{\mathrm{hdim}^{\mathcal{S}}_{G}(H) \mid H \trianglelefteqslant_{\mathrm{c}} G\}.$$

In this way, the normal Hausdorff spectrum of G provides a snapshot of the normal subgroup structure of G. While plenty of examples of groups with infinite Hausdorff spectra are known, this is not the case for the normal Hausdorff spectra. Indeed, if we consider the examples of the finitely generated profinite groups with full Hausdorff spectra in the previous chapter, then all of them have finite normal Hausdorff spectra (actually in almost all of the cases the normal Hausdorff spectrum is just $\{0, 1\}$).

Thus, already twenty years ago, Shalev [71, Problem 16] put up the challenge to construct finitely generated pro-p groups with infinite normal Hausdorff spectra and he asked whether the normal Hausdorff spectra could even contain infinite real intervals. Recently, Klopsch and Thillaisundaram in [50] succeeded in constructing such examples with respect to the five standard filtration series. However, even though the normal Hausdorff spectra of their groups each contain infinite intervals, none of the spectra covers the full interval $[0, 1]$. They thus presented the following problems.

Problem 7.2 ([50, Problem 1.2])**.** Does there exist a finitely generated pro-p group G

(i) with countably infinite normal Hausdorff spectrum $\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteqslant}(G)$,

(ii) with full normal Hausdorff spectrum $\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteqslant}(G) = [0, 1]$,

(iii) such that 1 is not an isolated point in $\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteqslant}(G)$,

for one or several of the standard filtration series $\mathcal{S} \in \{\mathcal{L}, \mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$?

In this chapter we will modify the construction of Klopsch and Thillaisundaram to produce the first example of a finitely generated pro-p group with full normal Hausdorff spectrum $[0,1]$ with respect to any of the five standard filtration series, solving in this way (ii) and (iii) of Problem 7.2 and also Problem 6.10 for all five standard series (as we have seen in Theorem 6.11, the latter problem was already solved previously for the series $\mathcal{D}$, $\mathcal{P}$, $\mathcal{P}^*$ and $\mathcal{F}$).

Section 7.2 will be devoted to producing such a pro-p group when p is odd and Section 7.3 when $p = 2$. First, we introduce in Section 7.1 some technical results that will be really helpful. From now on, all subgroups of profinite groups are tacitly understood to be closed subgroups to simplify the notation.

7.1 A criterion for a full normal Hausdorff spectra

The main ingredient of the proof of Theorems 7.7 and 7.20, where it is proved that the groups that we will construct have full normal Hausdorff spectra, is Proposition 7.6 below. For the proof we first establish two lemmas. The first one is a variation of [51, Proposition 5.2].

Lemma 7.3. *Let G be a countably based pro-p group, and let $Z \trianglelefteqslant_{\mathrm{c}} G$ be infinite. Let $\mathcal{S}\colon Z_0 \geqslant Z_1 \geqslant \dots$ be a filtration series of Z consisting of G-invariant subgroups $Z_i \trianglelefteqslant_{\mathrm{o}} Z$. Let $\eta \in [0,1]$ be such that the normal closure in G of every finite collection of elements $z_1, \dots, z_m \in Z$ satisfies $\mathrm{hdim}_Z^{\mathcal{S}}(\langle z_1, \dots, z_m\rangle^G) \leqslant \eta$. Then there exists $H \leqslant_{\mathrm{c}} Z$ with $H \trianglelefteqslant G$ such that $\mathrm{hdim}_Z^{\mathcal{S}}(H) = \eta$.*

Proof. The claim can be verified in close analogy to the proof of [51, Proposition 5.2]. One constructs the subgroup $H \leqslant_{\mathrm{c}} Z$ as $H = \langle H_0 \cup H_1 \cup \cdots\rangle$, where $1 = H_0 \leqslant H_1 \leqslant \cdots$ is a suitable ascending sequence of subgroups $H_i \leqslant_{\mathrm{c}} Z$ each of which is the normal closure in G of finitely many elements. To see that the argument in op. cit. can be used, it suffices to observe that, for each $i \in \mathbb{N}$, the pro-p group G/Z_i acts nilpotently on the finite p-group Z/Z_i (and its quotients by G-invariant subgroups). □

Lemma 7.4. *Let G be a countably based profinite group with an infinite abelian normal subgroup $Z \trianglelefteqslant_{\mathrm{c}} G$ and $x \in G$ such that $G = \langle x\rangle C_G(Z)$. Let $\mathcal{S} : Z = Z_0 \geqslant Z_1 \geqslant \cdots$ be a filtration series of Z consisting of G-invariant subgroups $Z_i \trianglelefteqslant_{\mathrm{o}} Z$; for $i \geqslant 0$, let p^{e_i} be the exponent of Z/Z_i. Suppose that, for every $i \geqslant 0$, there exist $n_i \in \mathbb{N}$ and $N_i \leqslant_{\mathrm{c}} Z$ such that*

$$\gamma_{n_i+1}(G) \cap Z \leqslant Z_i \leqslant N_i \qquad \text{and} \qquad \liminf_{i\to\infty} \frac{e_i n_i}{\log_p |Z : N_i|} = 0.$$

Then every finite collection of elements $z_1, \dots, z_m \in Z$ satisfies

$$\mathrm{hdim}_Z^{\mathcal{S}}(\langle z_1, \dots, z_m\rangle^G) = 0.$$

Proof. Consider first a single element $z \in Z$. Since $G = \langle x\rangle C_G(Z)$, we have

$$\langle z\rangle^G = \langle z, [z,x], [z,x,x], \dots\rangle,$$

and since $\gamma_{n_i+1}(G) \cap Z \leqslant Z_i$ for $i \in \mathbb{N}$, we deduce that

$$\langle z\rangle^G Z_i = \langle z, [z,x], \dots, [z, x, \overset{n_i-1}{\dots}, x]\rangle Z_i;$$

in particular, since Z is abelian, this yields

$$\log_p|\langle z\rangle^G Z_i : Z_i| \leqslant e_i n_i.$$

Now consider finitely many elements $z_1, \dots, z_m \in Z$. Since Z is abelian, we have $\langle z_1, \dots, z_m\rangle^G = \langle z_1\rangle^G \cdots \langle z_m\rangle^G$. From this we deduce

$$\mathrm{hdim}_Z^{\mathcal{S}}(\langle z_1, \dots, z_m\rangle^G) \leqslant \liminf_{i\to\infty} \frac{\sum_{j=1}^m \log_p|\langle z_j\rangle^G Z_i : Z_i|}{\log_p|Z : Z_i|} \leqslant \liminf_{i\to\infty} \frac{me_in_i}{\log_p|Z : N_i|} = 0,$$

and the result follows. □

For an infinite countably based pro-p group G, equipped with a filtration series $\mathcal{S}\colon G = G_0 \geqslant G_1 \geqslant \cdots$, and a closed subgroup $H \leqslant_{\mathrm{c}} G$ we adopt the following terminology from [50].

Definition 7.5. We say that H has *strong* Hausdorff dimension in G with respect to a filtration series $\mathcal{S}$ if its Hausdorff dimension is given by a proper limit, i.e., if

$$\mathrm{hdim}_G^{\mathcal{S}}(H) = \lim_{i\to\infty} \frac{\log_p|HG_i : G_i|}{\log_p|G : G_i|}.$$

Using the previous two lemmas, we follow the proof of [51, Theorem 5.4] to obtain our main tool.

Proposition 7.6. *Let G be a countably based pro-p group with an infinite abelian normal subgroup $Z \trianglelefteq_{\mathrm{c}} G$ such that $G/C_G(Z)$ is procyclic. Let $\mathcal{S}\colon G = G_0 \geqslant G_1 \geqslant \cdots$ be a filtration series of G and consider the induced filtration series $\mathcal{S}|_Z\colon Z = G_0 \cap Z \geqslant G_1 \cap Z \geqslant \cdots$ of Z; for $i \geqslant 0$, let p^{e_i} be the exponent of $Z/(G_i \cap Z)$. Suppose that, for every $i \geqslant 0$, there exist $n_i \in \mathbb{N}$ and $M_i \leqslant_{\mathrm{c}} G$ such that*

$$\gamma_{n_i+1}(G) \cap Z \leqslant G_i \cap Z \leqslant M_i \qquad \text{and} \qquad \liminf_{i\to\infty} \frac{e_in_i}{\log_p|Z : M_i \cap Z|} = 0.$$

If Z has strong Hausdorff dimension $\xi = \mathrm{hdim}_G^{\mathcal{S}}(Z) \in [0,1]$ then we have

$$[0,\xi] \subseteq \mathrm{hspec}_{\trianglelefteqslant}^{\mathcal{S}}(G).$$

7.2 Construction of a pro-p group with full normal Hausdorff spectra

Our construction proceeds as follows. Throughout the section, let p denote an odd prime. For an integer $k \geqslant 1$, consider the finite wreath product

$$W_k = B_k \rtimes \langle \dot{x}_k\rangle \cong \langle \dot{y}_k\rangle \wr \langle \dot{x}_k\rangle,$$

with cyclic top group $\langle \dot{x}_k\rangle \cong C_{p^k}$ and elementary abelian base group

$$B_k = \prod_{j=0}^{p^k-1} \langle \dot{y}_k^{\dot{x}_k^j}\rangle \cong C_p^{p^k}.$$

Basic structural properties of the finite wreath products W_k transfer naturally to the inverse limit $W \cong \varprojlim_k W_k$ with connection homomorphisms given by

$$\begin{aligned} \phi_{ij} : W_i &\longrightarrow W_j \\ \dot{x}_i &\longmapsto \dot{x}_j \\ \dot{y}_i &\longmapsto \dot{y}_j \end{aligned}$$

for all $i \geqslant j$, i.e., the pro-p wreath product

$$W = \langle \dot{x}, \dot{y} \rangle = B \rtimes \langle \dot{x} \rangle \cong C_p \mathbin{\hat{\wr}} \mathbb{Z}_p$$

with procyclic top group $\langle \dot{x} \rangle \cong \mathbb{Z}_p$ and elementary abelian base group

$$B = \overline{\langle \dot{y}^{\dot{x}^j} \mid j \in \mathbb{Z} \rangle} \cong C_p^{\aleph_0}.$$

Let $F = F_2 = \langle \tilde{x}, \tilde{y} \rangle$ be the free pro-p group on two generators, and let $\eta\colon F \to W$, resp. $\eta_k\colon F \to W_k$, for $k \geqslant 1$, denote the continuous epimorphisms induced by $\tilde{x} \mapsto \dot{x}$ and $\tilde{y} \mapsto \dot{y}$, resp. $\tilde{x} \mapsto \dot{x}_k$ and $\tilde{y} \mapsto \dot{y}_k$. Set $R = \ker(\eta) \trianglelefteqslant_{\mathrm{c}} F$ and $R_k = \ker(\eta_k) \trianglelefteqslant_{\mathrm{o}} F$; set also $Y = \eta^{-1}(B) \trianglelefteqslant_{\mathrm{c}} F$ and $Y_k = \eta_k^{-1}(B_k) \trianglelefteqslant_{\mathrm{o}} F$. We define

$$\begin{aligned} G &= F/N, \quad \text{where } N = [R, Y]Y^p \trianglelefteqslant_{\mathrm{c}} F, \\ G_k &= F/N_k, \quad \text{where } N_k = [R_k, Y_k]Y_k^p \langle \tilde{x}^{p^k} \rangle^F. \end{aligned} \tag{7.1}$$

Furthermore, we write

$$\begin{aligned} H = Y/N \trianglelefteqslant_{\mathrm{c}} G \qquad &\text{and} \qquad Z = R/N \trianglelefteqslant_{\mathrm{c}} G, \\ H_k = Y_k/N_k \trianglelefteqslant G_k \qquad &\text{and} \qquad Z_k = R_k/N_k \trianglelefteqslant G_k. \end{aligned}$$

We denote the images of $\tilde{x}, \tilde{y}$ in G, resp. in G_k, by x, y, resp. x_k, y_k, so that $G = \overline{\langle x, y \rangle}$ and $G_k = \langle x_k, y_k \rangle$.

We observe that the finite groups G_k, $k \geqslant 1$, naturally form an inverse system and that $G \cong \varprojlim_k G_k$. Indeed, it can be checked from the definition that $R_k = \langle \tilde{x}^{p^k} \rangle^F R$, and from this that $N_k = \langle \tilde{x}^{p^k} \rangle^F N$. Hence, since $\langle \tilde{x} \rangle^F \cap N = 1$, it follows that $\cap_{k \geqslant 1} N_k = N$. Furthermore, we have $[H, Z] = 1$, and $[H_k, Z_k] = 1$ for all $k \geqslant 1$. Our aim in Sections 7.2.1 and 7.2.2 will be proving the following.

Theorem 7.7 ([33, Theorem 1.1])**.** *For $p > 2$, the 2-generator pro-p group G constructed above has full normal Hausdorff spectra with respect to the five standard filtration series, that is,*

$$\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteqslant}(G) = [0, 1]$$

for every $\mathcal{S} \in \{\mathcal{L}, \mathcal{D}, \mathcal{P}, \mathcal{P}^*, \mathcal{F}\}$.

As said, this resolves (ii) and (iii) of Problem 7.2 and also Problem 6.10 for all five standard filtration series.

We introduce the following notation for Sections 7.2.1 and 7.2.2. We write $c_1 = y$ and $c_i = [y, x, \overset{i-1}{\ldots}, x]$ for $i \geqslant 2$; furthermore, we set $c_{i,1} = [c_i, y]$ and $c_{i,j} = [c_i, y, x, \overset{j-1}{\ldots}, x]$ for $j \geqslant 2$. To keep the notation manageable, we denote, for $k \in \mathbb{N}$, the corresponding elements in the finite group G_k by the same symbols (suppressing the parameter k): $c_1 = y_k$ and $c_i = [y_k, x_k, \overset{i-1}{\ldots}, x_k]$ for $i \geqslant 2$, and similarly $c_{i,1} = [c_i, y_k]$ and $c_{i,j} = [c_i, y_k, x_k, \overset{j-1}{\ldots}, x_k]$ for $j \geqslant 2$. From the context it will be clear whether our considerations apply to G or one of the groups G_k.

7.2.1 The structure of the finite groups G_k

In this section we collect some structural results for the finite p-groups G_k defined in Section 7.2. We begin with some results for the groups W_k.

Proposition 7.8 ([50, Proposition 2.6])**.** *For $k \in \mathbb{N}$, the wreath product $W_k \cong C_p \wr C_{p^k}$ is nilpotent of class p^k. Moreover:*

(i) *The lower central series of W_k satisfies*

$$W_k = \gamma_1(W_k) = \langle \dot{x}_k, \dot{y}_k \rangle \gamma_2(W_k) \text{ with } W_k/\gamma_2(W_k) \cong C_{p^k} \times C_p,$$

and

$$\gamma_i(W_k) = \langle [\dot{y}_k, \dot{x}_k, \overset{i-1}{\ldots}, \dot{x}_k] \rangle \gamma_{i+1}(W_k) \text{ with } \gamma_i(W_k)/\gamma_{i+1}(W_k) \cong C_p$$

for $2 \leqslant i \leqslant p^k$. In particular, the base group satisfies

$$B_k = \langle \dot{y}_k \rangle \gamma_2(W_k) = \langle \dot{y}_k, [\dot{y}_k, \dot{x}_k], \ldots, [\dot{y}_k, \dot{x}_k, \overset{p^k-1}{\ldots}, \dot{x}_k] \rangle.$$

(ii) *The lower p-series of W_k has length p^k and it satisfies*

$$P_i(W_k) = \langle \dot{x}^{p^{i-1}}, [\dot{y}, \dot{x}, \overset{i-1}{\ldots}, \dot{x}] \rangle P_{i+1}(W_k) \quad \text{with} \quad P_i(W_k)/P_{i+1}(W_k) \cong C_p \times C_p$$

for $1 \leqslant i \leqslant k$, and

$$P_i(W_k) = \langle [\dot{y}, \dot{x}, \overset{i-1}{\ldots}, \dot{x}] \rangle P_{i+1}(W_k) \quad \text{with} \quad P_i(W_k)/P_{i+1}(W_k) \cong C_p$$

for $k < i \leqslant p^k$.

(iii) *The dimension subgroup series of W_k has length p^k. In particular, for $p^{k-1} + 1 \leqslant i \leqslant p^k$, it satisfies $D_i(W_k) = \gamma_i(W_k)$.*

(iv) *The Frattini series of W_k has length $k+1$ and, for $0 \leqslant i \leqslant k$ it satisfies*

$$\Phi_i(W_k) = \langle \dot{x}^{p^i} \rangle \gamma_{\frac{p^i-1}{p-1}+1}(W_k) \quad \text{with} \quad \Phi_i(W_k)/\Phi_{i+1}(W_k) \cong C_p \times \overset{p^i+1}{\ldots} \times C_p$$

and

$$\Phi_k(W_k) = \gamma_{\frac{p^k-1}{p-1}+1}(W_k) \quad \text{with} \quad \Phi_k(W_k)/\Phi_{k+1}(W_k) \cong C_p \times \overset{\frac{p^{k+1}-2p^k+1}{p-1}}{\ldots} \times C_p.$$

Proposition 7.9. *For $k \in \mathbb{N}$, we have $G_k = \langle x_k \rangle \ltimes H_k$, where $\langle x_k \rangle \cong C_{p^k}$ and H_k is freely generated in the variety of class-2 nilpotent groups of exponent p by the conjugates $y_k^{x_k^j}$, $0 \leqslant j < p^k$. In particular, the logarithmic order of G_k is*

$$\log_p|G_k| = k + p^k + \binom{p^k}{2}.$$

Proof. The proof is very similar to that of [50, Lemma 5.1]. From $G_k/Z_k \cong W_k$ we obtain

$$\log_p|G_k| = \log_p|G_k/Z_k| + \log_p|Z_k| = k + p^k + \log_p|Z_k|.$$

By construction, Z_k is elementary abelian, and from [50, Eq. (3.1)] we get

$$Z_k = \left\langle \left[y_k^{x_k^i}, y_k^{x_k^j} \right] \mid 0 \leqslant i < j \leqslant p^k - 1 \right\rangle.$$

This yields $\log_p|G_k| \leqslant k + p^k + \binom{p^k}{2}$.

Consider the finite p-group

$$M = \langle b_0, \ldots, b_{p^k-1} \rangle = E/\gamma_3(E)E^p, \tag{7.2}$$

where E is the free group on p^k generators. Then, the images of $b_0, \ldots, b_{p^k-1}$ generate independently the elementary abelian quotient M/M', and the commutators $[b_i, b_j]$ with $0 \leqslant i < j \leqslant p^k - 1$ generate independently the elementary abelian subgroup M'. The latter can be checked, for instance, by considering homomorphisms from M onto the group $\mathrm{Heis}(\mathbb{F}_p)$ of upper unitriangular 3×3 matrices over the prime field $\mathbb{F}_p$. This is a group of order p^3, nilpotency class 2 and of exponent p generated by two elements, say r and s (observe that being the exponent p comes from the fact that p is odd). For any pair of generators b_i, b_j of M, consider the map from M to $\mathrm{Heis}(\mathbb{F}_p)$ sending b_i to r, b_j to s and b_n to 1 for every $1 \leqslant n \leqslant p^k - 1$, $n \neq i, j$. This is clearly an epimorphism, and since the derived subgroup of $\mathrm{Heis}(\mathbb{F}_p)$ is generated by $[r, s]$, it follows that the commutator $[b_i, b_j]$ is independent from the other commutators that arise from the generating set $\{b_0, \ldots, b_{p^k-1}\}$. Next consider the faithful action of the cyclic group $A \cong \langle a \rangle \cong C_{p^k}$ on M induced by

$$b_i^a = \begin{cases} b_{i+1} & \text{if } 0 \leqslant i \leqslant p^k - 2, \\ b_0 & \text{if } i = p^k - 1. \end{cases}$$

We define $\hat{G}_k = A \ltimes M$ and note that $\log_p|G_k| \leqslant k + p^k + \binom{p^k}{2} = \log_p|\hat{G}_k|$. Furthermore, it is easy to see that $\hat{G}_k/M' \cong W_k$. Now, let $F\langle \tilde{x}, \tilde{y} \rangle$ be the free pro-p group on 2 generators and consider the epimorphism from F to $\hat{G}$ sending $\tilde{x}$ and $\tilde{y}$ to a and b_0 respectively. Then it follows that N_k lies in the kernel of this map, and so $|G_k| \geqslant |\hat{G}_k|$. From $|G_k| \leqslant |\hat{G}_k|$ we conclude that $G_k \cong \hat{G}_k$. □

Remark 7.10. The proof of Proposition 7.9 shows that $[H_k, H_k] = Z_k$ for $k \in \mathbb{N}$, and thus $[H, H] = Z$.

Understanding the lower central series of the groups G_k will be the key in order to use Proposition 7.6. Furthermore, it will allow us to easily compute the lower p-series and the dimension subgroup series of G_k.

Proposition 7.11. *For $k \in \mathbb{N}$, the nilpotency class of G_k is $2p^k - 1$. The terms of the lower central series of G_k are as follows:*

$$\gamma_1(G_k) = G_k = \langle x_k, y_k \rangle \gamma_2(G_k) \quad \textit{with } G_k/\gamma_2(G_k) \cong C_{p^k} \times C_p$$

and, with the notation

$$I_1 = \{i \mid 2 \leqslant i \leqslant p^k \textit{ with } i \equiv_2 0\}, \qquad I_2 = \{i \mid 2 \leqslant i \leqslant p^k \textit{ with } i \equiv_2 1\},$$
$$I_3 = \{i \mid p^k + 1 \leqslant i \leqslant 2p^k - 1 \textit{ with } i \equiv_2 0\}, \quad I_4 = \{i \mid p^k + 1 \leqslant i \leqslant 2p^k - 1 \textit{ with } i \equiv_2 1\},$$

the series continues as

$$\gamma_i(G_k) = \begin{cases} \langle c_i,\, c_{2,i-2},\, c_{4,i-4},\, \ldots,\, c_{i-2,2}\rangle\gamma_{i+1}(G_k) & \text{for } i \in I_1, \\ \langle c_i,\, c_{2,i-2},\, c_{4,i-4},\, \ldots,\, c_{i-1,1}\rangle\gamma_{i+1}(G_k) & \text{for } i \in I_2, \\ \langle c_{i-p^k+1,p^k-1},\, c_{i-p^k+3,p^k-3},\, \ldots,\, c_{p^k-1,i-p^k+1}\rangle\gamma_{i+1}(G_k) & \text{for } i \in I_3, \\ \langle c_{i-p^k,p^k},\, c_{i-p^k+2,p^k-2},\, \ldots,\, c_{p^k-1,i-p^k+1}\rangle\gamma_{i+1}(G_k) & \text{for } i \in I_4 \end{cases}$$

with

$$\gamma_i(G_k)/\gamma_{i+1}(G_k) \cong \begin{cases} C_p^{i/2} & \text{for } i \in I_1, \\ C_p^{(i+1)/2} & \text{for } i \in I_2, \\ C_p^{(2p^k-i)/2} & \text{for } i \in I_3, \\ C_p^{(2p^k-i+1)/2} & \text{for } i \in I_4. \end{cases}$$

Proof. The description of $\gamma_1(G_k)$ modulo $\gamma_2(G_k)$ is clear. Now consider $i \in I_1$, that is $2 \leqslant i \leqslant p^k$ and $i \equiv_2 0$. Our first aim is to show, by induction on i, that

$$\begin{aligned} \gamma_i(G_k) &= \langle c_i,\, c_{2,i-2},\, c_{4,i-4},\, \ldots,\, c_{i-2,2}\rangle\gamma_{i+1}(G_k), \\ \gamma_{i+1}(G_k) &= \langle c_{i+1},\, c_{2,i-1},\, c_{4,i-3},\, \ldots, c_{i,1}\rangle\gamma_{i+2}(G_k). \end{aligned} \tag{7.3}$$

The induction base, i.e., the case $i = 2$, is clear: $\gamma_2(G_k) = \langle [x_k, y_k]\rangle\gamma_3(G_k) = \langle c_2\rangle\gamma_3(G_k)$ and $\gamma_3(G_k) = \langle [c_2, x_k], [c_2, y_k]\rangle\gamma_4(G_k) = \langle c_3, c_{2,1}\rangle\gamma_4(G_k)$. Next suppose that $i \geqslant 4$. The induction hypothesis yields

$$\begin{aligned} \gamma_{i-2}(G_k) &= \langle c_{i-2},\, c_{2,i-4},\, c_{4,i-6},\, \ldots,\, c_{i-4,2}\rangle\gamma_{i-1}(G_k), \\ \gamma_{i-1}(G_k) &= \langle c_{i-1},\, c_{2,i-3},\, c_{4,i-5},\, \ldots,\, c_{i-2,1}\rangle\gamma_i(G_k). \end{aligned}$$

From $c_{m,n} \in [H_k, H_k] = Z_k$ we deduce $[c_{m,n}, y_k] = 1$ for all $m, n \geqslant 1$. This gives

$$\gamma_i(G_k) = \langle c_i,\, c_{i-1,1},\, c_{2,i-2},\, c_{4,i-4},\, \ldots,\, c_{i-2,2}\rangle\gamma_{i+1}(G_k).$$

We put

$$M = \langle c_i,\, c_{2,i-2},\, c_{4,i-4},\, \ldots, c_{i-2,2}\rangle\gamma_{i+1}(G_k)$$

and aim to show that $c_{i-1,1} \in M$. This will establish the first equation in (7.3); the second equation then follows immediately, again from $[c_{n,m}, y_k] = 1$ for $m, n \geqslant 1$.

As $c_{i-1,1} = [c_{i-2}, x_k, y_k]$, the Hall–Witt identity yields

$$c_{i-1,1}[x_k, y_k, c_{i-2}][y_k, c_{i-2}, x_k] \equiv 1 \pmod{M}.$$

Furthermore, $[y_k, c_{i-2}, x_k] \equiv c_{i-2,2}^{-1} \equiv 1$ modulo M, and this gives

$$c_{i-1,1} \equiv [c_{i-2}, c_2]^{-1} \pmod{M}.$$

Thus it suffices to prove that

$$[c_m, c_n] \equiv 1 \pmod{M} \qquad \text{for all } m, n \in \mathbb{N} \text{ with } m \geqslant n \geqslant 2 \text{ and } m + n = i.$$

We argue by induction on $m-n$. If $m-n = 0$ then $m = n$ and $[c_m, c_n] = 1$. Now suppose that $m-n > 0$, which, since i is even, implies that $m-n \geqslant 2$. As $[c_m, c_n] = [c_{m-1}, x_k, c_n]$, the Hall–Witt identity yields

$$[c_m, c_n][x_k, c_n, c_{m-1}][c_n, c_{m-1}, x_k] \equiv 1 \pmod{M},$$

where $[x_k, c_n, c_{m-1}] \equiv [c_{m-1}, c_{n+1}] \equiv 1 \pmod M$ by induction. This yields

$$[c_m, c_n] \equiv [c_n, c_{m-1}, x_k]^{-1} \equiv [[c_n, c_{m-1}]^{-1}, x_k] \pmod M.$$

From $[c_n, c_{m-1}]^{-1} \in \gamma_{i-1}(G_k)$ we deduce that

$$[c_n, c_{m-1}]^{-1} \equiv c_{i-1}^{r_0} c_{2,i-3}^{r_2} c_{4,i-5}^{r_4} \cdots c_{i-2,1}^{r_{i-2}} \pmod{\gamma_i(G_k)}$$

for suitable $r_0, r_2, \ldots, r_{i-2} \in \mathbb{Z}$. It follows that

$$[c_m, c_n] \equiv [[c_n, c_{m-1}]^{-1}, x_k] \equiv c_i^{r_0} c_{2,i-2}^{r_2} c_{4,i-4}^{r_4} \cdots c_{i-2,2}^{r_{i-2}} \equiv 1 \pmod M.$$

This finishes the proof of (7.3). Finally, we observe from (7.3) that

$$\gamma_i(G_k)/\gamma_{i+1}(G_k) \cong C_p^{l(i)} \qquad \text{and} \qquad \gamma_{i+1}(G_k)/\gamma_{i+2}(G_k) \cong C_p^{l(i+1)},$$

where $l(i) \leqslant i/2$ and $l(i+1) \leqslant i/2 + 1$; below we will see that, in fact, all the generators appearing in (7.3) are necessary.

Now consider $i \in I_3$, that is $p^k + 1 \leqslant i \leqslant 2p^k - 2$ and $i \equiv_2 0$. Since the exponent of H is p, Lemma 2.6 yields

$$c_{p^k+1} \equiv [y_k, x_k^{p^k}] = [y_k, 1] = 1 \pmod{\gamma_{p^k+2}(G_k)},$$

thus $c_{p^k+1} \in \gamma_{p^k+2}(G_k)$ and $c_{p^k+1,n} \in \gamma_{p^k+n+2}(G_k)$ for $n \geqslant 1$. For similar reasons, we have $c_{n,p^k+1} \in \gamma_{p^k+n+2}(G_k)$ for all $n \geqslant 1$. This yields, by induction on i,

$$\begin{aligned} \gamma_i(G_k) &= \langle c_{i-p^k+1,p^k-1},\, c_{i-p^k+3,p^k-3},\, \ldots,\, c_{p^k-1,i-p^k+1} \rangle \gamma_{i+1}(G_k), \\ \gamma_{i+1}(G_k) &= \langle c_{i-p^k+1,p^k},\, c_{i-p^k+3,p^k-2},\, \ldots,\, c_{p^k-1,i-p^k+2} \rangle \gamma_{i+2}(G_k). \end{aligned} \tag{7.4}$$

Similarly as before, we observe that

$$\gamma_i(G_k)/\gamma_{i+1}(G_k) \cong C_p^{l(i)} \qquad \text{and} \qquad \gamma_{i+1}(G_k)/\gamma_{i+2}(G_k) \cong C_p^{l(i+1)},$$

where $l(i), l(i+1) \leqslant (2p^k - i)/2$. Extending the argument one step further, we obtain $\gamma_{2p^k}(G_k) = 1$: the group G_k has nilpotency class at most $2p^k - 1$.

Finally, it suffices to check that the upper bounds that we derived from (7.3) and (7.4) for the logarithmic orders $\log_p|\gamma_i(G_k) : \gamma_{i+1}(G_k)|$, $1 \leqslant i \leqslant 2p^k - 1$, sum to the logarithmic order of G_k. Indeed, based on Proposition 7.9, we confirm that

$$\begin{aligned} &(k+1) + \sum_{i=2}^{p^k} \lceil i/2 \rceil + \sum_{i=p^k+1}^{2p^k-1} \lceil (2p^k - i)/2 \rceil \\ &\quad = k + 4 \sum_{i=1}^{\frac{p^k-1}{2}} i + \frac{p^k+1}{2} = k + 4\binom{\frac{p^k+1}{2}}{2} + \frac{p^k+1}{2} = k + p^k + \binom{p^k}{2} \\ &\quad = \log_p|G_k|, \end{aligned}$$

as desired. □

Corollary 7.12. *For $i \in \mathbb{N}$ we have*

$$\log_p|Z : \gamma_i(G) \cap Z| = \begin{cases} 2\sum_{j=1}^{(i-3)/2} j = (i^2 - 4i + 3)/4 & \text{if } i \equiv_2 1, \\ 2\sum_{j=1}^{(i-4)/2} j + \frac{i-2}{2} = (i^2 - 4i + 4)/4 & \text{if } i \equiv_2 0. \end{cases}$$

Proof. The claim follows from the standard identity

$$|\gamma_2(G):\gamma_i(G)| = |\gamma_2(G):\gamma_i(G)Z||\gamma_i(G)Z:\gamma_i(G)| = |\gamma_2(W):\gamma_i(W)||Z:\gamma_i(G)\cap Z|$$

and Propositions 7.8 and 7.11. □

For a better understanding of the previous theorem see the concrete example in Figure 7.1.

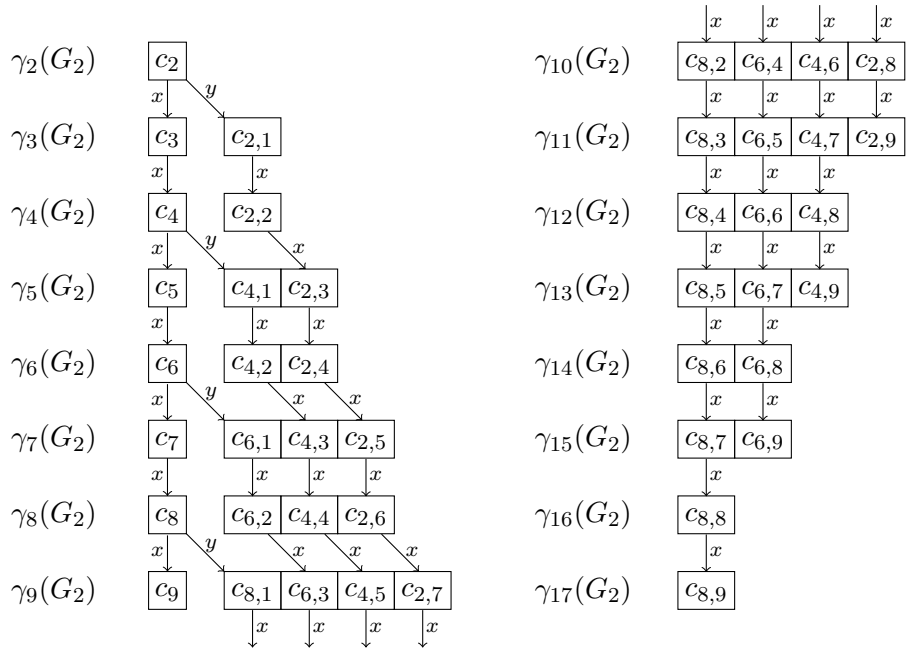

Figure 7.1: The generator structure of the lower central series of G_2 for $p = 3$. The label x (or y) in the arrows indicates commutation with x (or y).

As said, from the lower central series of G_k, it is easy to compute the lower p-series and the dimension subgroup series of G_k.

Proposition 7.13. *For $k \in \mathbb{N}$, the p-central series of G_k has length $2p^k - 1$ and its terms satisfy, for $1 \leqslant i \leqslant 2p^k - 1$,*

$$P_i(G_k) = \langle x_k^{p^{i-1}} \rangle \gamma_i(G_k).$$

Proof. The description of $P_1(G_k) = \gamma_1(G_k)$ is correct. Now suppose that $i \geqslant 2$. By induction, we have

$$P_{i-1}(G_k) = \langle x_k^{p^{i-2}} \rangle \gamma_{i-1}(G_k).$$

Recall that $P_i(G_k) = [P_{i-1}(G_k), G_k]P_{i-1}(G_k)^p$ and consider the two factors one after the other. The first factor satisfies

$$[P_{i-1}(G_k), G_k] = [\langle x_k^{p^{i-2}} \rangle \gamma_{i-1}(G_k), G_k] = [\langle x_k^{p^{i-2}} \rangle, G_k]\gamma_i(G_k),$$

and since the exponent of H is p, Lemma 2.6 yields

$$[\langle x_k^{p^{i-2}} \rangle, G_k] \leqslant [G_k^{p^{i-2}}, G_k] \leqslant \gamma_{p^{i-2}+1}(G_k).$$

From $p^{i-2}+1 \geqslant i$ we deduce that $[P_{i-1}(G_k), G_k] = \gamma_i(G_k)$.

The second factor satisfies

$$P_{i-1}(G_k)^p \equiv \langle x_k^{p^{i-2}} \rangle^p \gamma_{i-1}(G_k)^p \equiv \langle x_k^{p^{i-1}} \rangle \pmod{\gamma_i(G_k)}.$$

We conclude that $P_i(G_k) = \langle x_k^{p^{i-1}} \rangle \gamma_i(G_k)$. □

Proposition 7.14. *For $k \in \mathbb{N}$, the dimension subgroup series of G_k has length $2p^k - 1$ and its terms satisfy, for $1 \leqslant i \leqslant 2p^k - 1$,*

$$D_i(G_k) = \langle x_k^{p^{l(i)}} \rangle \gamma_i(G_k), \quad \textit{where } l(i) = \lceil \log_p(i) \rceil.$$

Proof. Let $i \in \mathbb{N}$. Since $\gamma_2(G_k)$ has exponent p, Lazard's formula (see [13, Theorem 11.2]) shows that

$$D_i(G_k) = \prod_{np^m \geqslant i} \gamma_n(G_k)^{p^m} = G_k^{p^{l(i)}} \gamma_i(G_k), \quad \text{where } l(i) = \lceil \log_p(i) \rceil.$$

Lemma 2.6 yields $a^{p^{l(i)}} b^{p^{l(i)}} \equiv (ab)^{p^{l(i)}}$ modulo $\gamma_{p^{l(i)}}(G)$ for all $a, b \in G_k$ and, as $p^{l(i)} \geqslant i$, we deduce that

$$D_i(G_k) = \langle x_k^{p^{l(i)}} \rangle \gamma_i(G_k),$$

as asserted. □

7.2.2 The normal Hausdorff spectra of G

In this section we establish Theorem 7.7; we split the proof into three parts and formulate three separate results, in dependence on the filtration series. The first result is directed to the filtration series $\mathcal{L}$ and $\mathcal{D}$ (Theorem 7.15), the second one to the filtration series $\mathcal{P}$ and $\mathcal{P}^*$ (Theorem 7.16) and the third one to the filtration series $\mathcal{F}$ (Theorem 7.19).

Theorem 7.15. *The pro-p group G has full normal Hausdorff spectra*

$$\operatorname{hspec}^{\mathcal{L}}_{\trianglelefteqslant}(G) = [0,1] \qquad \textit{and} \qquad \operatorname{hspec}^{\mathcal{D}}_{\trianglelefteqslant}(G) = [0,1]$$

with respect to the lower p-series $\mathcal{L}$ and the dimension subgroup series $\mathcal{D}$.

Proof. Let $\mathcal{S}$ be $\mathcal{L}$, resp. $\mathcal{D}$. Write $\mathcal{S}\colon G = S_0 = S_1 \geqslant S_2 \geqslant \ldots$, where $S_i = P_i(G)$, resp. $S_i = D_i(G)$, for $i \geqslant 1$, and observe that $Z \leqslant \gamma_2(G)$; compare Remark 7.10. Thus, since $\langle x_k \rangle \cap \gamma_2(G_k) = 1$, Proposition 7.13, resp. Proposition 7.14, yields

$$S_i \cap Z = \gamma_i(G) \cap Z \quad \text{for } i \geqslant 1.$$

From Corollary 7.12 we see that

$$\lim_{i\to\infty} \frac{i}{\log_p |Z : \gamma_i(G) \cap Z|} = 0. \tag{7.5}$$

This allows us to pin down the Hausdorff dimension of $Z \leqslant_{\mathrm{c}} G$:

$$\begin{aligned}\operatorname{hdim}^{\mathcal{S}}_G(Z) &= \liminf_{i\to\infty} \left(\frac{\log_p |G : S_i|}{\log_p |S_i Z : S_i|} \right)^{-1} = \liminf_{i\to\infty} \left(\frac{\log_p |G : S_i Z| + \log_p |S_i Z : S_i|}{\log_p |S_i Z : S_i|} \right)^{-1} \\ &= \liminf_{i\to\infty} \left(\frac{\log_p |G : S_i Z|}{\log_p |Z : S_i \cap Z|} + 1 \right)^{-1} = \liminf_{i\to\infty} \left(\frac{\log_p |G : S_i Z|}{\log_p |Z : \gamma_i(G) \cap Z|} + 1 \right)^{-1} = 1,\end{aligned}$$

where the last equality follows from (7.5) and the fact that $\log_p|G : S_iZ| \leqslant 2i$, by Proposition 7.8 and Proposition 7.14. In particular, Z has strong Hausdorff dimension.

Thus Proposition 7.6, with $e_i = 1$, $n_i = i$ and $M_i = \gamma_i(G)$, yields

$$[0,1] = [0, \mathrm{hdim}_G^{\mathcal{S}}(Z)] \subseteq \mathrm{hspec}_{\leqslant}^{\mathcal{S}}(G),$$

as we wanted. □

Theorem 7.16. *The pro-p group G has full normal Hausdorff spectra*

$$\mathrm{hspec}_{\leqslant}^{\mathcal{P}}(G) = [0,1] \qquad \textit{and} \qquad \mathrm{hspec}_{\leqslant}^{\mathcal{P}^*}(G) = [0,1]$$

with respect to the p-power series $\mathcal{P}$ and the iterated p-power series $\mathcal{P}^*$.

Proof. Recall our notation $\pi_i(G) = G^{p^i}$ and $\pi_i^*(G)$ for the terms of the series $\mathcal{P}$ and $\mathcal{P}^*$. Our first aim is to show that

$$\gamma_{2p^i}(G) \leqslant G^{p^i} \leqslant \pi_i^*(G) \leqslant \langle x^{p^i}\rangle \gamma_{p^i}(G) \quad \text{for all } i \geqslant 0. \tag{7.6}$$

Let $i \geqslant 0$. From the construction of G and G_k, since as said $N_k = \langle \tilde{x}_k^{p^k}\rangle^F N$, it is easily seen that $G/G^{p^k} \cong G_k/G_k^{p^k}$ for $k \in \mathbb{N}$. Hence Proposition 7.11 yields $\gamma_{2p^i}(G/G^{p^k}) = 1$, so that $\gamma_{2p^i}(G) \leqslant G^{p^i}$. Clearly, we have $G^{p^i} \leqslant \pi_i^*(G)$. It remains to justify the last inclusion in (7.6). We proceed by induction on i. For $i = 0$ even equality holds, trivially. Now suppose that $i \geqslant 1$. The induction hypothesis yields

$$\pi_{i-1}^*(G) \leqslant \langle x^{p^{i-1}}\rangle \gamma_{p^{i-1}}(G).$$

Let $g \in \pi_{i-1}^*(G)$, and write $g = x^{mp^{i-1}}h$ with $m \in \mathbb{Z}_p$ and $h \in \gamma_{p^{i-1}}(G) \cap H$ (here the intersection with H is relevant only when $i = 1$). Since $H^p = 1$, Lemma 2.6 yields $g^p = x^{mp^i}z$ with $x^{mp^i} \in \langle x^{p^i}\rangle$ and $z \in \gamma_p(\langle x^{p^{i-1}}, h\rangle)$. Thus it suffices to show that $\gamma_p(\langle x^{p^{i-1}}, h\rangle) \leqslant \gamma_{p^i}(G)$.

Suppose that c is an arbitrary commutator of weight $n \geqslant 2$ in $\{x^{p^{i-1}}, h\}$; we show by induction on n that $c \in \gamma_{np^{i-1}}(G)$. For $n = 2$, it suffices to consider $c = [h, x^{p^{i-1}}]$, and Lemma 2.6 shows that $c \in \gamma_{2p^{i-1}}(G)$. For $n \geqslant 3$, we see by induction that it suffices to consider $c = [d, h]$ and $[d, x^{p^{i-1}}]$ with $d \in \gamma_{(n-1)p^{i-1}}(G)$; if $c = [d, h]$, the result follows immediately, and, if $c = [d, x^{p^{i-1}}]$, the result follows again by Lemma 2.6. This concludes the proof of (7.6).

Let $\mathcal{S} = \mathcal{P}$, resp. $\mathcal{S} = \mathcal{P}^*$, and write $S_i = \pi_i(G) = G^{p^i}$, resp. $S_i = \pi_i^*(G)$, for $i \geqslant 0$. Recall that $Z \leqslant \gamma_2(G)$; compare Remark 7.10. Thus (7.6) yields

$$\gamma_{2p^i}(G) \cap Z \leqslant S_i \cap Z \leqslant \big(\langle x^{p^i}\rangle \gamma_{p^i}(G)\big) \cap Z = \gamma_{p^i}(G) \cap Z. \tag{7.7}$$

From Corollary 7.12 we see that

$$\lim_{i\to\infty} \frac{2p^i}{\log_p|Z : \gamma_{p^i}(G) \cap Z|} = 0. \tag{7.8}$$

As in the proof of Theorem 7.15 we want to apply Proposition 7.6, here with $e_i = 1$, $n_i = 2p^i$ and $M_i = \gamma_{p^i}(G)$, to conclude that G has full normal Hausdorff spectrum.

It remains to check that $\mathrm{hdim}_G^{\mathcal{S}}(Z) = 1$. We observe that, for $i \geqslant 0$,

$$\log_p|G : S_iZ| \leqslant \log_p|G_i : G_i^{p^i} Z_i| \leqslant \log_p|W_i| = i + p^i \leqslant 2p^i,$$

and thus, by (7.7) and (7.8),

$$\lim_{i\to\infty} \frac{\log_p|G : S_iZ|}{\log_p|Z : S_i \cap Z|} \leqslant \lim_{i\to\infty} \frac{\log_p|G : S_iZ|}{\log_p|Z : \gamma_{p^i}(G) \cap Z|} = 0.$$

As in the proof of Theorem 7.15 we conclude that $\mathrm{hdim}_G^{\mathcal{S}}(Z) = 1$. □

A little extra work is required to determine the normal Hausdorff spectrum of G with respect to the Frattini series. We define

$$z_{i,j} = \begin{cases} [c_i, c_j] \in \gamma_{i+j}(G) & \text{for } i, j \geqslant 1, \\ 1 & \text{otherwise.} \end{cases} \tag{7.9}$$

Proposition 7.8 and Remark 7.10 show that

$$H = \langle c_i \mid i \geqslant 1\rangle \qquad \text{and} \qquad Z = \langle z_{i,j} \mid 1 \leqslant j < i\rangle.$$

Moreover, since for every k the number of pairs (i, j) with $1 \leqslant i < j$ such that $i + j < k$ is precisely the number obtained in Corollary 7.12, it can be seen that, for $k \geqslant 2$ we have

$$\gamma_k(G) \cap Z = \langle z_{i,j} \mid 1 \leqslant j < i \text{ and } i + j \geqslant k\rangle. \tag{7.10}$$

Lemma 7.17. *For $i, j \in \mathbb{N}$ and $r \geqslant 0$, we have*

$$[z_{i,j}, x, \overset{r}{\ldots}, x] = \prod_{s=0}^{r} \prod_{t=0}^{s} z_{i+r-t,j+r-s+t}^{\binom{r}{s}\binom{s}{t}}.$$

Proof. We argue by induction on r. For $r = 0$ both sides are equal to $z_{i,j}$. Now suppose that $r \geqslant 1$. We observe that, for $m, n \geqslant 1$,

$$[z_{m,n}, x] = z_{m,n}^{-1}[c_m^x, c_n^x] = z_{m,n}^{-1}[c_m c_{m+1}, c_n c_{n+1}] = z_{m+1,n}\, z_{m,n+1}\, z_{m+1,n+1}. \tag{7.11}$$

Thus the induction hypothesis yields

$$[z_{i,j}, x, \overset{r}{\ldots}, x] = [[z_{i,j}, x, \overset{r-1}{\ldots}, x], x] = \prod_{s=0}^{r} \prod_{t=0}^{s} [z_{i+r-1-t,j+r-1-s+t}, x]^{\binom{r-1}{s}\binom{s}{t}},$$

and, in view of (7.11), the result follows from the identity

$$\begin{aligned} \binom{r-1}{s-1}\binom{s-1}{t} + \binom{r-1}{s-1}\binom{s-1}{t-1} + \binom{r-1}{s}\binom{s}{t} \\ = \binom{r-1}{s-1}\binom{s}{t} + \binom{r-1}{s}\binom{s}{t} = \binom{r}{s}\binom{s}{t} \end{aligned}$$

for $0 \leqslant s \leqslant r$ and $0 \leqslant t \leqslant s$. □

Lemma 2.6 and Lemma 7.17 lead directly to a useful corollary.

Corollary 7.18. *For $i, j \in \mathbb{N}$ and $k \geqslant 0$, we have*

$$[z_{i,j}, x^{p^k}] = z_{i+p^k,j} z_{i,j+p^k} z_{i+p^k,j+p^k}^{-1}.$$

Proof. By Lemma 2.6 we have $[z_{i,j}, x^{p^k}] = [z_{i,j}, x, \overset{p^k}{\ldots}, x]$ since the exponent of Z is p, and since p divides $\binom{p^k}{n}$ for all $n \neq 0, p^k$, the result follows. □

Theorem 7.19. *The pro-p group G has full normal Hausdorff spectrum*

$$\operatorname{hspec}^{\mathcal{F}}_{\trianglelefteqslant}(G) = [0, 1]$$

with respect to the Frattini series $\mathcal{F}$.

Proof. For $i \geqslant 0$, we write $[i]_p = (p^i - 1)/(p-1)$ and note, for $i \geqslant 1$, that $[i-1]_p + p^{i-1} = [i]_p$. We consider

$$C_i = \langle x^{p^i} \rangle \ltimes \langle c_j \mid j \geqslant 1 + [i]_p \rangle \leqslant_{\mathrm{c}} G$$

and claim, for $i \geqslant 1$, that

$$\Psi_i^-(G) \leqslant \Phi_i(G) \leqslant \Psi_i^+(G), \tag{7.12}$$

where

$$\Psi_i^-(G) = C_i\big(\gamma_{1+2[i-1]_p+p^{i-1}}(G) \cap Z\big) \quad \text{and} \quad \Psi_i^+(G) = C_i\big(\gamma_{2+2[i-1]_p}(G) \cap Z\big).$$

For $i = 1$ the assertion is that $\Phi(G) = C_1(\gamma_2(G) \cap Z) = \langle x^p, c_2, c_3, \ldots \rangle(\gamma_2(G) \cap Z)$, which follows since $\Phi(G) = \langle x^p \rangle \gamma_2(G)$. Now suppose that $i \geqslant 2$. Lemma 2.6 and the observation that $p^{i-1} \geqslant 2p^{i-2}$ yield

$$[\gamma_{2+2[i-2]_p}(G) \cap Z, x^{p^{i-1}}] \leqslant \gamma_{2+2[i-2]_p+p^{i-1}}(G) \cap Z \leqslant \gamma_{2+2[i-1]_p}(G) \cap Z;$$

since $[Z, H] = 1$, we have $[\gamma_{2+2[i-2]_p}(G) \cap Z, c_n] = 1$ for all $n \geqslant 1$. Furthermore, Lemma 2.6 gives

$$[c_n, x^{p^{i-1}}] \equiv c_{n+p^{i-1}} \pmod{\gamma_{2n+p^{i-1}}(G) \cap Z} \quad \text{for all } n \geqslant 1, \tag{7.13}$$

and hence

$$[C_{i-1}, x^{p^{i-1}}] \leqslant C_i\big(\gamma_{2+2[i-1]_p+p^{i-1}}(G) \cap Z\big).$$

By induction, $\Phi_{i-1}(G) \leqslant \Psi_{i-1}^+(G) = C_{i-1}\big(\gamma_{2+2[i-2]_p}(G) \cap Z\big)$, and this implies

$$\begin{aligned}\Phi_i(G) = \Phi(\Phi_{i-1}(G)) &\leqslant \langle x^{p^i} \rangle [C_{i-1}, C_{i-1}]\big(\gamma_{2+2[i-1]_p}(G) \cap Z\big) \\ &\leqslant C_i\big(\gamma_{2+2[i-1]_p}(G) \cap Z\big) = \Psi_i^+(G).\end{aligned}$$

It remains to check the first inclusion in (7.12); by induction, it suffices to show that

$$\Psi_i^-(G) \leqslant K, \quad \text{where } K = \Phi\big(\Psi_{i-1}^-(G)\big).$$

First we show that $\gamma_{1+2[i-1]_p+p^{i-1}}(G) \cap Z \leqslant K$ implies $C_i \leqslant K$. Clearly, $x^{p^i} \in C_{i-1}^p \leqslant K$, and (7.13) shows that, for $j \geqslant 1 + [i]_p$, there exists $d_j \in \gamma_{2(j-p^{i-1})+p^{i-1}}(G) \cap Z \leqslant \gamma_{1+2[i-1]_p+p^{i-1}}(G) \cap Z$ such that

$$c_j = [c_{j-p^{i-1}}, x^{p^{i-1}}] d_j \in [C_{i-1}, C_{i-1}] \leqslant K.$$

Thus it suffices to prove that $\gamma_{1+2[i-1]_p+p^{i-1}}(G) \cap Z \leqslant K$.

From (7.10) we recall that

$$\gamma_{1+2[i-1]_p+p^{i-1}}(G) \cap Z = \langle z_{j,k} \mid 1 \leqslant k < j \text{ and } j+k \geqslant 1+2[i-1]_p+p^{i-1} \rangle.$$

From $[C_{i-1}, C_{i-1}] \leqslant K$ we deduce that

$$z_{m,n} \in K \quad \text{for } m > n \geqslant 1+[i-1]_p. \tag{7.14}$$

Thus, it remains to see that $z_{j,k} \in K$ for $j,k \in \mathbb{N}$ satisfying

$$1 \leqslant k < j, \qquad j+k \geqslant 1+2[i-1]_p+p^{i-1} \qquad \text{and} \qquad k \leqslant [i-1]_p.$$

Given such $j,k \in \mathbb{N}$, we observe that

$$k < 1+[i-1]_p \leqslant j-p^{i-1} \qquad \text{and} \qquad (j-p^{i-1})+k \geqslant 1+2[i-1]_p;$$

hence (7.10) implies

$$z_{j-p^{i-1},k} \in \gamma_{1+2[i-1]_p}(G) \cap Z \leqslant \gamma_{1+2[i-2]_p+p^{i-2}}(G) \cap Z \leqslant \Psi^-_{i-1}(G).$$

We apply Corollary 7.18 to deduce that

$$z_{j,k}\, z_{j-p^{i-1},k+p^{i-1}}\, z_{j,k+p^{i-1}} = [z_{j-p^{i-1},k}, x^{p^{i-1}}] \in [\Psi^-_{i-1}(G), C_{i-1}] \leqslant K. \tag{7.15}$$

As $j > k+p^{i-1} \geqslant 1+[i-1]_p$, we see from (7.14), for $m=j$ and $n=k+p^{i-1}$ that $z_{j,k+p^{i-1}} \in K$. Similarly, we deduce that $z_{j-p^{i-1},k+p^{i-1}} \in K$, if $j-p^{i-1} > k+p^{i-1}$, and, finally, $z_{j-p^{i-1},k+p^{i-1}} = z^{-1}_{k+p^{i-1},j-p^{i-1}} \in K$, if $j-p^{i-1} \leqslant k+p^{i-1}$ and thus $j-p^{i-1} \geqslant 1+[i-1]_p$. Feeding this information into (7.15), we obtain $z_{j,k} \in K$ which concludes the proof of (7.12).

From (7.12) we deduce that

$$\gamma_{1+2[i-1]_p+p^{i-1}}(G) \cap Z \leqslant \Phi_i(G) \cap Z \leqslant \gamma_{2+2[i-1]_p}(G) \cap Z,$$

and from Corollary 7.12 we see that

$$\lim_{i\to\infty} \frac{2[i-1]_p+p^{i-1}}{\log_p |Z : \gamma_{2+2[i-1]_p}(G) \cap Z|} = 0.$$

As in the proof of Theorem 7.15 we want to apply Proposition 7.6, here with $e_i = 1$, $n_i = 2[i-1]_p + p^{i-1}$ and $M_i = \gamma_{2+2[i-1]_p}(G)$, to conclude that G has full normal Hausdorff spectrum.

It remains to check that $\operatorname{hdim}^{\mathcal{F}}_G(Z) = 1$. From Proposition 7.8 we see that $\log_p |G : \Phi_i(G)Z| = i + [i]_p$, and hence Corollary 7.12 implies

$$\lim_{i\to\infty} \frac{\log_p |G : \Phi_i(G)Z|}{\log_p |Z : \Phi_i(G) \cap Z|} = 0.$$

As in the proof of Theorem 7.15 we see that $\operatorname{hdim}^{\mathcal{F}}_G(Z) = 1$. □

Theorem 7.7 summarises the results in Theorems 7.15, 7.16 and 7.19.

7.3 A pro-2 group with full normal Hausdorff spectra

To end with Chapter 7 we will modify the construction in Section 7.2 to produce a pro-2 group with full normal Hausdorff spectra with respect to the five standard filtration series.

The unique difference in the construction of the pro-p group when $p = 2$ is that we slightly change the definitions of N and N_k in (7.1), so that in this case we set

$$G = F/N, \quad \text{where } N = [R, Y]R^2 \trianglelefteqslant_{\mathrm{c}} F,$$
$$G_k = F/N_k, \quad \text{where } N_k = [R_k, Y_k]R_k^2\langle \tilde{x}^{2^k}\rangle^F.$$

We denote again by H and Z the closed normal subgroups of G corresponding to Y/N and R/N, and we denote by H_k and Z_k the normal subgroups of G_k corresponding to Y_k/N_k and R_k/N_k. We also set $G = \langle x, y\rangle$ and $G_k = \langle x_k, y_k\rangle$ and we adapt the notation introduced before Section 7.2.1 to the pro-2 group G.

Our goal will be proving the following.

Theorem 7.20 ([35])**.** *The 2-generator pro-2 group G constructed above has full normal Hausdorff spectra with respect to all the standard filtration series, that is,*

$$\mathrm{hspec}^{\mathcal{S}}_{\trianglelefteqslant}(G) = [0, 1]$$

for every $\mathcal{S} \in \{\mathcal{L}, \mathcal{D}, \mathcal{P}, \mathcal{F}\}$.

Remark 7.21. Note that for pro-2 groups the iterated 2-power series $\mathcal{P}^*$ and the Frattini series $\mathcal{F}$ coincide. Indeed since groups of exponent 2 are always abelian, we have $\Phi(H) = H^2H' = H^2$ for every pro-2 group H.

7.3.1 Adapting structural results for $p = 2$

We proceed now in close analogy to Section 7.2. We start computing the orders of the G_k.

Proposition 7.22. *For $k \in \mathbb{N}$, the logarithmic order of G_k is*

$$\log_2 |G_k| = k + 2^{k+1} + \binom{2^k}{2} = k + 2^{2k-1} + 2^{k+1} - 2^{k-1}.$$

Proof. The proof is almost the same as that of Proposition 7.9. Just note that in this case, by construction, the subgroup Z_k is elementary abelian and

$$Z_k = \langle \{(y_k^{x_k^i})^2 \mid 0 \leqslant i \leqslant 2^k - 1\} \cup \{[y_k^{x_k^i}, y_k^{x_k^j}] \mid 0 \leqslant i < j \leqslant 2^k - 1\}\rangle,$$

so that

$$\log_2 |G_k| = k + 2^k + \log_2 |Z_k| \leqslant k + 2^{k+1} + \binom{2^k}{2}.$$

Thus, the result follows as in Proposition 7.9 just changing the definition of M in (7.2) to

$$M = E/[\Phi(E), E]\Phi(E)^2,$$

where E is the free group on 2^k generators. In this case, the elementary abelian subgroup $\Phi(M)$ is generated independently by the elements $b_0^2, \dots, b_{2^k-1}^2$ together with the commutators $[b_i, b_j]$ for $0 \leqslant i < j \leqslant 2^k - 1$, which can be verified by considering homomorphisms from M onto groups of the form $C_2^{2^k-1} \times C_4$ and $C_2^{2^k-2} \times \mathrm{Heis}(\mathbb{F}_2)$. □

Our next goal is computing the lower central series of the G_k. In order to do so, we need the following lemmas.

Lemma 7.23. *Let $k \in \mathbb{N}$ and let G_k be as above. Then:*

(i) *For $2^{k-1}+1 \leqslant i \leqslant 2^k$, we have $c_i^4 = 1$ and $c_i^2 \in \gamma_{i+1}(G_k)$.*

(ii) *For $i \geqslant 2^k+1$, we have $c_i^2 = 1$.*

(iii) *For $i \geqslant 2^k + 2^{k-1} + 1$, we have $c_i \in \gamma_{i+1}(G_k)$.*

Proof. (i) As H_k has exponent 4 it is clear that $c_i^4 = 1$. In addition, since $[H_k, H_k] \leqslant Z_k$ has exponent 2, it follows from Lemma 2.6 that

$$1 = [y_k, x_k^{2^{k-1}}] \equiv [y_k, x_k, \overset{2^{k-2}}{\ldots}, x_k]^2 [y_k, x_k, \overset{2^{k-1}}{\ldots}, x_k] \pmod{\gamma_{2^{k-1}+2}(G_k)}. \tag{7.16}$$

Therefore $c_{2^{k-2}+1}^2 \equiv c_{2^{k-1}+1} \pmod{\gamma_{2^{k-1}+2}(G_k)}$, and hence

$$c_{2^{k-1}+1}^2 \equiv 1 \pmod{\gamma_{2^{k-1}+2}(G_k)}.$$

Now, for $2^{k-1}+2 \leqslant i \leqslant 2^k$, notice from Lemma 2.21 that

$$\begin{aligned} c_i \equiv [c_{2^{k-1}+1}, x_k, \overset{i-2^{k-1}-1}{\ldots}, x_k] &\equiv [c_{2^{k-2}+1}^2, x_k, \overset{i-2^{k-1}-1}{\ldots}, x_k] \\ &\equiv [y_k, x_k, \overset{i-2^{k-1}+2^{k-2}-1}{\ldots}, x_k]^2 \pmod{\gamma_{i+1}(G_k)}, \end{aligned}$$

hence the result.

(ii) This follows immediately from the fact that by Proposition 7.8 we have $c_i \in Z_k$ for $i \geqslant 2^k + 1$.

(iii) It suffices to prove the result for $i = 2^k + 2^{k-1} + 1$. From (7.16), we obtain

$$c_i = [c_{2^k+1}, x_k, \overset{2^{k-1}}{\ldots}, x_k] \equiv [c_{2^{k-1}+1}^2, x_k, \overset{2^{k-1}}{\ldots}, x_k] \pmod{\gamma_{i+1}(G_k)}.$$

As

$$[c_{2^{k-1}+1}^2, x_k, \overset{2^{k-1}}{\ldots}, x_k] \equiv c_{2^k+1}^2 \pmod{\gamma_{i+1}(G_k)}$$

we have $c_i \equiv c_{2^k+1}^2 \pmod{\gamma_{i+1}(G_k)}$, and by (ii), it follows that $c_i \in \gamma_{i+1}(G)$, as required. □

We adjust the notation introduced in (7.9) to the pro-2 group G. It follows immediately that the result in Lemma 7.17 works also for the $p = 2$ case, even if the groups in consideration are not exactly the same. So, abusing notation, we will keep using Lemma 7.17 also for the pro-2 group G.

Lemma 7.24. *Let $k \in \mathbb{N}$. In the group G_k, for $m \in \mathbb{N}$ even, we have*

$$c_{m,2^k} \in \gamma_{2^k+m+1}(G_k).$$

Proof. Note that

$$c_{m,2^k} = [z_{m,1}, x_k, \overset{2^k-1}{\ldots}, x_k],$$

and since $z_{i,j} \in \gamma_{i+j}(G_k)$ for every $i, j \in \mathbb{N}$, we have by Lemma 7.17 that

$$[z_{m,1}, x_k, \overset{2^k-1}{\ldots}, x_k] = \prod_{n=0}^{2^k-1} z_{m+2^k-1-n,1+n}^{\binom{2^k-1}{n}} \pmod{\gamma_{2^k+m+1}(G_k)}.$$

In addition, the exponent of Z_k is 2 by construction. Hence, since by Theorem 2.7 all the binomial numbers $\binom{2^k-1}{n}$ are odd, we get

$$[z_{m,1}, x_k, \overset{2^k-1}{\ldots}, x_k] = \prod_{n=0}^{2^k-1} z_{m+2^k-1-n,1+n} \pmod{\gamma_{2^k+m+1}(G_k)}.$$

Recall that $c_i \in Z_k$ for every $i \geqslant 2^k+1$ by Proposition 7.8, so $z_{m+2^k-1-n,1+n} = 1$ for all $n \leqslant m-2$. Thus,

$$\begin{aligned}[z_{m,1}, x_k, \overset{2^k-1}{\ldots}, x_k] &= \prod_{n=m-1}^{2^k-1} z_{m+2^k-1-n,1+n} \pmod{\gamma_{2^k+m+1}(G_k)} \\ &= \prod_{n=0}^{2^k-m} z_{2^k-n,m+n} \pmod{\gamma_{2^k+m+1}(G_k)} \\ &= \prod_{n=0}^{2^k-m/2} z_{2^k-n,m+n} \prod_{n=m/2+1}^{2^k-m} z_{2^k-n,m+n} \pmod{\gamma_{2^k+m+1}(G_k)}.\end{aligned}$$

As $z_{i,j} = z_{j,i}^{-1}$ for all $i, j \in \mathbb{N}$ and since m is even, we finally obtain

$$[z_{m,1}, x_k, \overset{2^k-1}{\ldots}, x_k] \equiv 1 \pmod{\gamma_{2^k+m+1}(G_k)},$$

as required. □

We are now able to describe explicitly the terms of the lower central series of the groups G_k. We will omit the proof of Proposition 7.25 since it is the same as the proof of Proposition 7.11 in nature. One only needs to adapt it to the pro-2 group G taking into account the results in Proposition 7.22 and Lemmas 7.23 and 7.24.

Proposition 7.25. *For $k \in \mathbb{N}$, the nilpotency class of G_k is $2^{k+1}-1$ and the lower central series of G_k satisfies:*

- $\gamma_1(G_k) = G_k = \langle x_k, y_k \rangle \gamma_2(G_k)$ *with*

$$\gamma_1(G_k)/\gamma_2(G_k) \cong C_{2^k} \times C_2.$$

- *If $2 \leqslant i \leqslant 2^k$, then*

$$\gamma_i(G_k) = \begin{cases} \langle c_i, c_{2,i-2}, c_{4,i-4}, \ldots, c_{i-2,2} \rangle \gamma_{i+1}(G_k) & \text{if } i \equiv_2 0, \\ \langle c_i, c_{2,i-2}, c_{4,i-4}, \ldots, c_{i-1,1} \rangle \gamma_{i+1}(G_k) & \text{if } i \equiv_2 1, \end{cases}$$

with

$$\gamma_i(G_k)/\gamma_{i+1}(G_k) \cong \begin{cases} C_4 \times C_2 \times \overset{(i-2)/2}{\ldots} \times C_2 & \text{if } 2 \leqslant i \leqslant 2^{k-1} \text{ and } i \equiv_2 0, \\ C_4 \times C_2 \times \overset{(i-1)/2}{\ldots} \times C_2 & \text{if } 2 \leqslant i \leqslant 2^{k-1} \text{ and } i \equiv_2 1, \\ C_2 \times \overset{i/2}{\ldots} \times C_2 & \text{if } 2^{k-1}+1 \leqslant i \leqslant 2^k \text{ and } i \equiv_2 0, \\ C_2 \times \overset{(i+1)/2}{\ldots} \times C_2 & \text{if } 2^{k-1}+1 \leqslant i \leqslant 2^k \text{ and } i \equiv_2 1. \end{cases} \tag{7.17}$$

- *If* $2^k + 1 \leqslant i \leqslant 2^k + 2^{k-1}$, *then*

$$\gamma_i(G_k) = \begin{cases} \langle c_i, c_{i-2^k+2,2^k-2}, c_{i-2^k+4,2^k-4}, \ldots, c_{2^k-2,i-2^k+2}, c_{2^k,i-2^k} \rangle \gamma_{i+1}(G_k) & \text{if } i \equiv_2 0, \\ \langle c_i, , c_{i-2^k+1,2^k-1}, c_{i-2^k+3,2^k-3}, \ldots, c_{2^k-2,i-2^k+2}, c_{2^k,i-2^k} \rangle \gamma_{i+1}(G_k) & \text{if } i \equiv_2 1, \end{cases}$$

with

$$\gamma_i(G_k)/\gamma_{i+1}(G_k) \cong \begin{cases} C_2 \times \overset{(2^{k+1}-i+2)/2}{\cdots} \times C_2 & \text{if } i \equiv_2 0, \\ C_2 \times \overset{(2^{k+1}-i+3)/2}{\cdots} \times C_2 & \text{if } i \equiv_2 1. \end{cases} \tag{7.18}$$

- *If* $2^k + 2^{k-1} + 1 \leqslant i \leqslant 2^{k+1}$, *then*

$$\gamma_i(G_k) = \begin{cases} \langle c_{i-2^k+2,2^k-2}, c_{i-2^k+4,2^k-4}, \ldots, c_{2^k-2,i-2^k+2}, c_{2^k,i-2^k} \rangle \gamma_{i+1}(G_k) & \text{if } i \equiv_2 0, \\ \langle c_{i-2^k+1,2^k-1}, c_{i-2^k+3,2^k-3}, \ldots, c_{2^k-2,i-2^k+2}, c_{2^k,i-2^k} \rangle \gamma_{i+1}(G_k) & \text{if } i \equiv_2 1, \end{cases}$$

with

$$\gamma_i(G_k)/\gamma_{i+1}(G_k) \cong \begin{cases} C_2 \times \overset{(2^{k+1}-i)/2}{\cdots} \times C_2, & \text{if } i \equiv_2 0, \\ C_2 \times \overset{(2^{k+1}-i+1)/2}{\cdots} \times C_2 & \text{if } i \equiv_2 1. \end{cases} \tag{7.19}$$

Remark 7.26. From Proposition 7.25 we deduce that the logarithmic order of $Z/(\gamma_n(G) \cap Z)$ is

$$2\Big(1 + 2 + \ldots + \frac{n-1}{2}\Big) = 2\binom{(n+1)/2}{2} = \frac{n^2-1}{4}$$

if n is odd or

$$2\Big(1 + 2 + \ldots + \frac{n-2}{2}\Big) + \frac{n}{2} = 2\binom{n/2}{2} + \frac{n}{2} = \frac{n^2}{4}$$

if n is even.

With Proposition 7.25 the lower 2-series and the dimension subgroup series of G_k can be deduced easily.

Proposition 7.27. *For* $k \in \mathbb{N}$, *the length of the lower* 2*-series of* G_k *is* $2^{k+1} - 1$ *and it satisfies*

$$P_1(G_k) = G_k$$

and

$$P_i(G_k) = \begin{cases} \langle x_k^{2^{i-1}}, c_{i-1}^2 \rangle \gamma_i(G_k) & \text{for } 2 \leqslant i \leqslant 2^{k-1} + 1, \\ \langle x_k^{2^{i-1}} \rangle \gamma_i(G_k) & \text{for } 2^{k-1} + 2 \leqslant i \leqslant 2^{k+1}. \end{cases}$$

Proof. If $i = 1$ or 2, the results are obvious, so consider $i = 3$. As

$$[\langle x_k^2, y_k^2 \rangle, G_k] \leqslant \gamma_2(G_k)^2 \gamma_3(G_k),$$

it suffices to show that $\langle x_k^2, y_k^2 \rangle^2 \leqslant \langle x_k^4 \rangle \gamma_3(G_k)$ and $\gamma_2(G_k)^2 \leqslant \langle c_2^2 \rangle \gamma_3(G_k)$. Note that

$$[y_k^2, x_k^2] \equiv [y_k, x_k]^4 = 1 \pmod{\gamma_3(G_k)},$$

and since $x_k^4, y_k^4 \in \langle x_k^4 \rangle \gamma_3(G_k)$, the first inclusion holds. The second inclusion follows from Proposition 7.25, as $[y_k, x_k]$ is the only generator of $\gamma_2(G_k)$ modulo $\gamma_3(G)$.

Now let $4 \leqslant i \leqslant 2^{k-1}$ and assume by induction that

$$P_{i-1}(G_k) = \langle x_k^{2^{i-2}}, c_{i-2}^2 \rangle \gamma_{i-1}(G_k).$$

On the one hand,

$$[P_{i-1}(G_k), G_k] = [\langle x_k^{2^{i-2}}, c_{i-2}^2 \rangle \gamma_{i-1}(G_k), G_k] = [\langle x_k^{2^{i-2}}, c_{i-2}^2 \rangle, G_k] \gamma_i(G_k)$$

and Proposition 7.25 and Lemma 2.6 yield

$$[\langle x_k^{2^{i-2}}, c_{i-2}^2 \rangle, G_k] \gamma_i(G_k) = [\langle c_{i-2}^2 \rangle, G_k] \gamma_i(G_k).$$

Then by similar arguments as above, one deduces that

$$[c_{i-2}^2, G_k] \gamma_i(G_k) = \langle c_{i-1}^2 \rangle \gamma_i(G_k).$$

On the other hand,

$$P_{i-1}(G_k)^2 \equiv \langle x_k^{2^{i-2}} \rangle^2 \gamma_{i-1}(G_k)^2 \equiv \langle x_k^{2^{i-1}}, c_{i-1}^2 \rangle \pmod{\gamma_i(G_k)},$$

so we conclude that

$$P_i(G_k) = \langle x_k^{2^{i-1}}, c_{i-1}^2 \rangle \gamma_i(G_k),$$

as asserted. The case $2^{k-1} + 2 \leqslant i \leqslant 2^{k+1}$ follows from (ii) of Lemma 7.23. □

Proposition 7.28. *For $k \in \mathbb{N}$, the length of the dimension subgroup series of G_k is 2^{k+1} and*

$$D_i(G_k) = \langle x_k^{2^{l(i)}} \rangle \gamma_{\lceil i/2 \rceil}(G_k)^2 \gamma_i(G_k) \quad \textit{for } 1 \leqslant i \leqslant 2^{k+1},$$

where $l(i) = \lceil \log_2 i \rceil$.

Proof. By [13, Theorem 11.2], we have

$$D_i(G_k) = \prod_{n \cdot 2^m \geqslant i} \gamma_n(G_k)^{2^m}$$

for every $i \in \mathbb{N}$, and since $\exp(\gamma_2(G_k)) = 4$, we obtain

$$D_i(G_k) = G_k^{2^{l(i)}} \gamma_{\lceil i/2 \rceil}(G_k)^2 \gamma_i(G_k).$$

The result is clear for $i = 1, 2$, so we assume $i \geqslant 3$. By Lemma 2.6, since the exponent of H is 4, for every $a, b \in G_k$ it follows that

$$(ab)^{2^{l(i)}} = a^{2^{l(i)}} b^{2^{l(i)}} [b, a, {}^{2^{l(i)-1}\cdots-1}, a]^{\binom{2^{l(i)}}{2^{l(i)-1}}} c$$

with $c \in \gamma_{2^{l(i)}}(G_k)$. Since $[b, a, {}^{2^{l(i)-1}\cdots-1}, a]^{\binom{2^{l(i)}}{2^{l(i)-1}}} \in \gamma_{\lceil i/2 \rceil}(G_k)^2$ and $\gamma_{2^{l(i)}}(G_k) \leqslant \gamma_i(G_k)$, we get

$$D_i(G_k) = \langle x_k^{2^{l(i)}} \rangle \gamma_{\lceil i/2 \rceil}(G_k)^2 \gamma_i(G_k),$$

as required. □

7.3.2 The normal Hausdorff spectra for $p = 2$

In this section we compute the normal Hausdorff spectra of G with respect to the standard filtration series $\mathcal{L}$, $\mathcal{D}$, $\mathcal{P}$, and $\mathcal{F}$.

Again, we will split the proof of Theorem 7.20 into three parts. We start with the filtration series $\mathcal{L}$ and $\mathcal{D}$.

Theorem 7.29. *The pro-2 group G has full normal Hausdorff spectra*

$$\mathrm{hspec}^{\mathcal{L}}_{\trianglelefteqslant}(G) = [0,1] \qquad \textit{and} \qquad \mathrm{hspec}^{\mathcal{D}}_{\trianglelefteqslant}(G) = [0,1]$$

with respect to the lower p-series $\mathcal{L}$ and the dimension subgroup series $\mathcal{D}$.

Proof. By Remark 7.26 we have

$$\liminf_{i\to\infty} \frac{i}{\log_2 |Z : P_i(G) \cap Z|} = 0 \quad \text{and} \quad \liminf_{i\to\infty} \frac{i}{\log_2 |Z : D_i(G) \cap Z|} = 0,$$

and they are furthermore given by proper limits. The proof now follows as in Theorem 7.15. □

For the filtration series $\mathcal{P}$, we define for all $n \in \mathbb{N}$ the subgroups

$$\Gamma_n = \langle x^{2^n} \rangle \gamma_{2^{n-1}}(G)^2 \gamma_{2^n}(G) \trianglelefteqslant G.$$

Lemma 7.30. *For each $n \in \mathbb{N}$, we have $\Gamma_n^2 \leqslant \Gamma_{n+1}$.*

Proof. We only have to check that $\Gamma_n' \leqslant \Gamma_{n+1}$. Clearly

$$[\gamma_{2^{n-1}}(G)^2, \gamma_{2^{n-1}}(G)^2 \gamma_{2^n}(G)] = 1$$

and $[\gamma_{2^n}(G), \gamma_{2^n}(G)] \leqslant \gamma_{2^{n+1}}(G) \leqslant \Gamma_{n+1}$, so it suffices to prove that

$$[\langle x^{2^n} \rangle, \gamma_{2^{n-1}}(G)^2 \gamma_{2^n}(G)] \leqslant \Gamma_{n+1}.$$

On the one hand, since the exponent of H is 4, Lemma 2.6 yields

$$[\gamma_{2^n}(G), x^{2^n}] \leqslant \gamma_{2^n+2^{n-1}}(G)^2 \gamma_{2^{n+1}}(G) \leqslant \Gamma_{n+1}.$$

On the other hand, for $2^{n-1} \leqslant i \leqslant 2^n - 1$, again by Lemma 2.6 we have

$$[c_i, x^{2^n}] \in \gamma_{2^n}(G)^2 \gamma_{2^n+2^{n-1}}(G),$$

so

$$[c_i^2, x^{2^n}] = [c_i, x^{2^n}]^2 [c_i, x^{2^n}, c_i] \in \Gamma_{n+1},$$

as required. □

Theorem 7.31. *The pro-2 group G has full normal Hausdorff spectrum*

$$\mathrm{hspec}^{\mathcal{P}}_{\trianglelefteqslant}(G) = [0,1]$$

with respect to the 2-power series $\mathcal{P}$.

Proof. An arbitrary element of G can be written as $x^n h$ with $h \in H$ and $n \in \mathbb{Z}_2$, and by Lemma 2.6, it follows that $(x^n h)^{2^k} \in \Gamma_k$. Then $G^{2^k} \leqslant \Gamma_k$ and, in particular, $G^{2^k} \cap Z \leqslant \Gamma_k \cap Z$. It is easy to see that

$$\Gamma_k \cap Z = (\gamma_{2^{k-1}}(G)^2 \gamma_{2^k}(G)) \cap Z = \gamma_{2^{k-1}}(G)^2 (\gamma_{2^k}(G) \cap Z),$$

and since $[\gamma_{2^{k-1}}(G), \gamma_{2^{k-1}}(G)] \leqslant \gamma_{2^k}(G) \cap Z$, it follows that

$$\gamma_{2^{k-1}}(G)^2 \leqslant \langle c_{2^{k-1}}^2, c_{2^{k-1}+1}^2, \ldots, c_{2^k-1}^2 \rangle (\gamma_{2^k}(G) \cap Z).$$

Thus, by Remark 7.26, we have

$$\log_2 |Z : \Gamma_k \cap Z| = \log_2 |Z : \gamma_{2^{k-1}}(G)^2 (\gamma_{2^k}(G) \cap Z)| = 2 \binom{2^{k-1}}{2}.$$

On the other hand, as in the proof of Theorem 7.16 we deduce that $\gamma_{2^{k+1}}(G) \leqslant G^{2^k}$. Thus,

$$\lim_{k \to \infty} \frac{2^{k+1}}{\log_2 |Z : \Gamma_k \cap Z|} = 0,$$

and we conclude as in Theorem 7.16. □

We are now concerned with the Frattini series $\mathcal{F}$. As in the p odd case, the result for this filtration is more technical than for the other filtrations. Even though the proof of Theorem 7.32 is very similar to the proof of Theorem 7.19, we will give all the main computations, as there are slight differences in many of the steps.

Since clearly $z_{i,j} \in \gamma_{i+j}(G)$, we deduce from Proposition 7.22 and Remark 7.26 that

$$\gamma_n(G) \cap Z = \langle c_l^2, z_{i,j} \mid 1 \leqslant j < i, i + j \geqslant n, l \geqslant n \rangle$$

for every $n \geqslant 2$.

Theorem 7.32. *The pro-2 group G has full normal Hausdorff spectrum*

$$\operatorname{hspec}_{\trianglelefteqslant}^{\mathcal{F}}(G) = [0, 1]$$

with respect to the Frattini series $\mathcal{F}$.

Proof. We claim that

$$T_k(\gamma_{2^k + 2^{k-1} - 1}(G) \cap Z) \leqslant \Phi_k(G) \leqslant \Gamma_k$$

where

$$T_k = \langle x^{2^k}, c_i^2, c_j \mid i \geqslant 2^{k-1}, j \geqslant 2^k \rangle$$

for all $k \in \mathbb{N}$. We will proceed by induction on k. If $k = 1$ the result is clear, so assume $k \geqslant 2$. On the one hand, it follows from Lemma 7.30 that

$$\Phi_k(G) = \Phi_{k-1}(G)^2 \leqslant \Gamma_{k-1}^2 \leqslant \Gamma_k.$$

Hence, it suffices to check that

$$T_k(\gamma_{2^k + 2^{k-1} - 1}(G) \cap Z) \leqslant \Delta,$$

where

$$\Delta = \Phi\big(T_{k-1}(\gamma_{2^{k-1}+2^{k-2}-1}(G) \cap Z)\big).$$

Of course we have $x^{2^k}, c_i^2 \in \Delta$ for all $i \geqslant 2^{k-1}$. We also have $T'_{k-1} \leqslant \Delta$, so $\langle z_{i,j} \mid i > j \geqslant 2^{k-1} \rangle \leqslant \Delta$. Let us see that $z_{i,j} \in \Delta$ whenever $i > j$, $i + j \geqslant 2^k + 2^{k-1} - 1$ and $j \leqslant 2^{k-1} - 1$. Consider the element $z_{i-2^{k-1},j}$ and observe that

$$z_{i-2^{k-1},j} \in \gamma_{2^k-1}(G) \cap Z$$

as

$$i - 2^{k-1} + j \geqslant 2^k - 1.$$

Therefore $[z_{i-2^{k-1},j}, x^{2^{k-1}}] \in \Delta$. By Corollary 7.18, it follows then that

$$z_{i,j} z_{i-2^{k-1},j+2^{k-1}} z_{i,j+2^{k-1}} \in \Delta.$$

On the one hand, we have $i > j + 2^{k-1}$ and $j + 2^{k-1} \geqslant 2^{k-1}$, so $z_{i,j+2^{k-1}} \in \Delta$. On the other hand, if $i - 2^{k-1} > j + 2^{k-1}$, then $z_{i-2^{k-1},j+2^{k-1}} \in \Delta$, and if $i - 2^{k-1} \leqslant j + 2^{k-1}$, then as $i - 2^{k-1} \geqslant 2^{k-1}$, we have

$$z_{i-2^{k-1},j+2^{k-1}} = z^{-1}_{j+2^{k-1},i-2^{k-1}} \in \Delta.$$

Therefore, $z_{i,j} \in \Delta$ and $\gamma_{2^k+2^{k-1}-1}(G) \cap Z \leqslant \Delta$.

Finally, for $j \geqslant 2^{k-1}$, observe that

$$[c_j, x^{2^{k-1}}] \equiv c^2_{j+2^{k-2}} c_{j+2^{k-1}} \pmod{\gamma_{2j+2^{k-1}}(G) \cap Z},$$

and since $\gamma_{2j+2^{k-1}}(G) \cap Z \leqslant \Delta$ and $c_i^2 \in \Delta$ for all $i \geqslant 2^{k-1}$, it follows that $c_j \in \Delta$ for all $j \geqslant 2^k$. We conclude that

$$T_k\big(\gamma_{2^k+2^{k-1}-1}(G) \cap Z\big) \leqslant \Delta \leqslant \Phi_k(G),$$

as claimed. In particular, we get

$$\gamma_{2^k+2^{k-1}-1}(G) \cap Z \leqslant \Phi_k(G) \cap Z \leqslant \Gamma_k \cap Z.$$

Now, from Remark 7.26 we deduce that

$$\liminf_{k\to\infty} \frac{2^k + 2^{k-1} - 1}{\log_2 |Z : \Gamma_k \cap Z|} = \lim_{k\to\infty} \frac{2^k + 2^{k-1} - 1}{\log_2 |Z : \Gamma_k \cap Z|} = 0. \tag{7.20}$$

We conclude as in the proof of Theorem 7.19. □

Again, Theorem 7 summarises the results in Theorems 7.29, 7.31 and 7.32.

Part III

Powerfully solvable and powerfully simple p-groups

Chapter 8

A brief introduction to powerfully nilpotent and powerfully solvable groups

Powerful groups have been, without any doubt, one of the main protagonists of Part I of the thesis. Indeed, they have been a good "platform" in which commutator calculus behaves particularly well. In this last part of the thesis we will make a further study of the theory of such groups, deepening in this way the knowledge on this topic.

For the purpose of bringing some order to the huge category of finite groups, one uses to classify them into some (not necessarily disjoint) subfamilies of groups. For instance, we can consider the families of finite simple groups, finite nilpotent groups, finite p-groups, finite solvable groups (or equivalently finite polycyclic groups), finite metabelian groups, finite supersolvable groups, etc.

When we focus, though, in the (still huge) family of finite p-groups, it does not make sense to consider the subfamily of finite nilpotent p-groups (which would coincide with the whole family of finite p-groups) or the subfamily of finite simple p-groups (which would consist only of the group C_p). The subclasses that one considers for these groups are thus more specific and must be tailored to the particular group structure of the finite p-groups.

However, we will see that in the family of powerful groups, there is a way in which one can consider subfamilies in an analogous way as for general finite groups. The way to do this is somehow assigning the role that the subgroups and the normal subgroups have in the context of general finite groups, to the *powerful* subgroups and the *powerfully embedded* subgroups of powerful groups, respectively.

This idea started with the notion of *powerfully nilpotent* group, which can be seen as the "powerful version" of the notion of finite nilpotent groups.

Definition 8.1. Let G be a finite p-group. If $K \leqslant H \leqslant G$, then a chain of subgroups

$$H = H_0 \geqslant H_1 \geqslant \cdots \geqslant H_n = K$$

is *powerfully central in* G if $[H_i, G] \leqslant H_{i+1}^p$ for all $i = 0, \ldots, n-1$.

Definition 8.2. A finite p-group G is said to be *powerfully nilpotent* if it has a powerfully central series

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = 1.$$

The smallest possible length of such a series is called the *powerful nilpotency class* of G.

This concept was introduced by Traustason and Williams in [75], where some general theory of powerfully nilpotent groups is developed. A remarkable result is that powerful nilpotence leads naturally to a classification in terms of what the authors call powerful coclass (the powerful coclass of a powerfully nilpotent group G of order p^n and powerful nilpotency class c is the number $n - c$). Thus, they show that for every prime p there are finitely many powerfully nilpotent p-groups for each given powerful coclass. They also determine the growth of powerfully nilpotent groups of exponent p^2 with respect to the order p^n: they show that the growth of such groups is $f(n) = p^{\alpha n^3 + o(n^3)}$ where $\alpha = (9 + 4\sqrt{2})/394$.

The study of these groups continued in [76], where the powerfully nilpotent groups of maximal powerful class are introduced. These groups can be seen as the analogous of finite p-groups of maximal class. Thus, it is shown that for any given positive integer r and prime $p > r$, there exists a powerfully nilpotent group of maximal powerful class, and their structure is analysed.

More about these groups can be found in [79] and [80], where, among other things, it is reflected that powerfully nilpotent groups arise naturally in the theory of finite p-groups; and in [77], where a full classification of, on the one hand, all powerfully nilpotent p-groups of rank 2, and on the other hand, all the powerfully nilpotent p-groups of order up to p^6, is given.

In the first half of Part III we will consider a natural larger class of powerful groups, namely, the *powerfully solvable groups*.

Definition 8.3. Let G be a finite p-group and $K \leqslant H \leqslant G$. We say that a chain

$$H = H_0 \geqslant H_1 \geqslant \cdots \geqslant H_n = K$$

is *powerfully abelian* if $[H_i, H_i] \leqslant H_{i+1}^p$ for all $i = 0, \ldots, n-1$.

Definition 8.4. A finite p-group G is *powerfully solvable* if there exists a powerfully abelian chain

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = 1.$$

The smallest possible length n is called the *powerful derived length* of G.

It is natural to think that we could define powerfully simple groups as the powerful groups with no proper non-trivial powerfully embedded subgroups. Nevertheless, this notion is not as satisfactory as one could expect, as the unique powerfully simple p-group would be C_p. Hence, we will be forced to define powerfully simple groups in a more restrictive family than that of powerful groups. In order to define it, we recall from Proposition 2.10 that all powerful groups have a basis. We will refer to it as a *powerful basis* of G, where G is a powerful group.

Definition 8.5. Let G be a powerful group and let $\{a_1, \ldots, a_r\}$ be a powerful basis of G, so that $|G| = o(a_1) \cdots o(a_r)$. We say that G is of *type*

$$(1, \overset{r_1}{\ldots}, 1, 2, \overset{r_2}{\ldots}, 2, \ldots)$$

if there are r_i generators of order p^i for every $i \geqslant 1$.

Note by (iii) of Proposition 2.8 that the number of generators of a powerful basis of order greater than or equal to p^n, where $n \geqslant 1$, is precisely $\log_p |G^{p^{n-1}} : G^{p^n}|$, so the number of generators of any given order of a basis of G is an invariant of the group. This means that the type of G is well defined. The family of groups in which the notion of powerfully simple groups will be defined is the rich family $\mathcal{P}$ of groups of type $(2, \overset{r}{\ldots}, 2)$ with $r \geqslant 1$. This will be discussed in Chapter 10.

All the results and ideas in Chapters 9 and 10 are collected in [36].

Chapter 9

Powerfully solvable groups

We focus now on some general aspects of the theory of powerfully solvable groups. In the remainder let p denote an odd prime.

We start in Section 9.1 by studying powerful groups of rank 2. On the one hand, we will show that all powerful p-groups of rank 2 are powerfully solvable, and on the other hand, based on the work in [77], we provide a classification of all these groups as well as a closed formula for the number of such groups of order p^k.

The notion of powerfully nilpotent presentation introduced in [75] is one of the most important characteristics of powerfully nilpotent groups, as it allows to describe them in a very explicit way. In Section 9.2 we extend this to powerfully solvable groups, introducing the notion of a *powerfully solvable presentation*. This will be useful later on when going through some classification and calculating growth.

With this, we classify in Section 9.3 all powerful groups of order up to p^5. As we will see, it turns out that these are all powerfully solvable.

Finally, based on [75], we discuss in Section 9.4 the growth of powerfully solvable groups of exponent p^2 and various other classes of powerful groups, like the powerful groups of type $(2, \dots, 2)$, which will be the central issue of Chapter 10.

9.1 Powerful groups of rank 2

We start with a basic criterion for the powerful solvability.

Proposition 9.1. *Let G be a powerful p-group. If $[G, G]$ is cyclic then G is powerfully solvable of powerful derived length at most 2.*

Proof. As G is powerful we have that $[G, G] = \langle g^p \rangle$ for some $g \in G$. Therefore

$$G \geqslant \langle g \rangle \geqslant 1$$

is a powerfully abelian chain. □

Let G be a powerful group generated by 2 elements, say $x, y \in G$. Then, $G' = \langle [x, y] \rangle \gamma_3(G)$, but since $\gamma_3(G) = [G', G] \leqslant (G')^p = \Phi(G')$, it follows that $G' = \langle [a, b] \rangle$,

so that G' is cyclic. Therefore, according to Proposition 9.1, powerful groups of rank 2 are all powerfully solvable.

Furthermore, suppose $[x,y] = g^{p^k}$ for some $g \in G \backslash G^p$ and $k \geqslant 1$. Then there exists $h \in G$ such that $G = \langle g, h \rangle$, and since $G' \leqslant \langle g \rangle$, it follows that $\langle g \rangle$ is normal in G. In addition, $G/\langle g \rangle$ is clearly cyclic, so it follows that powerful groups of rank 2 all are metacyclic.

In [41, Chapter 11] a classification of all finite metacyclic p-groups is given, and in particular, if one singles out the powerful groups of rank 2, a full classification for them can be obtained. Alternatively, in [77] the powerfully nilpotent groups of rank 2 are classified and a closed formula is found for the number of powerfully nilpotent groups of order p^k. In fact, there is implicitly the following classification of all powerful p-groups of rank 2.

Theorem 9.2. *The powerful groups of rank* 2 *are divided in the following two families of groups:*

(i) *Semidirect products:*

$$G = \langle a, b \mid a^{p^n} = b^{p^m} = 1,\ [a,b] = a^{p^r} \rangle$$

with $n - r \leqslant m$ *and* $1 \leqslant r \leqslant n-1$.

(ii) *Non-semidirect products:*

$$G = \langle a, b \mid a^{p^n} = 1,\ b^{p^m} = a^{p^l},\ [a,b] = a^{p^r} \rangle$$

with $1 \leqslant r < l \leqslant n-1$ *and* $n - r \leqslant l < m$.

Moreover, all these groups are pairwise non-isomorphic.

From [77] we also know that a group above is powerfully nilpotent if and only if $r \geqslant 2$. Thus, it is easy to determine that there are $\lfloor \frac{k-1}{2} \rfloor$ semidirect products and $\lfloor \frac{k-4}{2} \rfloor$ non-semidirect products of order p^k that are not powerfully nilpotent. From this, the discussion above and [77, Proposition 2.2] we also get the following enumeration.

Theorem 9.3. *For* $k \geqslant 3$, *the number of powerful* p*-groups of rank* 2 *and order* p^k *is*

$$\begin{aligned}
\frac{k^3+12k^2+12k}{72} &\quad \text{if} \quad k \equiv_6 0,\\
\frac{k^3+12k^2+3k-16}{72} &\quad \text{if} \quad k \equiv_6 1,\\
\frac{k^3+12k^2+12k-8}{72} &\quad \text{if} \quad k \equiv_6 2,\\
\frac{k^3+12k^2+3k}{72} &\quad \text{if} \quad k \equiv_6 3,\\
\frac{k^3+12k^2+12k-16}{72} &\quad \text{if} \quad k \equiv_6 4,\\
\frac{k^3+12k^2+3k-8}{72} &\quad \text{if} \quad k \equiv_6 5.
\end{aligned}$$

Proof. This can be verified by routine computations just noting that the semidirect products in Theorem 9.2 have order p^{n+m}, while the non-semidirect products have order p^{n+m-l}. □

9.2 Powerful presentations

Our aim in this section is to find suitable generators that not only form a powerful basis of G, but also satisfy special relations that will yield what we will call a *powerfully solvable presentation* of G. The next lemma is essential for this purpose.

Lemma 9.4. *Let G be a finite p-group and let $K < H \leqslant G$ where $[H,H] \leqslant K^p$. If for some positive integer n we have $K^{p^n} = H^{p^n}$, then there exists $x \in H \backslash K$ such that $x^{p^n} = 1$.*

Proof. Observe that

$$[K,K] \leqslant [H,H] \leqslant K^p \leqslant H^p,$$

so both H and K are powerful. By Lemma 2.13 they are power abelian, so in particular, $|H : H^{p^n}| = |\Omega_n(H)|$ and $|K : K^{p^n}| = |\Omega_n(K)|$. Now, since $K < H$ and $H^{p^n} = K^{p^n}$, we must have $\Omega_n(K) < \Omega_n(H)$, so take $x \in \Omega_n(H) \backslash \Omega_n(K)$. Thus, the order of x is p^n and $x \in H \backslash K$, as desired.

□

Note that the property of being powerfully solvable is preserved under taking quotients. In particular, if G is powerfully solvable, then so is G/G^{p^2}. As next theorem shows, the converse is also true. Furthermore, there exists a special generating set of G that, arranged in a specific way, gives a suitable powerfully abelian chain.

Theorem 9.5. *Let G be a finite p-group of rank r and exponent p^e where G/G^{p^2} is powerfully solvable. Then G is powerfully solvable. Furthermore, we can choose our generators $a_1, a_2, \ldots, a_r$ such that $|G| = o(a_1) \cdots o(a_r)$ and such that the chain*

$$\begin{array}{rcccl}
G = \langle a_1, a_2, \ldots, a_r \rangle & \geqslant & \langle a_1^p, a_2, \ldots, a_r \rangle & \geqslant \cdots \geqslant & G^p \\
G^p = \langle a_1^p, a_2^p, \ldots, a_r^p \rangle & \geqslant & \langle a_1^{p^2}, a_2^p, \ldots, a_r^p \rangle & \geqslant \cdots \geqslant & G^{p^2} \\
 & \vdots & & & \\
G^{p^{e-1}} = \langle a_1^{p^{e-1}}, a_2^{p^{e-1}}, \ldots, a_r^{p^{e-1}} \rangle & \geqslant & \langle a_1^{p^e}, a_2^{p^{e-1}}, \ldots, a_r^{p^{e-1}} \rangle & \geqslant \cdots \geqslant & G^{p^e} = 1
\end{array}$$

is powerfully abelian.

Proof. Suppose, using the fact that G/G^{p^2} is powerfully solvable, that

$$G = K_0 > K_1 > \cdots > K_m = G^{p^2}$$

is a chain that is powerfully abelian modulo G^{p^2}. Notice that $[G,G] \leqslant K_1^p G^{p^2} \leqslant G^p$ and the group is hence powerful. In particular, we have $[G^p, G] \leqslant G^{p^2}$ and $(G^p)^p = G^{p^2}$. Therefore, the chain

$$G = K_0 G^p \geqslant K_1 G^p \geqslant \cdots \geqslant K_m G^p = G^p$$

is also powerfully abelian. Removing redundant terms and refining if necessary, we get a powerfully abelian chain

$$G = H_0 > H_1 > \cdots > H_r = G^p$$

where the factors are of size p. Now notice that for $0 \leqslant i \leqslant r-1$ and $0 \leqslant j \leqslant e$ we have $[H_i^{p^j}, H_i^{p^j}] = [H_i, H_i]^{p^{2j}} \leqslant H_{i+1}^{p^{j+1}}$. This gives us the powerfully abelian chain we wanted.

It remains to see that we can furthermore pick our generators such that $a_1, \dots, a_r$ is a powerful basis for G. Let us pick our generators of G such that for every $1 \leqslant i \leqslant r-1$ we have $H_i = \langle a_{i+1}, \dots, a_r \rangle G^p$. If

$$H_i^p = H_{i+1}^p \tag{9.1}$$

for some $1 \leqslant i \leqslant r-1$ then we know from Lemma 9.4 that we can pick a_{i+1} such that $a_{i+1}^p = 1$. In addition, note that in general, if $a \in G$ has order p, then

$$[H_i, H_i] \leqslant \langle H_j, a \rangle^p \text{ implies } [H_i, H_i] \leqslant H_j^p \tag{9.2}$$

for every $0 \leqslant i < j \leqslant r-1$.

On the other hand, observe from Lemma 2.14 that $|H_i^p : H_{i+1}^p| \leqslant p$ for all $1 \leqslant i \leqslant r-1$, so the number of times that equality (9.1) happens is exactly $r - \log_p |G^p : G^{p^2}|$. We write $r_1 = \log_p |G^p : G^{p^2}|$, and observe that r_1 coincides with the rank of G^p. Thus, we can reorder the generators and assume that the generators of order p are the $a_1, \dots, a_{r-r_1}$ (we also relabel the other generators keeping the initial order), so that

$$G^p = H_0^p = \cdots = H_{r-r_1}^p > \cdots > H_r^p = G^{p^2}.$$

Indeed, in such a case, it follows from (9.2) that

$$G = H_0 \geqslant \cdots \geqslant H_r = G^p$$

is still a powerfully abelian chain. Now consider the chain

$$G^{p^2} = H_{r-r_1}^{p^2} \geqslant \cdots \geqslant H_r^{p^2} = G^{p^3}.$$

Again if $H_i^{p^2} = H_{i+1}^{p^2}$, then we know by Lemma 9.4 that we can pick a_{i+1} such that $a_{i+1}^{p^2} = 1$. Continuing in this manner we see that we can choose our generators such that for $1 \leqslant i \leqslant r$ we have $o(a_i) = p^j$ where j is the smallest positive integer such that $H_{i-1}^{p^j} = H_i^{p^j}$. Also, we have that the rank of G^{p^i} is then the number of $1 \leqslant i \leqslant r$ such that $a_i^{p^j} \neq 1$. Let r_j be the rank of G^{p^j}. Then, since $r_e = 0$, we obtain

$$|G| = p^{r_0 + r_1 + \cdots + r_{e-1}} = p^{r_0 - r_1} \cdot (p^2)^{r_1 - r_2} \cdots (p^{e-1})^{r_{e-1} - r_e} = o(a_1) \cdots o(a_r).$$

This finishes the proof. □

It follows, in particular, from Theorem 9.5 that a powerfully solvable group of order p^n and rank r always have generators $a_1, \dots, a_r$ satisfying the relations

$$a_1^{p^{n_1}} = 1, \dots, a_r^{p^{n_r}} = 1 \tag{9.3}$$

and

$$[a_j, a_i] = a_1^{m_1(i,j)} \cdots a_r^{m_r(i,j)}, \ 1 \leqslant i < j \leqslant r, \tag{9.4}$$

where all the power indices $m_k(i,j)$ are divisible by p and where furthermore $p^2 | m_k(i,j)$ whenever $k \leqslant i$.

Moreover, G is the largest finite p-group satisfying these relations. To see this let H be the largest finite p-group satisfying these relations. The group H/H^{p^2} is powerfully solvable and thus H is powerfully solvable by Theorem 9.5. In particular H is powerful and therefore $|H| \leqslant o(a_1) \cdots o(a_r)$. However, G is a homomorphic image of H and thus $|H| = o(a_1) \cdots o(a_r)$. Hence H is isomorphic to G.

A presentation with generators $a_1, \dots, a_r$ and relations of the form (9.3) and (9.4) is called a *powerfully solvable presentation*. We say that such a presentation is *consistent* if the presentation determines a group of order $p^{n_1} \cdots p^{n_r}$.

9.3 Classification of powerful groups of order up to p^5

In this section we fully classify all powerful p-groups of order up to and including p^5. It turns out that these are all powerfully solvable. As we will see in Section 10.2, the same cannot be said for powerful groups of order p^6, as there many powerful groups of order p^6 that are not powerfully solvable. Though, we will show that non powerfully solvable groups of order p^6 are all of a special kind.

Let us start with our task in this section. There are 2 non-abelian groups of order p^3. The Heisenberg group cannot be powerful, as it is a non-abelian p-group of exponent p. The other group is a semidirect product of a cyclic group of order p^2 by a cyclic group of order p:

$$G_1 = \langle a, b \mid a^{p^2} = b^p = 1,\ [a, b] = a^p \rangle.$$

Notice that this group is powerfully solvable with a powerfully abelian chain $G > \langle a \rangle > 1$. It is, however, not powerfully nilpotent. This comes from the fact that if

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_{n-2} \geqslant G_{n-1} \geqslant G_n = 1$$

is a powerfully central chain of minimal length, then $G_{n-1} \leqslant Z(G)$ and so $[G_{n-2}, G] \leqslant G_{n-1}^p \leqslant Z(G)^p$, which contradicts the assumption of minimality since $Z(G)^p = 1$ and so $G_{n-2} \leqslant Z(G)$. Adding to this the 3 abelian groups of order p^3, we see that there are in total 4 powerful (and also powerfully solvable) groups of order p^3.

Before moving on we consider a general setting like in [77] that includes a number of groups that will occur, namely the non-abelian groups of type $(1, \overset{t}{\ldots}, 1, n)$ where n is an integer greater than 1. Suppose

$$G = \langle a_1, \ldots, a_t, b \rangle$$

is a powerful group of this type where a_i is of order p and b of order p^n. Notice that $G^p = \langle b^p \rangle$ is cyclic and it follows from [75, Corollary 3.3] that $G^p \leqslant Z(G)$. In particular G is nilpotent of class at most 2 and $[G, G]^p = [G^p, G] = 1$. Observe also that $\Omega_1(G) = \langle a_1, \ldots, a_t, b^{p^{n-1}} \rangle$, so $[G, G] = \langle b^{p^{n-1}} \rangle$. Now, consider the vector space $V = \Omega_1(G)G^p/G^p$ over $\mathbb{F}_p$. The commutator operation naturally induces an alternating form on V through

$$(xG^p, yG^p) = \lambda \text{ if } [x, y] = b^{\lambda p^{n-1}}.$$

Without loss of generality we can suppose by [40, Proposition 1] that our generators have been chosen such that we get the following orthogonal decomposition

$$V = \langle a_1G^p, a_2G^p \rangle \oplus \cdots \oplus \langle a_{2s-1}G^p, a_{2s}G^p \rangle \oplus V^\perp$$

where $V^\perp = \langle a_{2s+1}G^p, \ldots, a_tG^p \rangle$ and $(a_{2i-1}G^p, a_{2i}G^p) = 0$ for $i = 1, \ldots, s$. There are now two cases to consider, depending on whether or not $Z(G) \leqslant \Omega_{n-1}(G)$.

Suppose first that $Z(G) \nleqslant \Omega_{n-1}(G)$. This means that $Z(G)$ contains some element $b^l u$ with $u \in \langle a_1, \ldots, a_t \rangle$ and $0 < l < p$. Thus without loss of generality we can assume that $b \in Z(G)$. We thus get a powerful group $G = A(n, t, s)$ with relations

$$\begin{aligned}
&a_1^p = \cdots = a_t^p = b^{p^n} = 1,\\
&[a_{2i-1}, a_{2i}] = b^{p^{n-1}} \text{ for } i = 1, \ldots, s,\\
&[a_i, a_j] = 1 \text{ otherwise for } 1 \leqslant i < j \leqslant t,\\
&[a_i, b] = 1 \text{ for } 1 \leqslant i \leqslant t.
\end{aligned}$$

The groups $A(n,t,s)$ are pairwise non-isomorphic since t and n are clearly invariants of the group and since $|Z(A(n,t,s))| = p^{n+t-2s}$. Notice also that all of them satisfy $\langle b\rangle \leqslant Z(G)$ and $[G,G] \leqslant \langle b^p\rangle$ and thus these groups are all powerfully nilpotent, as was observed in [77]. Notice that for a fixed $n \geqslant 2$ and $t \geqslant 2$ we get $\lfloor t/2\rfloor$ such groups.

We then consider the case when $Z(G) \leqslant \Omega_{n-1}(G)$. Notice first that replacing b by a suitable $ba_1^{\alpha_1}\cdots a_{2s}^{\alpha_{2s}}$, we can assume that b commutes with $a_1,\dots,a_{2s}$. As $b \notin Z(G)$ we then must have $t > 2s$ and similarly, replacing a_i by a suitable $a_{2s+1}^{\alpha_{2s+1}}\cdots a_t^{\alpha_t}$, we can pick our generators $a_{2s+1},\dots,a_t$ such that $[a_{2s+1},b] = b^{p^{n-1}}$ and $[a_{2s+2},b] = \cdots = [a_t,b] = 1$. We thus arrive at a group $G = B(n,t,s)$ satisfying the relations

$$\begin{aligned}
&a_1^p = \cdots = a_t^p = b^{p^n} = 1,\\
&[a_{2i-1},a_{2i}] = b^{p^{n-1}} \text{ for } i = 1,\dots,s,\\
&[a_i,a_j] = 1 \text{ otherwise for } 1 \leqslant i < j \leqslant t,\\
&[a_1,b] = \cdots = [a_{2s},b] = [a_{2s+2},b] = \cdots = [a_t,b] = 1 \text{ for } 1 \leqslant i \leqslant t,\\
&[a_{2s+1},b] = b^{p^{n-1}}.
\end{aligned}$$

Again, the groups $B(n,t,s)$ are pairwise non-isomorphic since $|Z(B(n,t,s)| = p^{n+t-2s-1}$. Notice that for a fixed $n \geqslant 2$ and $t \geqslant 1$ there are $\lfloor (t-1)/2\rfloor$ such groups. Notice also that when $n \geqslant 3$ then the group is powerfully nilpotent as $\langle b^p\rangle \leqslant Z(G)$ and $[G,G] \leqslant \langle b^{p^2}\rangle$. For $n = 2$ this is not the case but the group is still powerfully solvable as we have a powerfully abelian chain $G > \langle b\rangle > 1$ with $[G,G] \leqslant \langle b^p\rangle$.

We are now ready for groups of order p^4. In the following we will omit writing relations of the form $[x,y] = 1$. From our analysis of non-abelian groups of rank 2 we get two such groups:

$$G_2 = \langle a,b \mid a^{p^2} = b^{p^2} = 1,\ [a,b] = a^p\rangle \ \text{ and } \ G_3 = \langle a,b \mid a^{p^3} = b^p = 1,\ [a,b] = a^{p^2}\rangle.$$

Here G_3 is furthermore powerfully nilpotent. The only non-abelian groups apart from these are of type $(1,1,2)$ and from the analysis of such groups above we know there are two groups:

$$G_4 = A(2,2,1) = \langle a,b,c \mid a^p = b^p = c^{p^2} = 1,\ [a,b] = c^p\rangle,$$

and

$$G_5 = B(2,2,0) = \langle a,b,c \mid a^p = b^p = c^{p^2} = 1,\ [a,c] = c^p\rangle.$$

Apart from these there are 5 abelian groups and we thus get in total 9 groups.

Finally we are concern with powerful groups of order p^5. Again our analysis of groups of rank 2 and those of type $(1,1,3)$ and $(1,1,1,2)$ gives us the following non-abelian powerfully solvable groups:

$$\begin{aligned}
G_6 &= \langle a,b \mid a^{p^2} = b^{p^3} = 1,\ [a,b] = a^p\rangle,\\
G_7 &= \langle a,b \mid a^{p^3} = b^{p^2} = 1,\ [a,b] = a^p\rangle,\\
G_8 &= \langle a,b \mid a^{p^3} = b^{p^2} = 1,\ [a,b] = a^{p^2}\rangle,\\
G_9 &= \langle a,b \mid a^{p^4} = b^p = 1,\ [a,b] = a^{p^3}\rangle,
\end{aligned}$$

and

$$\begin{aligned}
G_{10} &= A(3,2,1) = \langle a,b,c \mid a^p = b^p = c^{p^3} = 1,\ [a,b] = c^{p^2}\rangle,\\
G_{11} &= B(3,2,0) = \langle a,b,c \mid a^p = b^p = c^{p^3} = 1,\ [a,c] = c^{p^2}\rangle,\\
G_{12} &= A(2,3,1) = \langle a,b,c,d \mid a^p = b^p = c^p = d^{p^2} = 1,\ [a,b] = d^p\rangle,\\
G_{13} &= B(2,3,0) = \langle a,b,c,d \mid a^p = b^b = c^p = c^{p^2} = 1,\ [a,b] = d^p, [c,d] = d^p\rangle,\\
G_{14} &= B(2,3,1) = \langle a,b,c,d \mid a^p = b^p = c^p = d^{p^2} = 1,\ [a,b] = d^p, [c,d] = d^p\rangle.
\end{aligned}$$

Here $G_8, G_9, G_{10}, G_{11}, G_{12}$ are furthermore powerfully nilpotent. Apart from these 9 groups, there are 7 abelian groups. We are now only left with the non-abelian groups of type $(1,2,2)$ that will contain a number of different groups, so we need to deal with a number of subcases.

Suppose that we have generators a, b, c of orders p, p^2, p^2.

Case 1: $Z(G)^p \neq 1$.

Notice that in this case we must have $|Z(G)^p| = p$ as otherwise $G/Z(G)$ is cyclic and thus G abelian. We can assume that $c \in Z(G)$ and that $Z(G)^p = \langle c^p \rangle$. Notice also that $[G,G] = \langle [a,b] \rangle$ is cyclic. There are two possibilities. On the one hand, if $[G,G] \leqslant Z(G)^p$, then we can choose our generators so that we get a group with the following presentation:

$$G_{15} = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [a,b] = c^p \rangle.$$

On the other hand if $[G,G] \nleqslant Z(G)^p$, then we can choose b such that $[a,b] = b^{pi}$ for some $0 < i \leqslant p-1$, and if j is the inverse of i modulo p, then replacing a by a^j we get a group with presentation

$$G_{16} = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [a,b] = b^p \rangle.$$

Notice that both these groups are powerfully solvable and that G_{15} is furthermore powerfully nilpotent.

Case 2: $Z(G)^p = 1$ and $G/Z(G)$ has rank 2.

In this case we have $Z(G) \leqslant \Omega_1(G) = \langle a, b^p, c^p \rangle$. If $Z(G) \leqslant \langle b^p, c^p \rangle$, then $Z(G) \leqslant G^p$ so $G/Z(G)$ has rank 3, which is a contradiction. Hence we must have $a \in Z(G)$. It is not difficult to see that, as we have done before, we can choose b, c such that $[b,c] = c^p$ and we get the powerfully solvable group

$$G_{17} = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [b,c] = c^p \rangle.$$

Before considering further cases, we first show that if $Z(G)^p = 1$ and $G/Z(G)$ has rank 3, then we must have $[G,G] = G^p$. Note that $|G^p| = p^2$, so suppose by contradiction, that $|G'| = p$. Observe that $G^p \leqslant Z(G)$, so $G/Z(G)$ is a vector space over $\mathbb{F}_p$. Then, the commutator map in G induces a non-degenerate alternating form on $G/Z(G)$, and so $\dim_{\mathbb{F}_p}(G/Z(G))$ is even. This is a contradiction since $G/Z(G)$ has rank 3. We have thus $[G,G] = G^p$. In order to distinguish further between different cases, we next turn our attention to $[\Omega_1(G), G]$. Notice that $\Omega_1(G) = \langle a \rangle G^p$, and since $a \notin Z(G)$, it follows that either $|[\Omega_1(G), G]|$ is of size p or p^2.

Case 3: $Z(G)^p = 1$, $G/Z(G)$ of rank 3 and $|[\Omega_1(G), G]| = p$.

Without loss of generality we can assume that $[\Omega_1(G), G] = \langle c^p \rangle$. There are two possibilities: either $c \in C_G(\Omega_1(G)) = C_G(a)$ or not. Suppose first that $c \in C_G(\Omega_1(G))$. Then we have $[a,c] = 1$, and we can pick b such that $[a,b] = c^p$. Replacing b by bc^l does not change these relations and thus we can assume that $[b,c] = b^{p\alpha}$ for some $0 < \alpha < p$. If we let β be the inverse of α modulo p and we replace a, c by a^β, c^β, then we arrive at a group with presentation

$$G_{18} = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [a,b] = c^p,\ [b,c] = b^p \rangle.$$

Notice that this is a powerfully solvable group with a powerfully abelian chain $G > \langle b, c\rangle > \langle b\rangle > 1$. Suppose now $c \notin C_G(\Omega_1(G))$. Since $|[\Omega_1(G), G]| = |[a, G]| = p$, it follows that the conjugacy class of a has order p, and so $|G : C_G(a)| = p$. Thus, we can pick b such that $b \in C_G(a)$ and $[a, b] = 1$. Replacing a by a suitable power of a we can suppose that $[a, c] = c^p$. As before, replacing b by bc^l does not change these relations, so we can also assume $[b, c] = b^{\alpha p}$ for some $0 < \alpha < p$. Finally, if we let β be the inverse of α modulo p and we replace c by c^β, we arrive at a group with presentation

$$G_{19} = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [a, c] = c^p,\ [b, c] = b^p\rangle.$$

This group is powerfully solvable with powerfully abelian chain $G > \langle b, c\rangle > \langle b\rangle > 1$.

Case 4: $Z(G)^p = 1$, $G/Z(G)$ of rank 3 and $|[\Omega_1(G), G]| = p^2$.

In this case, commutation with a induces a bijective linear map

$$\begin{aligned} F_a : G/\Omega_1(G) &\longrightarrow G^p \\ x\Omega_1(G) &\longmapsto [a, x]. \end{aligned}$$

Identifying $x\Omega_1(G)$ with x^p, we can think of F_a as a linear operator on a 2-dimensional vector space over $\mathbb{F}_p$. Also replacing b, c by a suitable ba^r, ca^s we can assume throughout that $[b, c] = 1$. All these groups are going to be powerfully solvable with powerfully abelian chain $G > \langle b, c\rangle > 1$.

Case 4.1. (F_a is a scalar multiplication). Notice that this property still holds if we replace a by any power of a and thus it is independent of what a we pick in $\Omega_1(G)\backslash G^p$. This is thus a characteristic property of G. Replacing a with a power of itself we can assume that F_a is the identity map. This gives us the group

$$G_{20} = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [a, b] = b^p,\ [a, c] = c^p\rangle.$$

Case 4.2. (F_a is not a scalar multiplication). Again we see that this is a characteristic property of G. We can now pick b and c such that

$$[a, b] = c^p,\ [a, c] = b^{p\alpha}c^{p\beta}.$$

Notice that the matrix for F_a is

$$\begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix}$$

with determinant $-\alpha$. It is easy to see that this is an invariant for the given a that does not depend on our choice of b and c. Now, if we replace a by a^r (and also c by c^r, which does not change the value of the determinant), then we get

$$[a, b] = c^p,\ [a, c] = b^{p\alpha r^2}c^{p\beta r},$$

and the new determinant becomes $-\alpha r^2$. Pick some fixed τ such that $-\tau$ is a non-square in $\mathbb{F}_p$. With appropriate choice of r we can then assume that the determinant of F_a is $-\alpha$ where either $\alpha = -1$ or $\alpha = \tau$. We thus have a group with one of the two presentations

$$G_{21}(\beta) = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [a, b] = c^p,\ [a, c] = b^{-p}c^{p\beta},\ [b, c] = 1\rangle,$$

and

$$G_{22}(\beta) = \langle a, b, c \mid a^p = b^{p^2} = c^{p^2} = 1,\ [a,b] = c^p,\ [a,c] = b^{p\tau}c^{p\beta},\ [b,c] = 1\rangle.$$

Suppose we pick a different $\bar{b} = b^r c^s$. Then for $\alpha \in \{-1, \tau\}$ we have

$$[a, \bar{b}] = [a,b]^r[a,c]^s = c^{pr}(b^{p\alpha}c^{p\beta})^s = b^{ps\alpha}c^{p(r+s\beta)} = \bar{c}^p$$

where $\bar{c} = b^{s\alpha}c^{r+s\beta}$. Then

$$\begin{aligned}[a,\bar{c}] &= [a,b]^{s\alpha}[a,c]^{r+s\beta} \\ &= c^{ps\alpha}(b^{p\alpha}c^{p\beta})^{r+s\beta} \\ &= (b^r c^s)^{p\alpha} \cdot (b^{s\alpha}c^{r+s\beta})^{p\beta} \\ &= \bar{b}^{p\alpha}\bar{c}^{p\beta}.\end{aligned}$$

This shows that for the given $\alpha \in \{-1, \tau\}$, the constant $\beta \in \mathbb{F}_p$ is an invariant, and so we get p distinct groups $G_{21}(\beta)$ and p distinct groups $G_{22}(\beta)$.

Adding up we have 7 abelian groups and the groups $G_6, \ldots, G_{20}, G_{21}(\beta), G_{22}(\beta)$, giving us in total $22 + 2p$ groups of order p^5.

Notice that all powerful groups of order up to and including p^5 are powerfully solvable. Now take a powerful group G of order p^6, and suppose it has a generator a of order p. Hence there exists $H < G$ such that $G = \langle a, H\rangle$, and consequently, since $H' \leqslant G' \leqslant G^p = H^p$, it follows that H is powerful of order p^5. In particular it is also powerfully solvable, so let

$$H = H_0 \geqslant H_1 \geqslant \cdots \geqslant H_n = 1$$

be a powerfully abelian chain of H. As $G' \leqslant H^p$ it then follows that the chain

$$G \geqslant H_0 \geqslant H_1 \geqslant \cdots \geqslant H_n = 1$$

is also powerfully abelian, so G is powerfully solvable. As a consequence, all powerful groups of order p^6 are powerfully solvable with the possible exceptions of some groups of type $(2,2,2)$. However, we will see in Section 10.2 that there are a number of groups of type $(2,2,2)$ that are not powerfully solvable.

9.4 Growth

To end this chapter, following the method introduced in [75], we compute the growth of the powerfully solvable groups of exponent p^2 with respect to the order p^n. So, let G be a powerfully solvable group of exponent p^2 and order p^n. From Theorem 9.5 and the discussion in Section 9.2, we know that we may assume that $G = \langle a_1, \ldots, a_y, a_{y+1}, \ldots, a_{y+x}\rangle$ where $o(a_1) = \cdots = o(a_y) = p$ and $o(a_{y+1}) = \cdots = o(a_{y+x}) = p^2$. Furthermore the generators can be chosen such that $|G| = p^{y+2x}$ and

$$[a_j, a_i] = a_{i+1}^{p\alpha_{i+1}(i,j)} \cdots a_{y+x}^{p\alpha_{y+x}(i,j)},$$

for $1 \leqslant i < j \leqslant y + x$, where $0 \leqslant \alpha_k(i,j) \leqslant p-1$ for $k = i+1, \ldots, y+x$. For each such pair (i,j) with $1 \leqslant i \leqslant y$ there are p^x possible relations for $[a_j, a_i]$, and there are

$yx + \binom{y}{2}$ such pairs. On the other hand, for a pair (i, j) where $y + 1 \leqslant i \leqslant y + x$, for each given i there are $y + x - i$ such pairs and p^{y+x-i} possible relations $[a_j, a_i]$. Adding up we see that the number of solvable presentations is $p^{h(x)}$ where

$$\begin{aligned} h(x) &= \left(yx + \binom{y}{2}\right) x + 1^2 + 2^2 + \cdots (x-1)^2 \\ &= \left((n-2x)x + \binom{n-2x}{2}\right) x + \frac{x(2x-1)(x-1)}{6} \\ &= \frac{1}{3}x^3 - \frac{(2n-1)}{2}x^2 + \frac{3n(n-1)+1}{6}x. \end{aligned}$$

Thus

$$h'(x) = x^2 - (2n-1)x + \frac{3n(n-1)+1}{6},$$

whose roots are $\frac{2n-1}{2} - \sqrt{\frac{1}{2}n^2 - \frac{n}{2} + \frac{1}{12}}$ and $\frac{2n-1}{2} + \sqrt{\frac{1}{2}n^2 - \frac{n}{2} + \frac{1}{12}}$. For large values of n we have that the first root is between 0 and $n/2$ whereas the latter is greater than n. Thus, for large n, the largest value of h in the interval between 0 and $n/2$ is $h(x(n))$ where $x(n) = \frac{2n-1}{2} - \sqrt{\frac{1}{2}n^2 - \frac{n}{2} + \frac{1}{12}}$. Now $\lim_{n\to\infty} x(n)/n = 1 - \frac{1}{\sqrt{2}}$. Therefore

$$\lim_{n\to\infty} \frac{h(x(n))}{n^3} = \lim_{n\to\infty} \frac{1}{3}(x(n)/n)^3 - (x(n)/n)^2 + \frac{1}{2}(x(n)/n)) = \frac{-1+\sqrt{2}}{6}.$$

Now, let us fix n. For any integer x where $0 \leqslant x \leqslant n/2$, let $\mathcal{P}(n, x)$ be the collection of all powerfully solvable presentations as above. It is not difficult to see that those presentations are consistent and thus the resulting group is of order p^n and rank $n - x$. Furthermore $a_1^p = \cdots = a_{n-2x}^p = 1$ and $a_{n-2x+1}^{p^2} = \cdots = a_{n-x}^{p^2} = 1$. We have just seen that, for large values of n, if we pick $x(n)$ such that the number of presentations is maximal then

$$|\mathcal{P}(n, x(n))| = p^{\alpha n^3 + o(n^3)}$$

where $\alpha = \frac{-1+\sqrt{2}}{6}$. Let $\mathcal{P}_n$ be the total number of the powerfully solvable presentations where $0 \leqslant x \leqslant n/2$. Then

$$\mathcal{P}_n = \mathcal{P}(n, 0) \cup \mathcal{P}(n, 1) \cup \cdots \cup \mathcal{P}(n, \lfloor n/2 \rfloor),$$

and thus

$$\begin{aligned} p^{\alpha n^3 + o(n^3)} &= |\mathcal{P}(n, x(n))| \leqslant |\mathcal{P}_n| \\ &= |\mathcal{P}(n, 0)| + \cdots + |\mathcal{P}(n, \lfloor n/2 \rfloor)| \leqslant n|\mathcal{P}(n, x(n))| = p^{\alpha n^3 + o(n^3)}. \end{aligned}$$

This shows that $|\mathcal{P}_n| = p^{\alpha n^3 + o(n^3)}$. Let us see that this is also the growth of powerfully solvable groups of exponent p^2 with respect to the order p^n. Clearly $p^{\alpha n^3 + o(n^3)}$ gives us an upper bound. We want to show that this is also a lower bound. Let $x = x(n)$ be as above and let $a_1, \ldots, a_{n-x}$ be a set of generators for a powerfully solvable group G where $a_1^p = \cdots = a_{n-2x}^p = 1$ and $a_{n-2x+1}^{p^2} = \cdots = a_{n-x}^{p^2} = 1$. Notice that $\langle a_1, \ldots, a_{n-2x} \rangle G^p = \Omega_1(G)$, which is a characteristic subgroup of G. It will be useful to consider a larger class of presentations for powerfully solvable groups of order p^n where we still require

$a_1^p = \cdots = a_{n-2x}^p = 1$ and $a_{n-2x+1}^{p^2} = \cdots = a_{n-x}^{p^2} = 1$. We let $\mathcal{Q}(n,x) = \mathcal{Q}(n,x(n))$ be the collection of all presentations with additional commutator relations

$$[a_i, a_j] = a_1^{p\alpha_1(i,j)} \cdots a_{n-x}^{p\alpha_{n-x}(i,j)} = a_{n-2x+1}^{p\alpha_{n-2x+1}(i,j)} \cdots a_{n-x}^{p\alpha_{n-x}(i,j)}.$$

The presentation is included in $\mathcal{P}(n,x)$ provided the resulting group is powerfully solvable of order p^n. Notice that $G^p \leqslant Z(G)$ and as a result the commutator relations above only depend on the cosets $\overline{a_1} = a_1G^p, \ldots, \overline{a_{n-x}} = a_{n-x}G^p$ and not on the exact values of $a_1, \ldots, a_{n-x}$. Consider the vector space $V = G/G^p$ over $\mathbb{F}_p$ and let $W = \mathbb{F}_p\overline{a_1} + \cdots + \mathbb{F}_p\overline{a_{n-2x}}$. Then let

$$H = \{\phi \in \mathrm{GL}(n-x,p) \mid \phi(W) = W\}.$$

There is now a natural action of H on $\mathcal{Q}(n,x)$. Suppose we have some presentation with generators $a_1, \ldots, a_{n-x}$ as above. Let $\phi \in H$ and suppose

$$\overline{a_i}^{\phi} = \beta_1(i)\overline{a_1} + \cdots + \beta_{n-x}(i)\overline{a_{n-x}}.$$

We then get a new presentation in $\mathcal{Q}(n,x)$ for G with respect to the generators $b_1, \ldots, b_{n-x}$ where $b_i = a_1^{\beta_1(i)} \cdots a_{n-x}^{\beta_{n-x}(i)}$.

Suppose there are l powerfully solvable groups of exponent p^2 and order p^n where furthermore $|G^p| = p^x$. Pick powerfully solvable presentations $p_1, \ldots, p_l \in \mathcal{P}(n,x)$ for these. Let q be a powerfully solvable presentation in $\mathcal{P}(n,x)$ of a group K with generators $b_1, \ldots, b_{n-x}$. Then q is also a presentation for an isomorphic group G with presentation p_i and generators $a_1, \ldots, a_{n-x}$. Let $\phi : K \to G$ be an isomorphism and let $\psi : K/K^p \to G/G^p$ be the corresponding linear isomorphism. This gives us a linear automorphism $\tau \in H$ induced by $\tau(\overline{a_i}) = \psi(\overline{b_i})$. Thus $q = p_i^{\tau}$, and therefore

$$\mathcal{P}(n,x) \subseteq p_1^H \cup p_2^H \cup \cdots \cup p_l^H.$$

Observe that $|H| \leqslant p^{(n-x)^2} \leqslant p^{n^2}$. From this we get

$$p^{\alpha n^3 + o(n^3)} = |\mathcal{P}(n,x)| \leqslant |p_1^H| + \cdots + |p_l^H| \leqslant lp^{n^2},$$

and it follows that $l \geqslant p^{\alpha n^3 + o(n^3)}$. We thus get the following result.

Theorem 9.6. *The number of powerfully solvable groups of exponent p^2 and order p^n is $p^{\alpha n^3 + o(n^3)}$, where $\alpha = \frac{-1+\sqrt{2}}{6}$.*

As mentioned in [75], the growth of all powerful p-groups of exponent p^2 and order p^n is $p^{\beta n^3 + o(n^3)}$ where $\beta = \frac{2}{27}$, so it actually coincides with the growth of all finite p-groups (see [70]). In other words, the growth of the powerful p-groups is the same as the growth of all finite p-groups. This claim was though not proved and we will fill in the details here.

As before we consider a group G of order $p^n = p^{y+2x}$ with generators $a_1, \ldots, a_{y+x}$ where $o(a_1) = \cdots = o(a_y) = p$ and $o(a_{y+1}) = \cdots = o(a_{y+x}) = p^2$. This time we can though include all powerful relations

$$[a_j, a_i] = a_1^{p\alpha_{y+1}(i,j)} \cdots a_{y+x}^{p\alpha_{y+x}(i,j)}$$

for $1 \leqslant i < j \leqslant y + x$, where $0 \leqslant \alpha_k(i,j) \leqslant p-1$ for $k = y+1, \ldots, y+x$. For each such pair (i,j) there are p^x possible relations for $[a_j, a_i]$. We thus see that the number of presentations is $p^{h(x)}$ where

$$h(x) = \binom{y+x}{2}x = \binom{n-x}{2}x = \frac{x^3}{2} - \frac{(2n-1)}{2}x^2 + \frac{n(n-1)}{2}x.$$

Thus

$$h'(x) = \frac{3}{2}\left(x^2 - \frac{2(2n-1)}{3}x + \frac{n(n-1)}{3}\right)$$

and using the same kind of analysis as before we see that for a large n, h takes its maximal value for $x(n) = \frac{2n-1}{3} - \sqrt{\frac{n^2}{9} - \frac{n}{9} + \frac{1}{9}}$. Notice that $\lim_{n\to\infty} \frac{x(n)}{n} = 1/3$. Therefore

$$\lim_{n\to\infty} \frac{h(x(n))}{n^3} = \lim_{n\to\infty} \frac{1}{2}\left(\frac{n-x(n)}{n}\right)\left(\frac{n-1-x(n)}{n}\right)\frac{x(n)}{n} = 2/27.$$

The same argument as above shows then that the growth of all powerful groups of exponent p^2 with respect to order p^n is $p^{\frac{2}{27}n^3+o(n^3)}$.

In Chapter 10 we will be working with a special subclass $\mathcal{P}$ of powerful p-groups, namely those that are of type $(2,\overset{r}{\ldots},2)$ with $r \geqslant 1$. In this case the number of presentations for groups of order p^n, n even, is $p^{h(n)}$ where $h(n) = \frac{n}{2}\binom{n/2}{2}$ and

$$\lim_{n\to\infty} \frac{h(n)}{n^3} = \lim_{n\to\infty} \frac{n/2(n/2-1)n/2}{2n^3} = 1/16.$$

Thus the growth here is $p^{\frac{1}{16}n^3+o(n^3)}$.

Chapter 10

Groups of type $(2, \ldots, 2)$ and powerfully simple groups

In this last chapter of the thesis we will consider the rich class $\mathcal{P}$ of all powerful p-groups of type $(2, \ldots, 2)$. As in the previous chapter, p stands for an odd prime.

In Section 10.1 we will see that powerful nilpotence and powerful solvability play a similar role here as nilpotence and solvability do in the class of all groups. In this way, the notion of a powerfully simple group arises naturally, which are the "powerful analogous" to finite simple groups. Actually, we will be able to prove a Jordan-Hölder-like result that reaffirms this. The main tool to prove it will be a convenient correspondence between the category of all groups in $\mathcal{P}$ with the category of the alternating algebras over $\mathbb{F}_p$.

Finally in Section 10.2 we will fully classify all the powerful groups of type $(2, 2, 2)$. This will be done by identifying such groups with 3×3 matrices over $\mathbb{F}_p$ and by considering a suitable equivalence relation on them. In this equivalent relation two matrices will be equivalent if and only if one is congruent to a scalar multiple of the other. Therefore, identifying these matrices with the bilinear form they define will be really helpful. The number of powerful groups of type $(2, 2, 2)$ turns out to depend on the prime p.

10.1 Groups of type $(2, \ldots, 2)$

We have seen that powerful nilpotence and powerful solvability is preserved under taking quotients. These properties, however, work badly under taking subgroups. Our next result underscores this.

Proposition 10.1. *Let G be any finite p-group of nilpotency class 2. Then there exists a powerfully nilpotent group H of powerful class 2 that contains G as a subgroup. Moreover, if G is powerful, then $\exp(H) = \exp(G)$.*

Proof. Suppose $[G, G]$ has a basis $a_1, \ldots, a_m$ as an abelian group, where $o(a_i) = p^{j_i}$ with $j_i \geqslant 1$ for all $i = 1, \ldots, m$. Let $N = \langle x_1 \rangle \times \cdots \times \langle x_m \rangle$ be a direct product of cyclic groups where $o(x_i) = p^{j_i+1}$. Now define $H = (G \times N)/M$ where $M = \langle a_1 x_1^{-p}, \ldots, a_m x_m^{-p} \rangle$. Then

G clearly embeds as a subgroup of H. Notice also that

$$1 \leqslant \langle x_1, \dots, x_m \rangle \leqslant H$$

is powerfully central and thus H is powerfully nilpotent of powerful class 2. Moreover, if G is powerful, then we have

$$\log_p \exp(N) = \log_p \exp(G') + 1 \leqslant \log_p \exp(G),$$

and so the exponent of H equals the exponent of G. □

This shows that the subgroup structure of a powerfully nilpotent group of powerful class 2 is quite arbitrary. As powerful groups of exponent p^2 are nilpotent of class 2, we immediately deduce the following corollary.

Corollary 10.2. *Let G be any powerful p-group of exponent p^2. Then there exists a powerfully nilpotent group H of exponent p^2 and powerful class 2 such that G is powerfully embedded in H.*

Remark 10.3. (i) There exist powerful p-groups of exponent p^2 that are not powerfully solvable (see Section 10.2), and thus a powerfully embedded subgroup of a powerfully nilpotent group of powerful class 2 does not even need to be powerfully solvable.

(ii) There exist powerfully nilpotent groups of exponent p^2 that are of arbitrary large powerful class, and so, the proposition above shows that a powerfully nilpotent group of powerful class 2 could have a powerfully embedded powerfully nilpotent subgroup of arbitrary large powerful class.

Thus powerful nilpotence and powerful solvability are in general not as satisfactory as notions for powerful groups as nilpotence and solvability for the class of all groups. For a rich subclass of powerful groups things, however, turn out much better. This is the class $\mathcal{P}$ of all powerful groups of type $(2,\dots,2)$ that we considered in Section 9.4. The good behaviour or the groups in $\mathcal{P}$ relies essentially on the following lemma.

Lemma 10.4. *Let $G \in \mathcal{P}$ and $H, K \leqslant G$ where $G^p \leqslant K$. Then $H^p \cap K^p = (H \cap K)^p$. In particular, $H \cap G^p = H^p$.*

Proof. Since G is powerful of exponent p^2, we have $G^p \leqslant Z(G)$, so it follows that the map

$$\begin{aligned} f : G/G^p &\to G^p \\ aG^p &\mapsto a^p \end{aligned}$$

is a bijection. Therefore,

$$\begin{aligned} H^p \cap K^p &= f(HG^p/G^p) \cap f(K/G^p) \\ &= f(HG^p \cap K/G^p) = f((H \cap K)G^p/G^p) \\ &= (H \cap K)^p \end{aligned}$$

where the equality in the second line follows since $K \geqslant G^p$. As $(H \cap K)^p \leqslant H^p \cap K^p$ we conclude that $H^p \cap K^p = (H \cap K)^p$. □

Theorem 10.5. *Let G be a powerfully nilpotent group in $\mathcal{P}$ and let H be a powerful subgroup of G. Then H is powerfully nilpotent of powerful class less than or equal to the powerful class of G.*

Proof. Suppose G has powerful nilpotency class c and that we have a powerfully central chain $G = G_0 > G_1 > \cdots > G_c = 1$. As $G^p \leqslant Z(G)$ and $(G^p)^p = 1$, multiplying a term by G^p makes no difference. Also as the powerful class is c we get a strictly decreasing powerfully central chain $G = G_0 > G_1G^p > \cdots > G_{c-1}G^p > 1$. Without loss of generality we can thus assume that $G_1, \dots, G_{c-1}$ contain G^p as a subgroup. We claim that

$$H = H \cap G_0 \geqslant H \cap G_1 \geqslant \cdots \geqslant H \cap G_{c-1} \geqslant 1$$

is powerfully central. Using Lemma 10.4 we have

$$[H \cap G_i, H] \leqslant [H, H] \cap [G_i, G] \leqslant H^p \cap G_{i+1}^p = (H \cap G_{i+1})^p,$$

for $0 \leqslant i \leqslant c-1$. Hence H is powerfully nilpotent of powerful class at most c. □

Theorem 10.6. *Let G be a powerfully solvable group in $\mathcal{P}$ and let H be a powerful subgroup of G. Then H is powerfully solvable of powerful derived length less than or equal to the powerful derived length of G.*

Proof. Suppose the powerful derived length of G is d and that we have a powerfully abelian chain $G = G_0 > G_1 > \cdots > G_d = 1$. Arguing like in the proof of the previous theorem, we can assume that G_{d-1} contains G^p. We show that

$$H = H \cap G_0 \geqslant H \cap G_1 \geqslant \cdots \geqslant H \cap G_{c-1} \geqslant H \cap G_c = 1$$

is a powerfully abelian chain. Using Lemma 10.4, we have

$$[H \cap G_i, H \cap G_i] \leqslant [H, H] \cap [G_i, G_i] \leqslant H^p \cap G_{i+1}^p = (H \cap G_{i+1})^p.$$

This shows that H is powerfully solvable of powerful derived length at most d. □

In view of Theorems 10.5 and 10.6, we introduce some useful notation. Let $G \in \mathcal{P}$. We say that H is a $\mathcal{P}$-subgroup of G and we write $H \leqslant_{\mathcal{P}} G$, if H is a subgroup of G such that $H \in \mathcal{P}$. We use $H \trianglelefteqslant_{\mathcal{P}} G$ for $H \in \mathcal{P}$ and H powerfully embedded in G. The notations $H <_{\mathcal{P}} G$ and $H \triangleleft_{\mathcal{P}} G$ are defined naturally in a similar way.

In this way we can work in the well-behaved category of powerful groups of type $(2,\dots,2)$, where the notions of nilpotence and solvability behave particularly well. In this setting, is then natural to consider the notion of *powerfully simple group*, which we define next.

Definition 10.7. We say that a group $G \in \mathcal{P}$ is *powerfully simple* if $G \neq 1$ and if $H \triangleleft_{\mathcal{P}} G$ implies that $H = 1$.

The notion of powerfully simple is thus the "powerful version" of finite simple groups, and in the same way as finite simple groups, maximality of normal subgroups can be characterised in terms of simplicity, as shown in Lemma 10.9 below.

Definition 10.8. Let $H, G \in \mathcal{P}$ with $H \triangleleft_{\mathcal{P}} G$. We say that H is a maximal powerfully embedded $\mathcal{P}$-subgroup of G if there is no $H < K < G$ such that $K \trianglelefteqslant_{\mathcal{P}} G$.

Observe that if $G \in \mathcal{P}$ and $H \trianglelefteq_{\mathcal{P}} G$, then the quotient G/H has naturally the structure of powerful group of type $(2,\dots,2)$. Otherwise, there exists an element $g \notin H$ such that $gH \in \Omega_1(G/H)$ but $gH \notin (G/H)^p$. Therefore, since $G^p = \Omega_1(G)$, we have $g^p \neq 1$ but $g^p \in H$. This is a contradiction since $g \notin H$.

Lemma 10.9. *Let $G \in \mathcal{P}$. Then H is a maximal powerfully embedded $\mathcal{P}$-subgroup of G if and only if G/H is powerfully simple.*

Proof. Let $H < K < G$. Now as H is powerful of type $(2,\dots,2)$ we have $H \cap G^p = H^p$. Therefore $[K,G] \leqslant K^pH$ if and only if

$$[K,G] \leqslant (K^pH) \cap G^p = K^p(H \cap G^p) = K^pH^p = K^p.$$

The result follows from this. □

Our next aim is proving a Jordan-Hölder type theorem for the category of groups of $\mathcal{P}$. For this purpose, we will show that this category is isomorphic to the category of alternating algebras over $\mathbb{F}_p$.

Definition 10.10. An *alternating algebra* V over $\mathbb{F}_p$ is an $\mathbb{F}_p$-vector space equipped with an alternating bilinear form, i.e., a map $(\,,\,) : V \times V \to V$ satisfying the following conditions:

(i) It is linear in each argument separately.

(ii) $(v,v) = 0$ for all $v \in V$.

A subset $U \subseteq V$ is an alternating subalgebra of V and we write $U \leqslant V$ if U is a subspace of V such that $(U,U) \leqslant U$. Similarly, U is an ideal of V and we write $U \trianglelefteq V$ if U is a subspace of V such that $(U,V) \leqslant U$.

Remark 10.11. Since we are only considering odd primes, property (ii) is equivalent to skew-symmetry, that is, $(v,w) = -(w,v)$ for all $v,w \in V$.

The notions of alternating algebra homomorphism, nilpotent alternating algebra, solvable alternating algebra and simple alternating algebra can be deduced naturally.

Now, let G be a powerful p-group of rank r in $\mathcal{P}$ and let $V = G/G^p$ be the associated vector space of dimension r over $\mathbb{F}_p$. The structure of G is determined by the commutator relations

$$[a,b] = c^p, \tag{10.1}$$

where there exists such $c \in G$ for each pair a,b in G. Notice that $[a,b]$ and c^p only depend on the cosets aG^p, bG^p and cG^p. Identifying the two vector spaces G/G^p and G^p under the map $xG^p \mapsto x^p$, we get a natural alternating product on V with the relations (10.1) translating to

$$(aG^p, bG^p) = cG^p.$$

Conversely, let V be an alternating algebra of dimension r over $\mathbb{F}_p$. Let $\{v_1,\dots,v_r\}$ be a basis of V and for every $1 \leqslant i < j \leqslant r$ write

$$(v_i,v_j) = \alpha_1(i,j)v_1 + \cdots + \alpha_r(i,j)v_r,$$

where $\alpha_1(i,j),\dots,\alpha_r(i,j) \in \mathbb{F}_p$. Then the group

$$G = \langle g_1,\dots,g_r \mid g_k^{p^2} = 1, [g_i,g_j] = g_1^{\alpha_1(i,j)p}\cdots g_r^{\alpha_r(i,j)p},\ k = 1,\dots,r,\ 1 \leqslant i < j \leqslant r\rangle$$

is a powerful group of type $(2,\overset{r}{\dots},2)$.

Moreover, it is easy to see that a homomorphism $\phi : G \to H$, where $G, H \in \mathcal{P}$, corresponds naturally to an alternating algebra homomorphism from the alternating algebra associated to G to the alternating algebra associated to H. The converse of this is also easy to prove.

We have shown the following.

Theorem 10.12. *The category of powerful groups of type* $(2,\dots,2)$ *and the category of alternating algebras are isomorphic.*

Moreover, if V is the alternating algebra corresponding to a group $G \in \mathcal{P}$, then its subalgebra structure is essentially the same as the subgroup structure of G.

Theorem 10.13. *Let* $G \in \mathcal{P}$ *and let* V *be its associated alternating algebra defined above. Let* $\mathcal{G}$ *be the collection of all* $\mathcal{P}$*-subgroups of* G *and let* $\mathcal{V}$ *be the collection of all the alternating subalgebras of* V*. Then there is an inclusion preserving one-to-one correspondence between* $\mathcal{G}$ *and* $\mathcal{V}$*, where powerfully embedded subgroups of* $\mathcal{G}$ *correspond to ideals in* $\mathcal{V}$*.*

Proof. Let $U \in \mathcal{V}$. Then there exist $u_1,\dots,u_t \in G$ such that $U = \langle u_1,\dots,u_t\rangle G^p/G^p$. Define $H = \langle u_1,\dots,u_t\rangle$ so that $U = HG^p/G^p$. For U to be in $\mathcal{V}$ it needs to be a subspace of V where $(U,U) \leqslant U$, which, by the definition of the alternating product, translates to $[HG^p, HG^p] = [H,H] \leqslant H^p$. Hence H is powerful of type $(2,\dots,2)$, so $H \in \mathcal{G}$. Moreover, if $U \trianglelefteqslant_{\mathcal{P}} V$, then this translates to $[H,G] \leqslant H^p$, so that $H \trianglelefteqslant_{\mathcal{P}} G$.

Conversely, for a subgroup H in $\mathcal{G}$, we have $[HG^p, HG^p] = [H,H] \leqslant H^p$, which, if $U = HG^p/G^p$, translates to $(U,U) \leqslant U$. In addition, if $H \trianglelefteqslant_{\mathcal{P}} G$, then we have $(U,G) \leqslant U$, so that $U \trianglelefteqslant V$. □

Remark 10.14. The same argument of the proof of the previous theorem also shows that G is powerfully nilpotent, resp. powerfully solvable, if and only if V is nilpotent, resp. solvable. Moreover, let $H, K \in \mathcal{G}$ and let U and W be the associated alternating algebras in $\mathcal{V}$. Suppose that H is powerfully embedded in K. Then K/H is powerfully simple if and only if W/U is a simple alternating algebra, and the latter happens if and only if U is a maximal ideal of W.

With this correspondence, we can now prove a Jordan-Hölder type theorem. Suppose $A, B, a, b \in \mathcal{V}$ where $A \trianglelefteqslant B$ and $a \trianglelefteqslant b$. Let $\mathcal{I}_A^B = \{Z \mid A \leqslant Z \leqslant B\}$ and $\mathcal{I}_a^b = \{z \mid a \leqslant z \leqslant b\}$. We get natural projections $P : \mathcal{I}_a^b \to \mathcal{I}_A^B$ and $Q : \mathcal{I}_A^B \to \mathcal{I}_a^b$ given by

$$P(z) = A + B \cap z \quad \text{and} \quad Q(Z) = a + b \cap Z.$$

The following is a version of the Zassenhaus lemma for alternating algebras.

Lemma 10.15. *We have* $P(a) \trianglelefteqslant P(b)$ *and* $Q(A) \trianglelefteqslant Q(B)$*. Furthermore* $P(b)/P(a)$ *is isomorphic to* $Q(B)/Q(A)$*.*

Proof. Notice that $P(a) = A + B \cap a$, $P(b) = A + B \cap b$, $Q(A) = a + b \cap A$ and $Q(B) = a + b \cap B$. As $A \trianglelefteqslant B$, we have

$$(P(a), P(b)) = (A + B \cap a, A + B \cap b) \leqslant A + (B \cap a, B \cap b).$$

Now as B is a subalgebra and $a \trianglelefteqslant b$ we have that this is contained in $P(a) = A + B \cap a$, so that $P(a) \trianglelefteqslant P(b)$. The second claim follows from this by symmetry.

Now for $P(b)/P(a)$, notice first that we have

$$B \cap b \cap P(a) = B \cap b \cap (A + B \cap a) = B \cap b \cap A + B \cap a = A \cap b + B \cap a,$$

and consequently

$$\begin{aligned} P(b)/P(a) &= (B \cap b + P(a))/P(a) \\ &\cong (B \cap b)/(B \cap b \cap P(a)) = (B \cap b)/(A \cap b + B \cap a), \end{aligned}$$

where the isomorphism is a vector space isomorphism. By symmetry, it follows that $P(b)/P(a) \cong Q(B)/Q(A)$ as vector spaces.

Now, for $u, v, w \in B \cap b$ it follows that

$$(u,v) + P(a) = w + P(a) \Leftrightarrow (u,v) + A \cap b + B \cap a = w + A \cap b + B \cap a,$$

and by symmetry

$$(u,v) + Q(A) = w + Q(A) \Leftrightarrow (u,v) + a \cap B + b \cap A = w + A \cap b + B \cap a.$$

The algebra isomorphism of $P(b)/P(a)$ and $P(B)/B(A)$ follows from this. □

The Jordan-Hölder theorem for alternating algebras is proved from this in the standard way.

Definition 10.16. Let V be an alternating algebra. A chain $0 = U_0 \lhd U_1 \lhd \cdots \lhd U_n = V$ is a *composition series* for V if all the factors $U_1/U_0, \dots, U_n/U_{n-1}$ are simple alternating algebras.

Theorem 10.17. *Let V be an alternating algebra. Then all composition series have the same length and same simple factors up to order.*

With this and the correspondence in Theorem 10.13, the Jordan-Hölder theorem for powerful groups of type $(2,\dots,2)$ follows easily.

Definition 10.18. Let $G \in \mathcal{P}$. A chain $1 = H_0 \lhd_{\mathcal{P}} H_1 \lhd_{\mathcal{P}} \cdots \lhd_{\mathcal{P}} H_n = G$ is a *powerful composition series* for G if all the factors $H_1/H_0, \dots, H_n/H_{n-1}$ are powerfully simple.

Theorem 10.19. *Let G be a group in $\mathcal{P}$ with two powerful composition series, say*

$$1 = H_0 \lhd_{\mathcal{P}} H_1 \lhd_{\mathcal{P}} \cdots \lhd_{\mathcal{P}} H_n = G$$

and

$$1 = K_0 \lhd_{\mathcal{P}} K_1 \lhd_{\mathcal{P}} \cdots \lhd_{\mathcal{P}} K_m = G.$$

Then $m = n$ and the powerfully simple factors $H_1/H_0, H_2/H_1, \dots, H_n/H_{n-1}$ are isomorphic to K_1/K_0, K_2/K_1, $\dots$, K_n/K_{n-1} (in some order).

Proof. Replace the terms H_i, K_j by their associated alternating algebras U_i, V_j. The result now follows from the Jordan-Hölder theorem for alternating algebras. □

Definition 10.20. We refer to the unique factors of a powerful composition series of a group $G \in \mathcal{P}$ as the *powerful composition factors* of G.

Finally, we see that as for finite groups, powerful solvability and powerful simplicity are somehow opposite concepts.

Corollary 10.21. *A group $G \in \mathcal{P}$ is powerfully solvable if and only if the powerful composition factors are cyclic of order p^2.*

Proof. Any powerful abelian chain of G consisting of subgroups in $\mathcal{P}$ can be refined to a chain with factors that are cyclic of order p^2. □

10.2 The classification of powerful groups of type $(2,2,2)$

We devote this last section to the classification of all powerful groups of type $(2,2,2)$. From Theorem 10.13 we know that this task is equivalent to classifying all simple alternating algebras of dimension 3.

Following [74], any given alternating algebra of dimension 3 over $\mathbb{F}_p$ can be represented by a 3×3 matrix over $\mathbb{F}_p$. This is done by identifying the matrix

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix}$$

with the 3-dimensional alternating algebra $V = \mathbb{F}_p x_1 + \mathbb{F}_p x_2 + \mathbb{F}_p x_3$ with relations

$$\begin{aligned} (x_2, x_3) &= \alpha_{11}x_1 + \alpha_{21}x_2 + \alpha_{31}x_3, \\ (x_3, x_1) &= \alpha_{12}x_1 + \alpha_{22}x_2 + \alpha_{32}x_3, \\ (x_1, x_2) &= \alpha_{13}x_1 + \alpha_{23}x_2 + \alpha_{33}x_3. \end{aligned}$$

This algebra would correspond to a powerful p-group of order p^6 with generators a_1, a_2, a_3 of order p^2 satisfying the relations

$$\begin{aligned} [a_2, a_3] &= a_1^{p\alpha_{11}} a_2^{p\alpha_{21}} a_3^{p\alpha_{31}} \\ [a_3, a_1] &= a_1^{p\alpha_{12}} a_2^{p\alpha_{22}} a_3^{p\alpha_{32}} \\ [a_1, a_2] &= a_1^{p\alpha_{13}} a_2^{p\alpha_{23}} a_3^{p\alpha_{33}}. \end{aligned}$$

Note that different choices of the basis of V give rise to different matrices that represent it. Indeed, if we choose another basis for V, say

$$\begin{aligned} y_1 &= g_{11}x_1 + g_{21}x_2 + g_{31}x_3, \\ y_2 &= g_{12}x_1 + g_{22}x_2 + g_{32}x_3, \\ y_3 &= g_{13}x_1 + g_{23}x_2 + g_{33}x_3, \end{aligned}$$

then we get

$$\begin{aligned} (y_2, y_3) &= \begin{bmatrix} g_{22} & g_{23} \\ g_{32} & g_{33} \end{bmatrix} (x_2, x_3) - \begin{bmatrix} g_{12} & g_{13} \\ g_{32} & g_{33} \end{bmatrix} (x_3, x_1) + \begin{bmatrix} g_{12} & g_{13} \\ g_{22} & g_{23} \end{bmatrix} (x_1, x_2), \\ (y_3, y_1) &= -\begin{bmatrix} g_{21} & g_{23} \\ g_{31} & g_{33} \end{bmatrix} (x_2, x_3) + \begin{bmatrix} g_{11} & g_{13} \\ g_{31} & g_{33} \end{bmatrix} (x_3, x_1) - \begin{bmatrix} g_{11} & g_{13} \\ g_{21} & g_{23} \end{bmatrix} (x_1, x_2), \\ (y_1, y_2) &= \begin{bmatrix} g_{21} & g_{22} \\ g_{31} & g_{32} \end{bmatrix} (x_2, x_3) - \begin{bmatrix} g_{11} & g_{12} \\ g_{31} & g_{32} \end{bmatrix} (x_3, x_1) + \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix} (x_1, x_2). \end{aligned}$$

Therefore, if

$$P = \begin{bmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{bmatrix},$$

then the matrix B representing V with respect to the basis $\{y_1, y_2, y_2\}$ is

$$P^{-1} \cdot A \cdot \mathrm{adj}(P)^t = \det(P) P^{-1} \cdot A \cdot (P^{-1})^t.$$

Thus, we define the action of the general linear group of degree 3 over $\mathbb{F}_p$, namely $\mathrm{GL}(3,\mathbb{F}_p)$, on the set of 3×3 matrices $M_3(\mathbb{F}_p)$ by

$$A^P = \det(P)^{-1}P^t\cdot A\cdot P.$$

In this way, two matrices A and B represent the same alternating algebra if and only if they lie in the same orbit with respect to this action, that is, if there exists $P\in \mathrm{GL}(3,\mathbb{F}_p)$ such that $A^P=B$. In this case, we write $A\simeq B$. Our goal will be finding a representative for each of these orbits.

This equivalence turns out to be slightly more general than being congruent (that is $B=P^tAP$).

Lemma 10.22. *Let $\lambda\in\mathbb{F}_p^*$. Then $\lambda A\simeq A$.*

Proof. Let $P=\frac{1}{\lambda}I$. Then $\det(P)^{-1}P^tAP=\lambda^3\cdot\frac{1}{\lambda^2}A=\lambda A$. □

From this we easily get the following corollary.

Proposition 10.23. *We have $A\simeq B$ if and only if there exists $\lambda\in\mathbb{F}_p$ such that A is congruent to λB.*

In particular two matrices that are congruent are equivalent in the sense above.

Now, each matrix A in $M_3(\mathbb{F}_p)$ can be written in a unique way as a sum of a symmetric and an anti-symmetric matrix, namely $A=A_s+A_a$ where

$$A_s=\frac{A+A^t}{2}\quad\text{and}\quad A_a=\frac{A-A^t}{2}.$$

We will consider all the possible combinations of the bilinear forms induced by the matrices A_s and A_a and with that we will be able to determine all the equivalence classes of $M_3(\mathbb{F}_p)$ and therefore all powerful p-groups of type $(2,2,2)$. We will start with the easiest cases when $A=A_s$ and $A=A_a$.

10.2.1 The orbits of the symmetric and anti-symmetric matrices

Note that

$$(A^t)^P=\det(P)^{-1}P^t\cdot A^t\cdot P=(\det(P)^{-1}P^t\cdot A\cdot P)^t=(A^P)^t,$$

so if A is symmetric, resp. anti-symmetric, then A^P is also symmetric, resp. anti-symmetric. In this section we determine the orbits of the symmetric and the anti-symmetric matrices.

Let us start with the symmetric matrices. Denote by $D(\alpha,\beta,\gamma)$ the 3×3 matrix with $\alpha,\beta,\gamma\in\mathbb{F}_p$ on the diagonal entries.

Theorem 10.24 ([11, Chapter 6, Theorem 2.7])**.** *Two non-singular $n\times n$ symmetric matrices are congruent if and only if they have the same determinant modulo $(\mathbb{F}_p^*)^2$.*

This implies that every symmetric matrix is congruent to a diagonal matrix of the following form: $D(1,1,1)$, $D(\tau,1,1)$, $D(1,1,0)$, $D(\tau,1,0)$, $D(1,0,0)$, $D(\tau,0,0)$ and $D(0,0,0)$, where τ is a fixed non-square in $\mathbb{F}_p^*$.

Now, by Proposition 10.23, $D(1,1,1)$ is equivalent to $\tau D(1,1,1)$ where the latter has determinant τ modulo $(\mathbb{F}_p^*)^2$. Hence $D(1,1,1)$ and $D(\tau,1,1)$ are equivalent. Also

$D(\tau,0,0) = \tau D(1,0,0)$ is equivalent to $D(1,0,0)$. When the rank is 2 then multiplying the matrix by a constant $\lambda \in \mathbb{F}_p^*$ doesn't change the value of the determinant modulo $(\mathbb{F}_p^*)^2$. Hence $D(1,1,0)$ and $D(\tau,1,0)$ are not equivalent. Up to equivalence we thus get only 5 matrices:

$$D(1,1,1),\ D(1,1,0),\ D(\tau,1,0),\ D(1,0,0) \text{ and } D(0,0,0).$$

The situation regarding the anti-symmetric matrices is simpler as there is only one non-trivial equivalence class. To see this, note that the rank of a 3×3 non trivial anti-symmetric matrix must be 0 or 2 (see [40, Proposition 1]). If V is a 3 dimensional vector space equipped with the alternating bilinear form $\langle\ ,\ \rangle_a$ induced from an anti-symmetric matrix of rank 2, then $\dim(V^{\perp_a}) = 1$, and so there exists a basis $\{v_1, v_2, v_3\}$ such that $v_3 \in V^{\perp_a}$. Hence we can assume that the anti-symmetric matrix is of the form

$$\begin{bmatrix} 0 & a & 0 \\ -a & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

with $a \in \mathbb{F}_p^*$, and according to Lemma 10.22, there is only one such matrix up to equivalence (in fact, it is easy to see that this matrix is also unique up to congruence).

10.2.2 Classification of the alternating algebras

Let now A be a general 3×3 matrix over $\mathbb{F}_p$ and let V be a 3 dimensional vector space. The symmetric part of A equips V with a corresponding symmetric bilinear form $\langle\ ,\ \rangle_s$ and the anti-symmetric part of A equips V with a corresponding alternating form $\langle\ ,\ \rangle_a$. Now there are two possibilities for $\langle\ ,\ \rangle_a$. If it is zero then A is symmetric and we get 5 alternating algebras corresponding to the 5 diagonal matrices listed above. Hence we assume from now on that $\langle\ ,\ \rangle_a$ is non-zero. Thus $V^{\perp_a}$ is of dimension 1, say

$$V^{\perp_a} = \mathbb{F}_p v_3,$$

so that

$$V = (\mathbb{F}_p v_1 + \mathbb{F}_p v_2) \oplus\!\!\!\!\!\!\perp_a \mathbb{F}_p v_3$$

for some $v_1, v_2 \in V$. For our classification we will divide first into 3 cases. For Case 1, we have $\langle v_3, v_3\rangle_s \neq 0$. For Case 2, we have $\langle v_3, v_3\rangle_s = 0$ and $(V^{\perp_a})^{\perp_s} = (\mathbb{F}_p v_3)^{\perp_s} = V$. Finally for Case 3, we have $\langle v_3, v_3\rangle_s = 0$ and $(V^{\perp_a})^{\perp_s} = (\mathbb{F}_p v_3)^{\perp_s} < V$.

Case 1: $\langle v_3, v_3\rangle_s \neq 0$.

By [11, Theorem 2.2], we can here find a basis v_1, v_2, v_3 for V where

$$V = \mathbb{F}_p v_1 \oplus\!\!\!\!\!\!\perp_s \mathbb{F}_p v_2 \oplus\!\!\!\!\!\!\perp_s \mathbb{F}_p v_3.$$

Case 1.1. Suppose first that the rank of $\langle\ ,\ \rangle_s$ is 1. In this case it is easy to see that we can pick our basis further so that

$$\begin{array}{lll} \langle v_1, v_2\rangle_a = 1, & \langle v_1, v_3\rangle_a = 0, & \langle v_2, v_3\rangle_a = 0, \\ \langle v_1, v_1\rangle_s = 0, & \langle v_2, v_2\rangle_s = 0, & \langle v_3, v_3\rangle_s = 1. \end{array}$$

Indeed, notice that by Lemma 10.22 we can always multiply the relevant matrix A by a constant to get $\langle v_3, v_3\rangle_s = 1$. Then, by [11, Lemma 2.1] we can pick v_1 and v_2 in $(\mathbb{F}_p v_3)^{\perp_s}$, and since the rank of A_s is 1 we must have $\langle v_1, v_1\rangle_s = 0$ and $\langle v_2, v_2\rangle_s = 0$. Finally, we can replace, if necessary v_i by a multiple of v_i so that $\langle v_1, v_2\rangle_a = 1$. In this case we thus have only 1 algebra.

Case 1.2. Suppose next that the rank of $\langle\ ,\ \rangle_s$ is 2. Here again by multiplying by a constant we can assume that $\langle v_3, v_3\rangle_s = 1$, and also that $v_1, v_2 \in (\mathbb{F}_p v_3)^{\perp_s}$. Moreover, by Theorem 10.24, and since the rank of $\langle\ ,\rangle_s$ is 2, we can further assume that $\langle v_2, v_2\rangle_s = 0$. Now $\langle v_1, v_1\rangle_s = \lambda^2$ or $\langle v_1, v_1\rangle_s = \tau\lambda^2$ for some $\lambda \in \mathbb{F}_p^*$. By replacing v_1 by $\frac{1}{\lambda}v_1$ we have that $\langle v_1, v_1\rangle_s$ is either 1 or τ. Notice that we have also seen above that these cases are genuinely distinct. Now that v_1 has been chosen we can replace v_2 by a suitable multiple to ensure that $\langle v_1, v_2\rangle_a = 1$. We thus get 2 algebras

$$\begin{array}{lll} \langle v_1, v_2\rangle_a = 1, & \langle v_1, v_3\rangle_a = 0, & \langle v_2, v_3\rangle_a = 0, \\ \langle v_1, v_1\rangle_s = 1, & \langle v_2, v_2\rangle_s = 0, & \langle v_3, v_3\rangle_s = 1. \end{array}$$

and

$$\begin{array}{lll} \langle v_1, v_2\rangle_a = 1, & \langle v_1, v_3\rangle_a = 0, & \langle v_2, v_3\rangle_a = 0, \\ \langle v_1, v_1\rangle_s = \tau, & \langle v_2, v_2\rangle_s = 0, & \langle v_3, v_3\rangle_s = 1. \end{array}$$

Case 1.3. We are only left with the case where the rank of $\langle\ ,\ \rangle_s$ is 3. By Theorem 10.24 and by taking a suitable multiple of v_1 to ensure that $\langle v_1, v_2\rangle_a = 1$, we can assume that

$$\begin{array}{lll} \langle v_1, v_2\rangle_a = 1, & \langle v_1, v_3\rangle_a = 0, & \langle v_2, v_3\rangle_a = 0, \\ \langle v_1, v_1\rangle_s = \alpha, & \langle v_2, v_2\rangle_s = 1, & \langle v_3, v_3\rangle_s = 1, \end{array}$$

where $\alpha \in \mathbb{F}_p^*$. We want to see when we get an equivalent algebra by changing α to β. If we multiply the presentation by a constant it must be by a square if we still want $\langle v_3, v_3\rangle_s = 1$. Say we multiply by λ^2 and then replace v_3 by $\frac{1}{\lambda}v_3$. Notice that we now have

$$\langle v_1, v_2\rangle_a = \lambda^2,\ \langle v_1, v_1\rangle_s = \alpha\lambda^2,\ \langle v_2, v_2\rangle_s = \lambda^2.$$

We are now looking for all possible $\bar{v}_1 = av_1 + bv_2$ and $\bar{v}_2 = cv_1 + dv_2$ where $\langle \bar{v}_1, \bar{v}_2\rangle_a = 1$, $\langle \bar{v}_1, \bar{v}_2\rangle_s = 0$ and $\langle \bar{v}_2, \bar{v}_2\rangle_s = 1$. This gives us the following system of equations:

$$\begin{aligned} \lambda^2(ad - bc) &= 1 \\ \lambda^2(\alpha ac + bd) &= 0 \\ \lambda^2(\alpha c^2 + d^2) &= 1. \end{aligned}$$

We look first for all the solutions where $c = 0$. Notice that in this case we must have $\lambda^2 ad = 1$, $\lambda^2 d^2 = 1$ and $b = 0$. Thus $\langle \bar{v}_1, \bar{v}_1\rangle_s = \lambda^2(\alpha a^2 + b^2) = \lambda^2 \frac{\alpha}{d^2\lambda^4} = \frac{\alpha}{\lambda^2 d^2} = \alpha$.

Next we look for solutions where $c \neq 0$ but $d = 0$. Then we must have $\lambda^2 bc = -1$, $\lambda^2 \alpha c^2 = 1$ and $a = 0$. Here $\langle \bar{v}_1, \bar{v}_1\rangle_s = \lambda^2(\alpha a^2 + b^2) = \frac{\lambda^2}{c^2\lambda^4} = \frac{\alpha}{\alpha c^2 \lambda^2} = \alpha$.

Finally we are left with finding all solutions where $cd \neq 0$. Then $a = -\frac{bd}{\alpha c}$, and the first equation above gives us

$$1 = -\lambda^2\left(\frac{bd^2}{\alpha c} + bc\right) = -\frac{b}{\alpha c}\cdot\lambda^2(d^2 + \alpha c^2) = -\frac{b}{\alpha c}.$$

Thus $b = -\alpha c$ and $a = -\frac{bd}{\alpha c} = d$. Therefore

$$\begin{aligned}\langle \bar{v}_1, \bar{v}_1 \rangle &= \lambda^2(\alpha a^2 + b^2) \\ &= \lambda^2(\alpha d^2 + \alpha^2 c^2) \\ &= \alpha\lambda^2(\alpha c^2 + d^2) \\ &= \alpha.\end{aligned}$$

We have thus seen that the value of α doesn't change and we have $p-1$ different algebras here.

Case 2: $\langle v_3, v_3 \rangle_s = 0$ *and* $(V^{\perp_a})^{\perp_s} = (\mathbb{F}_p v_3)^{\perp_s} = V$.

Again we consider several subcases.

Case 2.1. Suppose that the rank of $\langle\ ,\ \rangle_s$ is zero. Then, as seen before, we have only 1 algebra.

$$\begin{array}{llll}\langle v_1, v_2 \rangle_a = 1, & \langle v_1, v_3 \rangle_a = 0, & \langle v_2, v_3 \rangle_a = 0, \\ \langle v_1, v_1 \rangle_s = 0, & \langle v_2, v_2 \rangle_s = 0, & \langle v_3, v_3 \rangle_s = 0.\end{array}$$

Case 2.2. Suppose next that the rank of $\langle\ ,\ \rangle_s$ is 1. By multiplying by a suitable constant we can assume that $\langle v_1, v_1 \rangle_s = 1$ and $\langle v_2, v_2 \rangle_s = 0$. Finally replacing v_2 by an appropriate multiple we can also assume that $\langle v_1, v_2 \rangle_a = 1$. We thus also get here only 1 algebra

$$\begin{array}{llll}\langle v_1, v_2 \rangle_a = 1, & \langle v_1, v_3 \rangle_a = 0, & \langle v_2, v_3 \rangle_a = 0, \\ \langle v_1, v_1 \rangle_s = 1, & \langle v_2, v_2 \rangle_s = 0, & \langle v_3, v_3 \rangle_s = 0.\end{array}$$

Case 2.3. Finally we are left with the case when the rank of $\langle\ ,\ \rangle_s$ is 2. Here, as done in Case 1.3, it is easy to see that we can pick our basis further so that

$$\begin{array}{llll}\langle v_1, v_2 \rangle_a = 1, & \langle v_1, v_3 \rangle_a = 0, & \langle v_2, v_3 \rangle_a = 0, \\ \langle v_1, v_1 \rangle_s = \alpha, & \langle v_2, v_2 \rangle_s = 1, & \langle v_3, v_3 \rangle_s = 0.\end{array}$$

Similar calculations as for Case 1.3 show that we get distinct algebras for different values of α. Thus here we have $p-1$ algebras.

Case 3: $\langle v_3, v_3 \rangle_s = 0$ *and* $(V^{\perp_a})^{\perp_s} = (\mathbb{F}_p v_3)^{\perp_s} < V$.

Since v_3 is not orthogonal to everything in V with respect to $\langle\ ,\ \rangle_s$, it follows that $(\mathbb{F}_p v_3)^{\perp_s}$ has dimension 2. Suppose

$$(\mathbb{F}_p v_3)^{\perp_s} = \mathbb{F}_p v_2 + \mathbb{F}_p v_3$$

and take $v_1 \in V \backslash (\mathbb{F}_p v_3)^{\perp_s}$ so that $\langle v_1, v_3 \rangle_s \neq 0$. Replacing if necessary v_1 by $\alpha v_1 + \beta v_3$ with $0 < \alpha, \beta \leqslant p-1$, we can assume $\langle v_1, v_1 \rangle_s = 0$. Similarly, taking if necessary a linear combination of v_2 and v_3 instead of v_2 we have $\langle v_1, v_2 \rangle_s = 0$. Hence we can pick our basis such that

$$\begin{array}{llll}\langle v_1, v_2 \rangle_a = 1, & \langle v_1, v_3 \rangle_a = 0, & \langle v_2, v_3 \rangle_a = 0, & \\ \langle v_1, v_1 \rangle_s = 0, & \langle v_1, v_2 \rangle_s = 0, & \langle v_1, v_3 \rangle_s = 1, & \langle v_2, v_3 \rangle_s = 0.\end{array}$$

Now there are two subcases.

Case 3.1. If the rank of $\langle\ ,\ \rangle_s$ is 2 then we must have $\langle v_2, v_2\rangle_s = 0$ and this gives us 1 algebra.

Case 3.2. If the rank of $\langle\ ,\ \rangle_s$ is 3 then $\langle v_2, v_2\rangle_s \neq 0$ and after multiplying by a suitable constant we can assume that this value is 1 (and then afterwards adjust things so that the other assumptions hold again). Thus we get again 1 algebra.

We have thus determined all the 3×3 presentation matrices up to equivalence, and adding up we got in total $12 + 2(p-1)$ such matrices. As we described at the beginning of the section this gives us a classification of all the alternating algebras of dimension 3 over $\mathbb{F}_p$ that in turn gives us a classification of all the powerful p-groups of type $(2,2,2)$.

Before listing these we state and prove a proposition that shows how we can see which of these are powerfully simple.

Proposition 10.25. *An alternating algebra V over $\mathbb{F}_p$ of dimension 3 is simple if and only if $V \cdot V = V$.*

Proof. This condition is clearly necessary as $V \cdot V$ is an ideal of V. To see that it is sufficient, suppose $V \cdot V = V$ and let I be a proper ideal. We want to show that $I = 0$. We argue by contradiction and suppose I is an ideal of dimension either 1 or 2. If I is of dimension 2, then V/I is 1 dimensional and thus we get the contradiction that $V \cdot V \leqslant I < V$. Now suppose I is of dimension 1, say $V = I + \mathbb{F}_p v_1 + \mathbb{F}_p v_2$. Then $V \cdot V \leqslant I + \mathbb{F}_p v_1 v_2$. But the dimension of $I + \mathbb{F} v_1 v_2$ is at most 2 and we get the contradiction that $V \cdot V < V$. □

Then the following corollary follows immediately.

Corollary 10.26. *Let V be an alternating algebra and let A be an associated matrix of V. Then V is simple if and only if* $\det(A) \neq 1$.

This corollary tells us how we read from the presentation whether a given alternating algebra is simple and thus whether the corresponding powerful group is powerfully simple. Moreover, according to the following proposition, it turns out that all non-powerfully simple groups of type $(2,2,2)$ are powerfully solvable.

Proposition 10.27. *Let $G \in \mathcal{P}$ be of type $(2,2,2)$. If G is not powerfully simple, then it is powerfully solvable.*

Proof. Note that $G^p \cong C_p \times C_p \times C_p$, and if $G' = G^p$, then G is powerfully simple by Corollary 10.26. Hence $G' < G^p$. If G' is cyclic then we are done by Proposition 9.1, so suppose that $G' = \langle a^p, b^p\rangle \cong C_p \times C_p$ for some $a, b \in G$. Now by Theorem 9.2 we may assume that $[a,b] \in \langle a^p\rangle$, and it follows that

$$G > \langle a, b\rangle > \langle a\rangle > 1$$

is a powerfully abelian chain. □

The work above gives us the following list of powerful p-groups of type $(2,2,2)$. As the power relations for all of these are $a_1^{p^2} = a_2^{p^2} = a_3^{p^2} = 1$ we omit them below. Here τ is a fixed non-square in $\mathbb{F}_p$.

$A_1 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^p,\ [a_3, a_1] = a_2^p,\ [a_1, a_2] = a_3^p \rangle$;
$A_2 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_2^{-p},\ [a_3, a_1] = a_1^p,\ [a_1, a_2] = a_3^p \rangle$;
$A_3 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^p a_2^{-p},\ [a_3, a_1] = a_1^p,\ [a_1, a_2] = a_3^p \rangle$;
$A_4 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^{p\tau} a_2^{-p},\ [a_3, a_1] = a_1^p,\ [a_1, a_2] = a_3^p \rangle$;
$A_5 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_2^{-p} a_3^p,\ [a_3, a_1] = a_1^p a_2^p,\ [a_1, a_2] = a_1^p \rangle$;
$A_6(\alpha) = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^{p\alpha} a_2^{-p},\ [a_3, a_1] = a_1^p a_2^p,\ [a_1, a_2] = a_3^p \rangle,\ 1 \leqslant \alpha \leqslant p-2$;
$B_1 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^{-p} a_2^{-p},\ [a_3, a_1] = a_1^p a_2^p,\ [a_1, a_2] = a_3^p \rangle$;
$B_2 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^p,\ [a_3, a_1] = a_2^p,\ [a_1, a_2] = 1 \rangle$;
$B_3 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^{p\tau},\ [a_3, a_1] = a_2^p,\ [a_1, a_2] = 1 \rangle$;
$B_4 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_2^{-p},\ [a_3, a_1] = a_1^p,\ [a_1, a_2] = 1 \rangle$;
$B_5 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^p a_2^{-p},\ [a_3, a_1] = a_1^p,\ [a_1, a_2] = 1 \rangle$;
$B_6 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_2^{-p} a_3^p,\ [a_3, a_1] = a_1^p,\ [a_1, a_2] = a_1^p \rangle$
$B_7(\alpha) = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^{p\alpha} a_2^{-p},\ [a_3, a_1] = a_1^p a_2^p,\ [a_1, a_2] = 1 \rangle,\ 1 \leqslant \alpha \leqslant p-2$;
$C_1 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^{-p} a_2^{-p},\ [a_3, a_1] = a_1^p a_2^p,\ [a_1, a_2] = 1 \rangle$;
$C_2 = \langle a_1, a_2, a_3 \mid [a_2, a_3] = a_1^p,\ [a_3, a_1] = 1,\ [a_1, a_2] = 1 \rangle$;
$D = \langle a_1, a_2, a_3 \mid [a_2, a_3] = 1,\ [a_3, a_1] = 1,\ [a_1, a_2] = 1 \rangle$.

Of these $12 + 2(p-1)$ groups, the $A_1, \ldots A_5, A_6(\alpha)$ are the powerfully simple ones. There are $5 + (p-2)$ of these.

Bibliography

[1] J.L. Abercrombie, Subgroups and subrings of profinite rings, *Math. Proc. Cambr. Phil. Soc.* **116** (1994), 209–222.

[2] M. Abért and B. Virág, Dimension and randomness in groups acting on rooted trees, *J. Amer. Math. Soc.* **18** (2005), 157–192.

[3] C. Acciarri, P. Shumyatsky, On profinite groups in which commutators are covered by finitely many subgroups, *Math. Z.* **279** (2013), 239–248.

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

[5] Y. Barnea, B. Klopsch, Index-subgroups of the Nottingham group, *Adv. Math.* **180** (2003), 187–221.

[6] Y. Barnea and A. Shalev, Hausdorff dimension, pro-p groups, and Kac-Moody algebras, *Trans. Amer. Math. Soc.* **349** (1997), 5073–5091.

[7] Y. Barnea and M. Vannacci, On hereditarily just infinite profinite groups with complete Hausdorff dimension spectrum, *J. Algebra Appl.* **18** (2019), Article ID 1950216, 10 p.

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

[9] N. Blackburn, On prime-power groups in which the derived group has two generators, *Proc. Cambridge Philos. Soc.* **53** (1957), 19–27.

[10] N. Blackburn, On a special class of p-groups, *Acta Math., Volume 100*, **1-2** (1958), 45-92.

[11] P.M. Cohn, *Algebra*, Vol. 2, 2nd edition, University College London, 1989.

[12] R.S. Dark, M.L. Newell, On conditions for commutators to form a subgroup, *J. London Math. Soc. (2)* **17** (1978), 251–262.

[13] J.D. Dixon, M.P.F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, 2nd edition. Cambridge University Press, 1999.

[14] M. Ershov, New just-infinite pro-p groups of finite width and subgroups of the Nottingham group, *J. Algebra* **275** (2004), 419–449.

[15] M. Ershov, On the commensurator of the Nottingham group, *Trans. Am. Math. Soc.* **362** (2010), 6663–6678.

[16] K. Falconer, *Fractal Geometry: Mathematical Foundations and Applications.* John Wiley & Sons, 1990.

[17] G. Fernández-Alcober, Omega subgroups of powerful p-groups, *Isr. J. Math.* **162** (2007), 75–79.

[18] G. Fernández-Alcober, I. de las Heras, Commutators in finite p-groups with 2-generator derived subgroup, *Isr. J. Math.* **232** (2019), 109–124.

[19] G. Fernández-Alcober, M. Morigi, Outer commutator words are uniformly concise, *J. London Math. Soc.(2)* **82** (2010), 581–595.

[20] W.B. Fite, On metabelian groups, *Trans. Amer. Math. Soc.* **3** (1902), 331–353.

[21] F.G. Frobenius, Uber die Primfactoren der Gruppendeterminante, *Sitzungsberichte der Köniqlich Preußischen Akademie der Wissenschaften zu Berlin* (1896), 1343–1382.

[22] O. Garaialde Ocaña, A. Garrido, and B. Klopsch, Pro-p groups of positive rank gradient and Hausdorff dimension, to appear in *J. London Math. Soc.*, `doi:10.1112/jlms.12295`.

[23] J. González-Sánchez, A. Jaikin, On the structure of normal subgroups of potent p-groups, *J. Algebra*, **276** (2004), 193-209.

[24] R.M. Guralnick, Expressing group elements as commutators, *Rocky Mountain J. Math.*, **10(3)** (1980), 651-654.

[25] R.M. Guralnick, Commutators and commutator subgroups, *Advances in Math.*, **45** (1982), 319–330.

[26] R.M. Guralnick, Generation of the lower central series. *Glasgow Math. J.* **23** (1982), 15-20.

[27] R.M. Guralnick, Generation of the lower central series II. *Glasgow Math. J.* **25** (1984), 193-201.

[28] A. Haar, Der Massbegriff in der Theorie der kontinuierlichen Gruppen, *Ann. Math.* **34** (1933), 147–169.

[29] P. Hall, A contribution to the theory of groups of prime-power order, *P. Lond. Math. Soc.* **36** (1934), 29–95.

[30] P. Hall, The classification of prime power groups, *J. für die Reine und Angew. Math.* **182** (1940), 130–141.

[31] F. Hausdorff, Dimension und äußeres Maß, *Math. Ann.*, **79** (1919), 157–179.

[32] I. de las Heras, Commutators in finite p-groups with 3-generator derived subgroup, *J. Algebra* **546** (2020), 201–217.

[33] I. de las Heras, B. Klopsch, A pro-p group with full normal Hausdorff spectra, *Math. Nachr.*, to appear.

[34] I. de las Heras, G. Morigi, Lower central words in finite p-groups, *Publ. Mat*, to appear.

[35] I. de las Heras, A. Thillaisundaram, A pro-2 group with full normal Hausdorff spectra, in process.

[36] I. de las Heras, G. Traustason, Powerfully solvable and powerfully simple group, arXiv: 2006.12593.

[37] L. Héthelyi, L. Lévai, On elements of order p in powerful p-groups, *J. Algebra* **270** (2003), 1–6.

[38] C.R. Hobby, A characteristic subgroup of a p-group, *Pacific J. Math.* **10** (1960), 853–858.

[39] K. Honda, On commutators in finite groups, *Comment. Math. Univ. St. Paul*, **2** (1953), 9–12.

[40] H. Hofer, E. Zehnder, *Symplectic Invariants and Hamiltonian Dynamics*, Birkhäuser, 1994.

[41] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[42] N. Ito, A theorem on the alternating group $\mathfrak{A}_n$ ($n \geqslant 5$), *Math. Japonicae* **2** (1951), 59–60.

[43] A. Jaikin-Zapirain, On the verbal width of finitely generated pro-p groups, *Rev. Mat. Iberoam.* **24** (2008), 617–630.

[44] L. Kappe, Groups with a cyclic term in the lower central series, *Arch. Math.* **30** (1978), 561–569.

[45] L.-C. Kappe, R.F. Morse, On commutators in p-groups, *J. Group Theory* **8** (2005), 415–429.

[46] R. Kaushik, M.K. Yadav, Commutators and commutator subgroups of finite p-groups, *J. Algebra*, to appear.

[47] L.-C. Kappe, R.F. Morse, On commutators in groups, in *Groups St Andrews 2005, Volume 2*, 531–558, Cambridge University Press, 2007.

[48] E.I. Khukhro, *p-Automorphisms of finite p-groups*, Cambridge University Press, 1998.

[49] B. Klopsch, Substitution Groups, Subgroup Growth and Other Topics, Ph.D. Thesis, Oxford, 1999.

[50] B. Klopsch and A. Thillaisundaram, A pro-p group with infinite normal Hausdorff spectra, *Pac. J. Math.* **303** (2019), 569–603.

[51] B. Klopsch, A. Thillaisundaram, and A. Zugadi-Reizabal, Hausdorff dimensions in p-adic analytic groups, *Israel J. Math.* **231** (2019), 1–23.

[52] H. von Koch, Sur une courbe continue sans tangente, obtenue par une construction géométrique élémentaire, *Ark. Mat.* **1** (1904), 681–704.

[53] E. Kummer, Uber die Ergänzungssätze zu den allgemeinen Reziprozitäts-gesetzen, *J. für die Reine und Angew. Math.* **44** (1852), 93–146.

[54] M. Larsen, A. Shalev, Words, Hausdorff dimension and randomly free groups, *Math. Ann.* **371** (2018), 1409–1427.

[55] C.R. Leedham-Green, S. McKay, *The Structure of Groups of Prime Power Order*, Oxford University Press, 2002.

[56] M.W. Liebeck, E.A. O'Brien, A. Shalev, and P.H. Tiep, The Ore conjecture, *J. European Math. Soc.* **12** (2010), 939–1008.

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

[58] I.D. Macdonald, On cyclic commutator subgroups. *J. London Math. Soc. (1)* **38** (1963), 419–422.

[59] I.D. Macdonald, *The theory of groups*, Clarendon Press, 1968.

[60] I.D. Macdonald, Commutators and their products. *Amer. Math. Monthly* **93** (1986), 440–444.

[61] J.J. McCutcheon, A class of p-groups, *J. London Math. Soc.* **5** (1972), 79–84.

[62] G.A. Miller, The regular substitution groups whose orders is less than 48, *Q. J. Math.*, **28** (1896), 232–284.

[63] G.A. Miller, On the commutator groups, *Bull. Amer. Math. Soc.*, **4** (1898), 135–139.

[64] G.A. Miller, On the commutators of a given group, *Bull. Amer. Math. Soc.*, **6** (1899), 105–109.

[65] O. Ore, Some remarks on commutators, *Proc. Amer. Math. Soc.* **2** (1951), 307–314.

[66] J. Petresco, Sur les commutateurs, *Math. Z.* **61** (1954), 348–356.

[67] D.J.S. Robinson, *A Course in the Theory of Groups*. Second edition. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[68] D.M. Rodney, On cyclic derived subgroups, *J. London Math. Soc. (2)* **8** (1974), 642–646.

[69] D.M. Rodney, Commutators and abelian groups, *J. Austral. Math. Soc.* **24** (1977), 79–91.

[70] C. Sims, Enumerating p-groups, *Proc. London Math. Soc.* **15** (1965), 151–166.

[71] A. Shalev, Lie methods in the theory of pro-p groups, 1–54, in: *New horizons in pro-p groups* (eds. M. du Sautoy et al.), Birkhäuser, Boston, 2000.

[72] A. Shalev, On almost fixed point free automorphisms, *J. Algebra* **157** (1993), 271–282.

[73] D. Segal, *Words, Notes on Verbal Width in Groups*. Cambridge University Press, 2009.

[74] G. Traustason, Symplectic alternating algebras, *Int. J. Algebra and Comp.* **18** (2008), 719–757.

[75] G. Traustason, J. Williams, Powerfully nilpotent groups, *J. Algebra* **522** (2019), 80–100.

[76] G. Traustason, J. Williams, Powerfully nilpotent groups of maximal powerful class, *Monatsh. Math.* **191**(4) (2020), 779-799.

[77] G. Traustason, J. Williams, Powerfully nilpotent groups of rank 2 or small order, *J. Group Theory*, to appear.

[78] H. Weber, *Lehrbuch der Algebra*, Vol. 2, second edition. Braunschweig, 1899.

[79] J. Williams, Omegas of agemos in powerful groups, *Int. J. Group Theory*, to appear.

[80] J. Williams, Normal subgroups of powerful p-groups, *Israel J. Math.*, to appear.

[81] J.S. Wilson, *Profinite groups*. Clarendon Press, Oxford, 1998.

[82] L. Wilson, On the power structure of powerful p-groups, *J. Group Theory* **5** (2002), 129–144.

[83] L. Wilson, *Powerful groups of prime power order*, Ph.D. Thesis, University of Chicago, 2002.